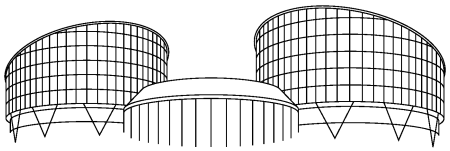

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

CORTE EUROPEA DEI DIRITTI DELL'UOMO

Guida alla giurisprudenza
della Corte europea
dei diritti dell'uomo

La protezione dei dati

Aggiornata in data 28 febbraio 2023

Gli editori o le organizzazioni che intendono tradurre e/o riprodurre la presente Guida integralmente, o parzialmente, in stampa, o in formato elettronico, sono invitati a compilare il modulo di contatto: *domanda di riproduzione o di ripubblicazione di una traduzione* per informazioni relative alla procedura di autorizzazione.

Per informazioni relative alle traduzioni delle Guide giurisprudenziali attualmente in corso, si prega di consultare l'elenco delle *traduzioni pendenti*.

La presente Guida è stata redatta originariamente in lingua francese. È aggiornata regolarmente e l'aggiornamento più recente è stato effettuato in data 28 febbraio 2023. Può subire modifiche di forma.

Le Guide giurisprudenziali possono essere scaricate dal sito *https://ks.echr.coe.int*. Per gli aggiornamenti relativi alla pubblicazione si prega di seguire il profilo Twitter della Corte sul sito *https://twitter.com/ECHR_CEDH*.

La presente traduzione è pubblicata a seguito di accordo con il Consiglio d'Europa e la Corte europea dei diritti dell'uomo sotto l'esclusiva responsabilità del Ministero della Giustizia italiano.

Il testo originale è stato utilizzato con l'autorizzazione del CdE/CEDU.

Indice

Nota per i lettori

La presente Guida fa parte della serie di Guide alla Convenzione pubblicata dalla Corte europea dei diritti dell'uomo (in prosieguo "la Corte", "la Corte europea" o "la Corte di Strasburgo") al fine di informare i professionisti del diritto in merito alle fondamentali sentenze e decisioni pronunciate dalla Corte. Questa particolare Guida analizza e reassume la giurisprudenza relativa a diversi articoli della Convenzione europea dei diritti dell'uomo (in prosieguo "la Convenzione" o "la Convenzione europea") in materia di protezione dei dati. Dovrebbe essere letta congiuntamente alle guide giurisprudenziali elaborate per articolo, cui essa rinvia sistematicamente.

La giurisprudenza citata è stata selezionata tra le sentenze e le decisioni di principio, le più importanti e/o le più recenti.*

Le sentenze e le decisioni della Corte non hanno soltanto la funzione di determinare le cause di cui essa è investita, bensì, più in generale, di chiarire, salvaguardare e sviluppare le norme istituite dalla Convenzione, contribuendo in tal modo all'osservanza, da parte degli Stati, degli impegni che hanno assunto in qualità di Parti contraenti (*Irlanda c. Regno Unito*, 18 gennaio 1978, § 154, Serie A n. 25, e, più recentemente, *Jeronovičs c. Lettonia* [GC], n. 44898/10, § 109, 5 2016).

Il sistema creato dalla Convenzione è quindi finalizzato a dirimere, nell'interesse generale, questioni di ordine pubblico, accrescendo in tal modo il livello di protezione dei diritti umani ed estendendo la relativa giurisprudenza a tutta la comunità degli Stati aderemti alla Convenzione (*Konstantin Markin c. Russia* [GC], 30078/06, § 89, CEDU 2012). La Corte ha infatti sottolineato il ruolo della Convenzione, "strumento costituzionale dell'ordine pubblico europeo" nel campo dei diritti umani (*Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi c. Irlanda* [GC], n. 45036/98, § 156, CEDU 2005-VI, e, più recentemente, *N.D. e N.T. c. Spagna* [GC], nn. 8675/15 e 8697/15, § 110, 13 febbraio 2020).

Il Protocollo n. 15 alla Convenzione ha recentemente inserito nel Preambolo della Convenzione il principio di sussidiarietà. Tale principio "impone una responsabilità condivisa tra gli Stati parti e la Corte" in ordine alla protezione dei diritti umani, e le autorità nazionali e i tribunali devono interpretare e applicare il diritto nazionale in modo da dare piena efficacia ai diritti e alle libertà sanciti dalla Convenzione e dai suoi Protocolli (*Grzęda c. Polonia* [GC], § 324).

*. La giurisprudenza citata può essere redatta in una o in entrambe le lingue ufficiali (l'inglese e il francese) della Corte e della Commissione europea dei diritti dell'uomo. Salvo diversa indicazione, i riferimenti concernono le sentenze di merito pronunciate da una Camera della Corte. L'abbreviazione "(dec.)" indica che si tratta della citazione di una decisione della Corte e "[GC]" che la causa è stata giudicata dalla Grande Camera. Le sentenze delle Camere non definitive alla data di pubblicazione del presente aggiornamento sono contrassegnate da un asterisco (*).

Introduzione

1. Il progresso tecnologico ha fatto compiere passi da gigante alla sorveglianza, all'intercettazione delle comunicazioni e alla conservazione dei dati, che hanno dato luogo a loro volta a maggiori sfide per la protezione dei dati personali. A decorrere dalla sentenza *Leander c. Svezia* del 1987, nella quale la "vecchia" Corte ha analizzato, per la prima volta, la questione della memorizzazione, da parte di un'autorità pubblica, dei dati personali di un individuo, la giurisprudenza degli organi della Convenzione in questo campo ha visto un significativo sviluppo.

2. Nel corso degli anni la Corte ha esaminato numerose situazioni in cui sono state sollevate questioni relative a questa problematica. Un ampio spettro di operazioni riguardanti i dati personali, quali la raccolta, la memorizzazione, l'uso e la diffusione di tali dati, è attualmente oggetto di una giurisprudenza degli organi della Convenzione che sarà descritta nella presente Guida. Tale giurisprudenza è stata elaborata in linea con la rapida evoluzione delle tecnologie dell'informatica e della comunicazione.

I. Definizioni e principi basilari della protezione dei dati

3. Il diritto alla protezione dei dati personali non è un diritto autonomo tra i vari diritti e le varie libertà previsti dalla Convenzione. La Corte ha tuttavia riconosciuto che la protezione dei dati personali è di fondamentale importanza per il godimento da parte di una persona del suo diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza, garantito dall'articolo 8 della Convenzione (*Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia* [GC], 2017, § 137; *Z c. Finlandia,* 1997, § 95). Tale articolo costituisce il principale vettore di protezione dei dati personali nel sistema della Convenzione, benché delle considerazioni connesse a tale protezione possano sorgere anche ai sensi di altre disposizioni della Convenzione e dei suoi Protocolli.

A. Terminologia della protezione dei dati

4. Lo sviluppo delle tecnologie ha comportato l'aumento delle tipologie di operazioni riguardanti dati personali che possono costituire un "trattamento automatizzato". Nonostante il generoso approccio della Corte alla definizione della nozione di "vita privata", che le ha permesso di elaborare una giurisprudenza in linea con l'evoluzione della società, una determinata operazione di trattamento dei dati non è necessariamente compresa nel campo di applicazione dell'articolo 8 o non compromette necessariamente uno degli interessi tutelati da tale articolo.

1. Nozione di dati personali e suo campo di applicazione

5. Nelle sue sentenze la Corte spiega la nozione di "dati personali" rinviando alla Convenzione n. 108 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale del 28 gennaio 1981, entrata in vigore nel 1985 e aggiornata nel 2018 ("Convenzione n. 108"), il cui fine è "quello di garantire, sul territorio di ciascuna Parte, ad ogni persona fisica (...) il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano" (articolo 1) (*Amann c. Svizzera* [GC], 2000, § 65; *Haralambie c. Romania*, 2009, § 77). La Corte ha indicato chiaramente che, ai sensi dell'articolo 2 della Convenzione n. 108, la nozione di dati a carattere personale descrive "ogni informazione concernente una persona fisica identificata o identificabile" (*Amann c. Svizzera* [GC], 2000, § 65; *Haralambie c. Romania,* 2009, § 77).

6. Tali dati comprendono non soltanto le informazioni che identificano direttamente un individuo ("l'interessato"), come il cognome o il prenome (*Guillot c. Francia*, 1996, §§ 21-22; *Mentzen c. Lettonia*

(dec.), 2004; *Güzel Erdagöz c. Turchia*, 2008, § 43; *Garnaga c. Ucraina*, 2013, § 36; *Henry Kismoun c. Francia,* 2013, § 25; *Hájovský c. Slovacchia*, 2021 §§ 11-12 e 41), bensì qualsiasi elemento che individui indirettamenre una persona, come un indirizzo IP (Internet Protocol) dinamico (*Benedik c. Slovenia*, 2018, §§ 107-108).

7. Benchè sembri che la questione della protezione dei dati personali riguardi principalmente le persone fisiche, in relazione al loro diritto di cui all'articolo 8 al rispetto della loro vita privata, anche le persone giuridiche hanno la facoltà di invocare tale diritto dinanzi alla Corte, se sono direttamente interessate da una misura che viola il loro diritto al rispetto della loro "corrispondenza" o del loro "domicilio". Ciò è avvenuto per esempio se è stato ordinato a una società di fornire una copia di tutti i dati di un server condiviso con altre società (*Bernh Larsen Holding AS e altri c. Norvegia*, 2013, § 106) o se il Ministero della Difesa, sulla base di un mandato, aveva intercettato le comunicazioni di ONG che si occupavano delle libertà civili (*Liberty e altri c. Regno Unito*, 2008, §§ 56-57). Tuttavia, in un caso relativo a misure riguardanti la tutela dei dati personali di membri di un'organizzazione religiosa e il rispetto della loro "vita privata", l'organizzazione non era interessato in modo diretto, e non era quindi una "vittima" ai sensi dell'articolo 34 della Convenzione (*Avilkina e altri c. Russia*, 2013, § 59).

8. I dati personali possono assumere forme molto differenti. Per esempio:

- Informazioni relative a un abbonato a internet associate a un indirizzo IP dinamico specifico attribuito in un determinato momento (*Benedik c. Slovenia*, 2018, §§ 108-109).
- Campioni di voci registrate di carattere permanente e sottoposte a un processo di analisi finalizzato direttamente a identificare una persona alla luce di altri dati personali (*P.G. e J.H. c. Regno Unito*, 2001, § 59).
- Campioni cellulari e profili del DNA (*S. e Marper c. Regno Unito* [GC], 2008, §§ 70-77) o impronte digitali (ibid., § 84) che, nonostante il loro carattere obiettivo e inoppugnabile, contenevano informazioni eccezionali sulla persona interessata e permettevano la sua precisa identificazione in un gran numero di circostanze (ibid., § 85).
- Informazioni relative a una determinata persona ottenute mediante documenti bancari, riguardanti particolari sensibili o un'attività professionale (*M.N. e altri c. San Marino*, 2015, §§ 51 e ss.).
- Dati relativi all'occupazione di una persona identificata o identificabile raccolti e memorizzati dalla polizia (*Khelili c. Svizzera*, 2011, § 56).
- Dati relativi all'utilizzo di internet e della messaggistica istantanea (Yahoo) da parte di un dipendente sul posto di lavoro, ottenuti mediante la sorveglianza (*Bărbulescu c. Romania* [GC], 2017, §§ 18, 74-81).
- Copia dei dati elettronici sequestrati in uno studio legale, benché non fossero stati decifrati, trascritti o attribuiti ufficialmente ai loro proprietari (*Kırdök e altri c. Turchia*, 2019, § 36).
- Dati raccolti nell'ambito di una videosorveglianza non segreta in un'università (*Antović e Mirković c. Montenegro*, 2017, §§ 44-45).
- Informazioni relative al reddito imponibile e al patrimonio di un elevato numero di persone, nonostante il fatto che il pubblico potesse accedere a tali dati a determinate condizioni (*Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia* [GC], 2017, § 138).
- Dati relativi alla nascita e all'abbandono di una persona, comprese le informazioni necessarie per scoprire la verità su un importante aspetto dell'identità personale (*Gaskin c. Regno Unito*, 1989, § 39; *Mikulić c. Croazia*, 2002, §§ 54-64; *Odièvre c. Francia* [GC], 2003, §§ 28-29).
- Dati compresi in un accordo di divorzio, comprendenti dettagli relativi alla divisione dei beni matrimoniali, all'affidamento e alla residenza di figli minori, all'accordo alimentare e a una visione d'insieme dei beni/del reddito del ricorrente (*Liebscher c. Austria*, 2021, §§ 31 e 68).

9. Ai sensi dell'articolo 2 della Convenzione n. 108, il "trattamento dei dati" comprende: "qualsiasi operazione o insieme di operazioni eseguite su dati personali, quali raccolta, conservazione, alterazione, reperimento, divulgazione, messa a disposizione, cancellazione o distruzione, oppure esecuzione di logiche e/o operazioni aritmetiche su tali dati". Lo sviluppo delle tecnologie ha dato luogo a un aumento dei tipi di operazione riguardanti dati personali che possono costituire un trattamento; la Corte ha individuato i seguenti tipici esempi:

- la raccolta da parte della polizia, presso un fornitore di servizi Internet, di informazioni associate all'indirizzo IP dinamico specifico di una persona (*Benedik c. Slovenia*, 2018, §§ 108-109).
- il fatto di raccogliere e memorizzare in modo sistematico informazioni di carattere pubblico relative a una persona, per esempio sulla sua attività politica (*Rotaru c. Romania* [GC], 2000, §§ 43-44; *Associazione "21 December 1989" e altri c. Romania*, 2011, §§ 167-168; *Amann c. Svizzera* [GC], 2000, §§ 65-67; *Catt c. Regno Unito*, 2019, § 93).
- l'inserimento del nominativo di una persona in una banca dati giudiziaria nazionale di autori di reati sessuali (*Gardel c. Francia*, 2009, § 58), nonché la raccolta e la memorizzazione delle impronte digitali di un sospettato (*M.K. c. Francia*, 2013, § 29).
- la registrazione segreta in un posto di polizia, al fine della memorizzazione permanente, di campioni vocali da utilizzare nell'identificazione delle persone interessate, mediante un processo di analisi nel contesto di altri dati personali (*P.G. e J.H. c. Regno Unito*, 2001, §§ 59-60).
- il fatto di filmare una persona nella stanza degli interrogatori della polizia, mediante telecamere installate per motivi di sicurezza e totalmente visibili, e la registrazione permanente della sequenza e il suo inserimento in un montaggio al fine di un ulteriore utilizzo (*Perry c. Regno Unito*, 2003, § 41).
- la raccolta e la conservazione sistematica di dati della sorveglianza GPS indicanti il luogo in cui si trova l'interessato e i suoi spostamenti pubblici (*Uzun c. Germania*, 2010, §§ 49-53).
- la pubblicazione in una rivista di un articolo illustrato da fotografie di celebrità scattate a loro insaputa (*Von Hannover c. Germania (n. 2)* [GC], 2012, §§ 95-99).
- la registrazione e la divulgazione ai media di sequenze provenienti da una televisione a circuito chiuso che mostravano una persona che tentava di suicidarsi in un luogo pubblico (*Peck c. Regno Unito*, 2003, §§ 59-63).
- la registrazione e la memorizzazione da parte della polizia di dati relativi alla ipotetica professione di una persona (*Khelili c. Svizzera*, 2011, § 56).
- la divulgazione ai giornalisti da parte di un ospedale psichiatrico di informazioni riservate estremamente sensibili relative alla vita privata di una paziente (*Mockutė c. Lituania*, 2018, § 99).
- la raccolta da parte dello Stato, nell'ambito di misure contro il doping nello sport, di informazioni relative ai luoghi in cui si trovavano atleti di alto livello e alle loro attività giornaliere, anche durante i fine settimana (*National Federation of Sportspersons' Associations and Unions (FNASS) e altri c. Francia*, 2018, §§ 155-159).
- la scannerizzazione e il caricamento sistematici della corrispondenza privata dei detenuti, sia in arrivo che in partenza, nel Server della rete giudiziaria nazionale (*Nuh Uzun e altri c. Turchia*, 2022, §§ 80-82).

10. La Corte considera quasi sempre tali misure delle ingerenze, aventi differenti livelli di gravità, nel diritto al rispetto della vita privata, del domicilio o della corrispondenza delle persone interessate.

11. Tuttavia, non tutte le operazioni relative a dati personali sono comprese nel campo di applicazione dell'articolo 8 o costituiscono ingerenze nei corrispondenti diritti. Pertanto, nella causa *Mehmedovic c. Svizzera* (dec.), 2018 (§ 18), la Corte ha ritenuto che informazioni sparse relative alla ricorrente, che

erano state raccolte fortuitamente e non avevano alcuna pertinenza con l'indagine in questione, non avessero costituito in alcun modo una raccolta di dati sistematica o permanente e non avevano quindi costituito un'ingerenza nel suo diritto al rispetto della sua vita privata. Inoltre, nella causa *Cakicisoy e altri c. Cipro* (dec.), 2014 (§§ 50-52), il fatto che le autorità avessero prelevato dei campioni ematici dei ricorrenti al fine di estrarre il profilo del loro DNA nell'ambito di un programma di esumazione finalizzato a identificare i loro parenti defunti, e che i campioni fossero stati distrutti quando erano scaduti i moduli di consenso, non è stato considerato un'ingerenza nel diritto dei ricorrenti al rispetto della loro vita privata.

12. Dalla giurisprudenza della Corte emerge che le operazioni relative ai dati personali sono comprese nel campo di applicazione dell'articolo 8 se le informazioni sono state raccolte in relazione a una precisa persona (*Amann c. Svizzera* [GC], 2000, §§ 66-67; *Rotaru c. Romania* [GC], 2000, §§ 43-44), se i dati in questione sono stati oggetto di una registrazione sistematica o permanente (*Uzun c. Germania*, 2010, § 51), se sono stati utilizzati in una procedura di analisi finalizzata direttamente a identificare una persona alla luce di altri dati personali (*P.G. e J.H. c. Regno Unito*, 2001, § 57) o se essi sono stati resi pubblici in modo o in misura eccedente quanto le persone avrebbero potuto ragionevolmente aspettarsi (*Peck c. Regno Unito,* 2003, §§ 58-59; *Perry c. Regno Unito,* 2003, § 38). Altre considerazioni riguarderanno il contesto specifico in cui sono state raccolte e conservate le informazioni, la natura delle registrazioni, il modo in cui sono utilizzate e trattate tali registrazioni e i risultati che possono essere ottenuti (*S. e Marper c. Regno Unito* [GC], 2008, § 67).

13. Un elemento significativo, benché non necessariamente determinante, è il fatto di sapere se una persona ha ragionevolmente diritto di aspettarsi la protezione della sua vita privata (*Perry c. Regno Unito,* 2003, § 37; *Bărbulescu c. Romania* [GC]*,* 2017, § 80). Quanto alle attività on-line, l'anonimato delle informazioni personali è un fattore fondamentale in tale valutazione e il fatto che un abbonato a un fornitore di servizi Internet non abbia nascosto il suo indirizzo IP dinamico non era determinante nella valutazione della questione di sapere se la sua aspettativa di privacy fosse ragionevole da un punto di vista obiettivo (*Benedik c. Slovenia*, 2018, § 116). Nel luogo di lavoro, le disposizioni del datore di lavoro non possono azzerare la vita privata sociale in tale luogo. Il rispetto per la vita privata e per la corrispondenza continua a esistere, benché esse possano essere limitate nella misura necessaria (*Bărbulescu c. Romania* [GC]*,* 2017, §§ 80-81). Le videoregistrazioni effettuate in un luogo pubblico utilizzando dei meccanismi di sorveglianza possono essere comprese nell'articolo 8 se la loro divulgazione, per le sue modalità o la sua portata, eccede quanto le persone avrebbero potuto ragionevolmente aspettarsi (*Peck c. Regno Unito*, 2003, § 62; *Perry c. Regno Unito,* 2003, §§ 41-43). Per quanto riguarda articoli della stampa relativi all'arresto di un attore televisivo, illustrati con fotografie, la Corte ha ritenuto che la "legittima aspettativa" dell'attore alla effettiva protezione della sua vita privata fosse stata ridotta dal fatto che egli aveva "cercato attivamente la ribalta", rivelando particolari della sua vita privata in diverse interviste (*Axel Springer AG c. Germania* [GC], 2012, § 101).

14. Quanto alla natura dei dati raccolti, alcuni tipi di dati personali e alcuni metodi di trattamento sono più problematici di altri perché rivelano informazioni più sensibili sul comportamento, le opinioni o i sentimenti delle persone (*Uzun c. Germania,* 2010, § 52, in cui la Corte ha comparato i dati raccolti mediante GPS ai dati raccolti mediante dispositivi di videosorveglianza o di sorveglianza acustica). La memorizzazione o la divulgazione, senza il consenso dell'interessato, di dati altamente intimi o sensibili, concernenti per esempio la salute di una persona, sono compresi necessariamente nel campo di applicazione dell'articolo 8 (*Z c. Finlandia,* 1997, § 71; *Radu c. Repubblica di Moldavia*, 2014, § 27; *Mockutė c. Lituania*, 2018, §§ 93-95). Data la natura e la quantità di informazioni personali contenute nei campioni cellulari, la loro conservazione deve *per se* essere considerata un'ingerenza nel diritto al rispetto della vita privata degli interessati, anche se soltanto una parte limitata di tali informazioni è effettivamente estratta o utilizzata dalle autorità e non è causato alcun immediato danno (*S. e Marper c. Regno Unito* [GC], 2008, §§ 70-77).

15. Il fatto che i dati personali siano già di dominio pubblico, o che il pubblico possa accedervi, non sottrae necessariamente tali dati alla protezione dell'articolo 8 (*Satakunnan Markkinapörssi Oy e*

Satamedia Oy c. Finlandia [GC], 2017, § 134). I dati di natura pubblica possono essere compresi nella "vita privata" di una persona se sono raccolti e memorizzati in modo sistematico (*P.G. e J.H. c. Regno Unito*, 2001, § 57; *Peck c. Regno Unito,* 2003, §§ 58-59; *Perry c. Regno Unito,* 2003, § 38), anche senza utilizzare metodi di sorveglianza segreta (*Rotaru c. Romania* [GC], 2000, §§ 43-44; *Antović e Mirković c. Montenegro*, 2017, §§ 44-45). L'articolo 8 della Convenzione prevede il diritto a una forma di autodeterminazione, che permette alle persone di invocare il loro diritto alla vita privata in relazione a dati che, benché neutri, siano raccolti, trattati e diffusi alla collettività e in forme o modalità tali da poter fare entrare in gioco diritti previsti dall'articolo 8 (*Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia* [GC], 2017, § 137).

16. Nella maggior parte dei casi in cui il trattamento dei dati personali era finalizzato a permettere alle autorità di svolgere un'indagine relativa alla persona interessata, o ad acquisire prove nell'ambito di un procedimento giudiziario dinanzi ai tribunali nazionali, la Corte ha ritenuto che tale trattamento fosse compreso nel campo di applicazione dell'articolo 8 e avesse comportanto un'ingerenza nel rispetto della vita privata della persona interessata (*Perry c. Regno Unito,* 2003, §§ 39-43; *Uzun c. Germania,* 2010, §§ 51-52; *Vukota-Bojić c. Svizzera*, 2016, §§ 57-59 ; *López Ribalda e altri c. Spagna* [GC], 2019, § 94 ; si raffronti, *a contrario*, *Lupker e altri c. Paesi Bassi*, 1992, relativa all'utilizzo da parte della polizia, al fine di identificare i ricorrenti, di fotografie che erano state consegnate volontariamente alle autorità, o che erano state scattate dalla polizia in relazione a precedenti arresti; *Friedl c. Austria*, 1994, §§ 50-51, sullo scatto di fotografie da parte delle autorità durante una manifestazione al fine di aprire un'indagine nei confronti dei ricorrenti per reati in materia di circolazione stradale).

17. Infine, perché entri in gioco l'articolo 8, i risultati derivanti dal trattamento di dati personali deve raggiungere un determinato livello di gravità e deve avvenire in modo da compromettere il godimento personale del diritto al rispetto della vita privata (*M.L. e W.W. c. Germania*, 2018, § 88). Nella causa *Vučina c. Croazia* (dec.) 2019 (§ 50), la Corte ha rigettato, in quanto incompatibile *ratione materiae,* una doglianza relativa alla pubblicazione di una fotografia su una rivista femminile sotto un titolo erroneo, che attribuiva alla ricorrente il nome di un'altra persona. Secondo la Corte, il basso livello di gravità di tale errore e il limitatissimo inconveniente causato non erano sufficienti a fare entrare in gioco l'articolo 8.

2. Specifiche categorie di dati

18. Alcune categorie di informazioni altamente intime o sensibili giustificano, secondo la Corte, una tutela rafforzata. Deve essere prestata attenzione anche ad altre categorie di dati, in considerazione degli sviluppi tecnologici che ampliano le possibilità di accesso a tali dati e comportano una maggiore interoperabilità.

a. Categorie cosiddette "sensibili"

19. Ai sensi dell'articolo 6 della Convenzione n. 108, i dati a carattere personale che rivelano l'origine razziale, le opinioni politiche, le convinzioni religiose o altre convinzioni, nonché i dati a carattere personale relativi alla salute o alla vita sessuale, nonché quelli relativi a condanne penali, non possono essere elaborati automaticamente, salvo qualora il diritto interno preveda appropriate garanzie. Le informazioni comprese in tali categorie, definite dalla Corte "sensibili", giustificano, a suo avviso, un accresciuto livello di tutela.

i. Dati che rivelano l'origine razziale o etnica

20. L'identità etnica di una persona deve essere considerata un importante elemento della sua vita privata (*S. e Marper c. Regno Unito*, [GC], 2008, § 66; *Ciubotaru c. Moldavia*, 2010, § 49). I dati sono particolarmente importanti se possono rivelare l'origine etnica o di altro tipo di una persona, tenendo presente la rapida velocità degli sviluppi nel campo della genetica e dell'informatica (*S. e Marper c.*

Regno Unito [GC], 2008, § 71). I campioni e i profili del DNA contengono informazioni molto sensibili e consentono alle autorità di accertare le relazioni genetiche tra le persone e valutare la loro probabile origine etnica (ibid., §§ 72-77; *Aycaguer c. Francia,* 2017, § 33). In una causa relativa all'indicazione dell'origine etnica di una persona nei registri ufficiali, la Corte, sottolineando la natura altamente sensibile della registrazione di tali dati, ha riconosciuto l'esistenza di un obbligo positivo da parte dello Stato di predisporre una procedura che consenta alla persona interessata di modificare l'origine etnica registrata sulla base di prove verificabili oggettivamente (*Ciubotaru c. Moldavia*, 2010, §§ 52-59).

ii. Dati che rivelano le opinioni politiche, le convinzioni religiose o di altro tipo, comprese quelle filosofiche

21. I dati che rivelano le opinioni politiche sono considerati una categoria di dati personali "sensibile" e, secondo la Corte, è inaccettabile che le autorità nazionali trascurino tale aspetto trattando tali dati seguendo le ordinarie norme interne, senza tenere conto della necessità di una accresciuta protezione (*Catt c. Regno Unito*, 2019, § 112). Nella causa *Catt c. Regno Unito*, del 2019, concernente la conservazione in una banca dati di polizia di dati relativi a un manifestante pacifico, nell'esame della legittimità dell'ingerenza i giudici nazionali avevano meramente rinviato alla legge sulla protezione dei dati in generale. La Corte ha constatato la violazione dell'articolo 8, sottolineando che il carattere sensibile dei dati in questione avrebbe dovuto costituire un elemento fondamentale della causa di cui erano investiti i giudici nazionali, come lo era dinanzi alla Corte (ibid., § 112). La Corte ha analogamente riscontrato la violazione dell'articolo 8 nella causa *M.D. e altri c. Spagna*, 2022, (§§ 63-64) concernente un rapporto redatto dalla polizia riguardo a giudici e magistrati, che esercitavano le loro funzioni in Catalogna e che avevano firmato un manifesto nel quale avevano esposto il loro parere giuridico a favore della possibilità dell'esercizio da parte del popolo catalano del cosiddetto "diritto di decidere", rapporto che rivelava, in particolare, le opinioni politiche di alcuni ricorrenti.

22. Il diritto alla protezione dei dati personali che rivelano le convinzioni religiose o altre convizioni, comprese quelle filosofiche, di una persona è stato esaminato dalla Corte nelle cause *Sinan Işık c. Turchia*, 2010 (§ 37) e *Mockutė c. Lituania*, 2018 (§ 117). Quanto all'indicazione della confessione religiosa sulle carte d'identità dei ricorrenti, la Corte ha sottolineato l'importanza del diritto alla protezione dei dati relativi alle convinzioni religiose, che costituivano uno degli elementi più essenziali che formano l'identità dei credenti e la loro concezione della vita, tutelati dall'articolo 9 della Convenzione (*Sinan Işık c. Turchia,* 2010, § 37).

iii. Dati che rivelano l'appartenenza a un sindacato

23. Anche i dati personali che rivelano l'appartenenza di una persona a un sindacato possono essere "sensibili" e giustificano quindi una protezione rafforzata. Nella causa *Catt c. Regno Unito*, del 2019 (§ 112), la polizia aveva raccolto informazioni relative alla partecipazione del ricorrente a manifestazioni organizzate da diversi sindacati, in particolare il suo nome, la sua presenza, la sua data di nascita e il suo indirizzo. In alcuni casi era stata descritta anche la sua apparizione, unitamente a fotografie scattate durante le manifestazioni in questione (ibid., § 10). La partecipazione a proteste pacifiche beneficia di una particore protezione ai sensi dell'articolo 11 della Convenzione, che contiene anche una protezione speciale per i sindacati (ibid., § 123). Benché la raccolta da parte della polizia di dati personali relativi al ricorrente potesse essere considerata giustificata, secondo la Corte non vi era alcuna impellente necessità di conservare i dati del ricorrente, in assenza di norme che fissassero un termine massimo definitivo per la conservazione di tali dati (ibid., §§ 117-119).

iv. Dati genetici e biometrici

24. La Corte ha trattato diverse cause concernenti la raccolta o la conservazione di:

- campioni cellulari (*Van der Velden c. Paesi Bassi* (dec.), 2005; *Schmidt c. Germania* (dec.), 2006; *S. e Marper c. Regno Unito* [GC], 2008; *Canonne c. Francia* (dec.), 2015; *Caruana*

c. Malta (dec.), 2018; *Trajkovski e Chipovski c. Macedonia del Nord*, 2020; *Boljević c. Serbia*, 2020);

- profili del DNA (*Van der Velden c. Paesi Bassi* (dec.), 2005; *Schmidt c. Germania* (dec.), 2006; *S. e Marper c. Regno Unito* [GC], 2008; *W. c. Paesi Bassi* (dec.), 2009; *Peruzzo e Martens c. Germania* (dec.), 2013; *Canonne c. Francia* (dec.), 2015; *Aycaguer c. Francia*, 2017; *Mifsud c. Malta*, 2019; *Gaughran c. Regno Unito*, 2020; *Trajkovski e Chipovski c. Macedonia del Nord*, 2020; *Dragan Petrović c. Serbia*, 2020);
- impronte digitali (*McVeigh, O'Neill ed Evans c. Regno Unito*, 1981; *Kinnunen c. Finlandia*, 1993; *S. e Marper c. Regno Unito* [GC], 2008; *Dimitrov-Kazakov c. Bulgaria*, 2011; *M.K. c. Francia*, 2013; *Suprunenko c. Russia* (dec), 2018; *Gaughran c. Regno Unito*, 2020; *P.N. c. Germania*, 2020); *Willems c. Paesi Bassi* (dec.), 2021);
- impronte palmari (*P.N. c. Germania*, 2020);
- campioni vocali (*P.G. e J.H. c. Regno Unito*, 2001; *Allan c. Regno Unito*, 2002; *Doerga c. Paesi Bassis*, 2004; *Vetter c. Francia*, 2005; *Wisse c. Francia*, 2005).

25. Tenendo presente la rapida velocità degli sviluppi nel campo della genetica e dell'informatica, la Corte non può sminuire l'importanza della possibilità che in futuro gli interessi della vita privata legati alle informazioni genetiche possano essere lesi in nuovi modi o in un modo che non può essere attualmente previsto con precisione (*S. e Marper c. Regno Unito* [GC], 2008, § 71).

26. Quanto ai campioni cellulari, data la natura e la quantità di informazioni personali che essi contengono, la loro conservazione deve essere considerata *per se* un'ingerenza nel diritto al rispetto della vita privata delle persone interessate. Il fatto che soltanto una limitata parte di tali informazioni sia effettivamente estratta o utilizzata dalle autorità mediante la profilazione del DNA e che in un particolare caso non sia causato alcun immediato pregiudizio non modifica tale conclusione (ibid., § 73; *Amann c. Svizzera* [GC], 2000, § 69).

27. In materia di profili del DNA, la possibiità di dedurre da essi l'origine etnica di una persona rende la loro conservazione ancora più sensibile e in grado di ledere il diritto alla vita privata, ed esige quindi un'accresciuta protezione (*S. e Marper c. Regno Unito* [GC], 2008, § 76). Benché le informazioni contenute nei profili possano essere considerate obiettive e inconfutabili, la loro capacità di fornire un mezzo per individuare le relazioni genetiche tra le persone è di per sé sufficiente per concludere che la loro conservazione costituisce un'ingerenza nel diritto alla vita privata delle persone interessate, nonostante le garanzie o il livello di probabilità di un pregiudizio in un dato caso (ibid., § 75; *Amann c. Svizzera* [GC], 2000, § 69). Tale conclusione non è influenzata dal fatto che, poiché le informazioni sono in forma codificata, esse siano intellegibili soltanto utilizzando l'informatica e possano essere interpretate soltanto da un limitato numero di persone (*S. e Marper c. Regno Unito* [GC], 2008, §§ 74-75).

28. Riguardo alle impronte digitali, poiché esse contengono oggettivamente informazioni uniche sulla persona interessata, che permettono di identificarla con precisione in un gran numero di circostanze, la conservazione di tali informazioni senza il consenso della persona interessata non può essere considerata neutrale o insignificante (ibid., § 84). Benché la conservazione delle impronte digitali nei registri delle autorità, in relazione a una persona identificata o identificabile, possa avere un impatto sulla vita privata inferiore alla conservazione di campioni cellulari e di profili del DNA (ibid., § 69), essa può dare luogo a importanti preoccupazioni in materia di rispetto della vita privata, nonostante il carattere obiettivo e inconfutabile di tali dati (ibid., § 85, che si discosta dalla giurisprudenza basata sulla decisione della Commissione relativa alla causa *Kinnunen c. Finlandia,* 1996). Nella causa *Willems c. Paesi Bassi* (dec.), 2021, le doglianze relative all'obbligo ai sensi della Legge in materia di passaporti che imponeva il rilievo delle impronte digitali al momento della richiesta di un passaporto, nonché la memorizzazione di tali impronte su un chip elettronico, a seguito del recepimento nella legislazione nazionale (senza lasciare alcun margine di manovra alle autorità nazionali) del Regolamento dell'Unione europea sule caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei

documenti di viaggio rilasciati dagli Stati membri, sono stae rigettate in quanto manifestamente infondate a causa della "presunzione di protezione equivalente" nel diritto dell'Unione europea (ibid., §§ 26-36).

29. A causa delle informazioni che contengono, la conservazione di campioni cellulari e di profili del DNA ha sulla vita privata un impatto maggiore della conservazione di impronte digitali (*S. e Marper c. Regno Unito* [GC], 2008, § 86). Tuttavia, mentre può essere necessario operare una distinzione tra il prelievo, l'utilizzo e la memorizzazione di impronte digitali, da una parte, e di campioni e profili, dall'altra, nel determinare la questione della giustificazione, la conservazione di impronte digitali costituisce *per se* un'ingerenza nel diritto al rispetto della vita privata.

30. In determinate circostanze, specialmente nelle cause finalizzate all'accertamento della paternità, le autorità possono obbligare una persona a sottoporsi a un esame del DNA, a condizione che i diritti di difesa della persona siano rispettati e che i giudici nazionali pervengano a un giusto equilibrio degli interessi in questione (*Mifsud c. Malta*, 2019, §§ 77-78). L'articolo 8 non proibisce di per sé il ricorso al fine di ottenere delle prove a un intervento medico contro la volontà di una persona sospettata o di un testimone, in quanto tali metodi, anche nella sfera civile, non violano di per sé lo Stato di diritto o la giustizia naturale (ibid., § 71). Un ordinamento che non dispone di mezzi per obbligare un padre putativo a osservare un ordine di un tribunale che dispone l'esecuzione di esami del DNA può in linea di principio essere considerato compatibile con gli obblighi derivanti dall'articolo 8, specialmente se prevede mezzi alternativi che permettono a un'autorità indipendente di determinare rapidamente la domanda di accertamento della paternità (*Mikulić c. Croazia*, 2002, §§ 55, 64).

v. Dati relativi alla salute, alla vita sessuale o all'orientamento sessuale

31. Le informazioni concernenti la salute di una persona costituiscono un importante elemento della sua vita privata (*Yvonne Chave nata Jullien c. Francia,* 1991, § 75; *L.L. c. Francia*, 2006; *Radu c. Moldavia*, 2014; *L.H. c. Lettonia*, 2014, § 56; *Konovalova c. Russia*, 2014, §§ 27, 41; *Y.Y. c. Russia*, 2016, § 38; *Surikov c. Ucraina*, 2017; *Frâncu c. Romania*, 2020, § 52). Il rispetto del carattere riservato di tali informazioni è cruciale, non soltanto per rispettare la vita privata del paziente, bensì anche per preservare la sua fiducia nella professione medica e nei servizi sanitari in generale. Tali considerazioni sono particolarmente valide riguardo alla protezione della riservatezza delle informazioni relative alla sieropositività di una persona all'HIV (*Z c. Finlandia*, 1997, § 96; *Kiyutin c. Russia*, 2011, § 64; *Armonienė c. Lituania*, 2008, § 40; *Biriuk c. Lituania*, 2008, § 39; *I. c. Finlandia*, 2008, § 38; *C.C. c. Spagna*, 2009, § 33; *Y. c. Turchia* (dec.), 2015, § 65; *P.T. c. Repubblica di Moldavia*, 2020, §§ 5-6, 26; *Y.G. c. Russia*, 2022, § 45). La divulgazione di tali dati può incidere drammaticamente sulla sua vita privata e familiare, nonché sulla sua situazione sociale e lavorativa, esponendola al disprezzo e al rischio di ostracismo (*Z c. Finlandia*, 1997, § 96; *C.C. c. Spagna*, 2009, § 33; *P. e S. c. Polonia*, 2012, § 128; *Avilkina e altri c. Russia,* 2013, § 45; *Y. c. Turchia* (dec.), 2015, § 65; *Y.G. c. Russia*, 2022, § 45).

31. L'interesse a proteggere la riservatezza di tali informazioni avrà pertanto un importante peso nel determinare la proporzionalità dell'ingerenza al fine legittimo perseguito. Una simile ingerenza non può essere compatibile con l'articolo 8 della Convenzione, salvo qualora essa sia giustificata da un'esigenza inderogabile di interesse pubblico (*Z c. Finlandia*, 1997, § 96). In considerazione del carattere altamente intimo e sensibile delle informazioni relative alla sieropositività di una persona all'HIV, qualsiasi misura statale che obblighi a comunicare o a divulgare tali informazioni senza il consenso del paziente esige un esame estremamente rigoroso da parte della Corte (ibid., § 96).

32. La Corte ha quindi constatato per esempio la violazione dell'articolo 8 nelle cause *Z c. Finlandia*, 1997 (§§ 113-114), a causa della pubblicazione dell'identità e della sieropositività all'HIV di una donna in una sentenza, pronunciata nel corso di un procedimento penale nei confronti di suo marito, che era stata riferita dalla stampa; *L.L. c. Francia*, 2006 (§§ 32-48), per la riproduzione in un decreto di divorzio di un estratto di un documento medico personale; *I. c. Finlandia*, 2008 (§§ 35-49), per l'insufficiente protezione dall'accesso non autorizzato alla cartella clinica di un'infermiera sieropositiva all'HIV; *C.C.*

c. Spagna, 2009 (§§ 26-41), per la pubblicazione dell'identità del ricorrente in una sentenza connessa alla sua sieropositività all'HIV; *P. e S. c. Polonia*, 2012 (§§ 128-137), per la divulgazione di informazioni da parte di un ospedale pubblico relative a una ragazza incinta che intendeva abortire a seguito di violenza sessuale; *Konovalova c. Russia*, 2014 (§§ 39-50), in cui la ricorrente aveva lamentato di avere dovuto partorire alla presenza di studenti di medicina senza avervi acconsentito; *P.T. c. Repubblica di Moldavia*, 2020 (§§ 24-33), per la presenza non necessaria di dati medici sensibili in un certificato destinato a vari usi; *Frâncu c. Romania*, 2020 (§ 52), per il rifiuto di concedere la celebrazione di un'udienza a porte chiuse, in una causa concernente la corruzione di un sindaco, relativamente a una domanda di scarcerazione per motivi di salute; e *Y.G. c. Russia*, 2022 (§§ 46-53), in cui il ricorrente ha lamentato che una banca dati contenente, in particolare, i suoi dati sanitari era stata messa in vendita in un mercato.

33. Le informazioni relative alla salute mentale di una persona costituiscono dei dati altamente sensibili (*Mockutė c. Lituania,* 2018, § 94, concernente la divulgazione di dati relativi alla salute mentale di un paziente da parte di un ospedale psichiatrico; *Malanicheva c. Russia* (dec.), 2016, §§ 13, 15-18, concernente la registrazione in una cartella ospedaliera di dati relativi al ricovero coatto dei ricorrenti), come i dati che rivelano l'identificazione o l'orientamento sessuale (*Dudgeon c. Regno Unito*, 1981, § 41, *J.L. c. Italia*, 2021, § 136, e *Drelon c. Francia*, 2022, § 79) e la vita sessuale di una persona, come i dati relativi a un aborto trasmessi da un'autorità pubblica a un'altra, senza il consenso della persona interessata (*M.S. c. Svezia*, 1997, §§ 41-42). La legislazione nazionale deve offrire adeguate garanzie per impedire la comunicazione o la divulgazione di tali dati non conforme alle garanzie di cui all'articolo 8 (*Z c. Finlandia*, 1997, § 95).

vi. Dati relativi a reati e a condanne penali

34. I dati relativi a reati, procedimenti penali, condanne o a misure cautelari connesse costituiscono una categoria di dati che giustifica un'accresciuta protezione ai sensi dell'articolo 6 della Convenzione n. 108 (*M.M. c. Regno Unito*, 2012, § 188). Il trattamento di dati personali relativi a una persona nei cui confronti è stato pronunciato il non luogo a procedere (*Brunet c. Francia,* 2014, §§ 38-40), che è stata ammonita (*M.M. c. Regno Unito*, 2012, §§ 188-190), condannata e cui è stata inflitta una pena (*Gardel c. Francia*, 2009, § 58 ; *Peruzzo e Martens c. Germania* (dec.), 2013, § 44; *Trajkovski e Chipovski c. Macedonia del Nord*, 2020, § 46) o sottoposta a una misura cautelare connessa quale il fermo in una stazione di polizia (*Suprunenko c. Russia*, (dec.), 2018, § 61), costituiranno un'ingerenza nel diritto della persona interessata al rispetto della sua vita privata.

35. Secondo la Corte, benché i dati contenuti in un casellario giudiziale siano, in un certo senso, delle informazioni pubbliche, la loro memorizzazione sistematica negli archivi centrali significa che essi possono essere divulgati molto tempo dopo l'evento quando tutti, tranne la persona interessata, lo hanno probabilmente dimenticato. Pertanto, poiché la condanna o l'ammonimento si perdono nel passato, esse diventano parte integrante della vita privata di una persona che deve essere rispettata (*M.M. c. Regno Unito*, 2012, § 188), tanto più se i dati concernono il remoto passato di una persona (*B.B. c. Francia*, 2009, § 57; *Catt c. Regno Unito*, 2019, § 93; *M.L. e W.W. c. Germania*, 2018, §§ 98-100).

36. Una misura che implica la conservazione, nei registri della polizia, dei dati identificativi di una persona, delle impronte digitali e delle fotografie identificative può avere gravi conseguenze per la stessa, rendendo più difficile la sua vita quotidiana (*Dimitrov-Kazakov c. Bulgaria*, 2011, §§ 8, 10, 13, 30). In una causa relativa alla registrazione di una persona come "delinquente" nei registri della polizia, successivamente al suo interrogatorio in relazione a una violenza sessuale, e alla conservazione di tale registrazione benché non fosse stata formulata alcuna imputazione, la Corte ha riscontrato la violazione dell'articolo 8, ritenendo che la persona interessata, proprio a causa della registrazione in questione, fosse stata sottoposta a diversi controlli di polizia in relazione a denunce per violenza sessuale o a scomparse di ragazze (ibid., §§ 8, 10, 13, 30).

b. Altre categorie di dati

37. Oltre ai dati definiti "sensibili", anche altre categorie di dati personali suscitano preoccupazione, specialmente date le tecniche di sorveglianza sempre più sofisticate e la capacità delle tecnologie dell'informazione e della comunicazione di rendere più difficile la vita quotidiana delle persone interessate.

i. Dati relativi all'impiego

38. La memorizzazione di dati relativi a una persona identificata o identificbile connessi alla sua professione e la loro conservazione costituiscono un'ingerenza nel diritto della persona interessata al rispetto della sua vita privata e familiare di cui all'articolo 8 (*Khelili c. Svizzera*, 2011, § 56; *Sõro c. Estonia*, 2015, §§ 49 e 56; *Florindo de Almeida Vasconcelos Gramaxo c. Portogallo*, 2022, §§ 95-96). Dato che le informazioni raccolte dalle autorità e conservate nei loro archivi sono attualmente oggetto di un trattamento automatizzato che facilita notevolmente l'accesso a tali dati e la loro trasmissione, tali misure potrebbero avere gravi conseguenze in grado di nuocere alla reputazione delle persone o di rendere più difficile la loro vita quotidiana. La Corte ha riscontrato la violazione dell'articolo 8 nella causa *Khelili c. Svizzera,* 2011 (§ 64), in cui la ricorrente era stata schedata dalla Polizia come "prostituta", registrazione successivamente corretta e sostituita nella banca dati da "cucitrice", e *Sõro c. Estonia*, 2015 (§ 63), in cui il ricorrente era stato obbligato a lasciare il lavoro successivamente alla divulgazione di dati relativi al suo impiego in qualità di autista per i vecchi Servizi di sicurezza. Nella causa *Florindo de Almeida Vasconcelos Gramaxo c. Portogallo*, 2022 (§§ 95-96), in cui il datore di lavoro del ricorrente aveva installato un sistema GPS nell'automobile di servizio del ricorrente, al fine di controllare le distanze percorse nel corso della sua attività professionale e, se del caso, durante gli spostamenti privati, la Corte ha ritenuto che le informazioni raccolte costituissero dei dati personali. Ha inoltre sottolineato che i dipendenti non erano stati autorizzati a disattivare il sistema GPS, quindi esso rimaneva attivo 24 ore su 24, sette giorni a settimana, con il risultato che la sorveglianza era permanente e sistematica, il che comportava chiaramente un'ingerenza nella vita privata del ricorrente[1].

ii. Dati finanziari

39. Le informazioni ottenute dalla documentazione bancaria di una persona costituiscono dei dati personali, sia che si tratti di informazioni sensibili di carattere privato che di informazioni relative alle attività professionali della persona interessata (*M.N. e altri c. San Marino,* 2015, § 51; *G.S.B. c. Svizzera*, 2015, § 51). La copiatura da parte delle autorità di dati bancari e la loro successiva memorizzazione, atti compresi sia nella nozione di "vita privata" che di "corrispondenza", costituiscono un'ingerenza ai fini dell'articolo 8 (*M.N. e altri c. San Marino*, 2015, § 55).

40. La Corte ha esaminato la questione della raccolta, del trattamento e della divulgazione di dati finanziari nell'ambito di: un'indagine penale (*M.N. e altri c. San Marino*, 2015, §§ 7-9, 53-55); la pubblicazione su vasta scala da parte della stampa di dati finanziari al fine di un dibattito su una questione di interesse generale (*Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia* [GC], 2017, §§ 172-173); l'obbligo per un avvocato di rivelare dati coperti dal segreto professionale dichiarando i suoi sospetti riguardo ad attività illecite come il riciclaggio da parte di suoi assistiti (*Michaud c. Francia,* 2012, §§ 91-92); la trasmissione di dati finanziari alle autorità di un altro Stato che non è parte della Convenzione (*G.S.B. c. Svizzera*, 2015, § 50); e infine, il rigetto di un'azione concernente la divulgazione di informazioni relative al codice fiscale e alla dichiarazione dei redditi della ricorrente durante un servizio televisivo su un procedimento penale nei confronti di suo marito (*Samoylova c. Russia*, 2021, §§ 83 e 90-93).

[1] Si veda altresì "Dati di localizzazione GPS" *infra*.

41. L'esistenza di un interesse generale a fornire accesso a notevoli quantità di dati fiscali e a permetterne la raccolta non significa necessariamente e automaticamente che vi sia anche un interesse generale alla divulgazione *en masse* di tali dati grezzi, in forma inalterata, senza alcun apporto analitico (*Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia* [GC], 2017, §§ 172-178, 198).

42. Benché, in materia fiscale, il margine di discrezionalità dello Stato sia più ampio quando si tratta della protezione di dati puramente finanziari, che non comprendono alcun dato personale o strettamente connesso all'identità della persona interessata (*G.S.B. c. Svizzera*, 2015, § 93), entrano in gioco considerazioni relative alla vita privata in situazioni in cui i dati fiscali siano stati raccolti riguardo a una precisa persona, o se sono stati resi pubblici in modo o in misura eccedente quanto la persona interessata avrebbe potuto ragionevolmente prevedere (*M.N. e altri c. San Marino*, 2015, §§ 52-53 ; *Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia* [GC], 2017, § 136).

iii. Dati relativi al traffico

43. I dati relativi al traffico comprendono i dati ottenuti da operatori telefonici che identificano la persona alla quale o dalla quale è trasmessa una comunicazione, unitamente alla data, all'ora e alla durata della comunicazione, ma che non riguardano il contenuto di tale comunicazione (*Malone c. Regno Unito,* 1984, §§ 83-84; *Copland c. Regno Unito*, 2007, § 43). Nell'ambito di un'indagine penale, la procedura nota come "conteggio", che riguarda l'uso di un dispositivo (un contatore collegato a una stampante di controllo) che registra i numeri composti su un determinato telefono, nonché l'ora e la durata di ciascuna telefonata, senza controllare o intercettare le comunicazioni, costituisce un'ingerenza nella vita privata della persona interessata (*Malone c. Regno Unito*, 1984, §§ 83-84). L'utilizzo di tali dati e, in particolare, dei numeri composti può dare luogo a una questione ai sensi dell'articolo 8, in quanto tali informazioni costituiscono un "elemento integrante delle comunicazioni effettuate per mezzo del telefono" (*Malone c. Regno Unito*, 1984, § 84; *Copland c. Regno Unito*, 2007, § 43). Secondo la Corte, anche la comunicazione di tali informazioni alla Polizia senza il consenso dell'abbonato costituisce, ad avviso della Corte, un'ingerenza in un diritto garantito dall'articolo 8 (*Malone c. Regno Unito*, 1984, § 84).

44. La prassi del "conteggio", che non viola l'articolo 8 se è svolta, per esempio, da parte del fornitore di un servizio telefonico per assicurare che l'abbonato riceva le fatture correttamente, deve essere distinta per la sua stessa natura dall'intercettazione delle telefonate (*Malone c. Regno Unito*, 1984, §§ 83-84; *P.G. e J.H. c. Regno Unito*, 2001, § 42). Il decreto di un tribunale inviato a una società telefonica al fine di ottenere i dati relativi alle telefonate effettuate a e da diversi telefoni cellulari di una persona, e che le chiede di raccogliere i dati relativi alle celle telefoniche al fine del successivo rilevamento dei suoi spostamenti, non era necessariamente incompatibile con l'articolo 8 nella misura in cui era autorizzato dalla legge e assicurava sufficienti garanzie contro le arbitrarietà (*Ben Faiza c. Francia*, 2018, §§ 56, 59, 69). La Corte non ha riscontrato alcuna violazione dell'articolo 8 in un caso in cui tali decreti dovevano essere autorizzati anticipatamente da un pubblico ministero sotto pena di nullità e potevano essere impugnati dinanzi ai tribunali, e in cui i dati ottenuti potevano essere esclusi dalle prove in caso di illegalità (ibid., §§ 79, 73).

45. I dati personali di utenti di carte SIM prepagate, quali i nomi, gli indirizzi e i numeri telefonici di abbonati a servizi di telefonia mobile, raccolti dai fornitori dei servizi, non possono essere considerati "insignificanti" (*Breyer c. Germania*, 2020, §§ 92-95). La mera memorizzazione, da parte di fornitori di servizi di comunicazione, di tali dati dell'abbonato, costituisce un'ingerenza nella vita privata dell'interessato, a prescindere dal successivo uso (ibid., § 92). Tale ingerenza è di carattere piuttosto limitato (ibid., § 95) e le autorità nazionali godono di un certo margine di discrezionalità in questo campo, in assenza di un'unanimità europea (ibid., § 90). L'assenza di notifica di una procedura di recupero non è incompatibile con l'articolo 8, nella misura in cui esiste un controllo da parte di un'autorità indipendente, competente a esaminare, se ritenuto giustificato, se sia accettabile trasmettere i dati a un'autorità richiedente, e una possibilità di ricorso da parte di chiunque ritenga

che i suoi diritti siano stati violati mediante una procedura di recupero o una domanda di comunicazione di dati (ibid., §§ 103-107).

46. Quanto ai dati relativi a una comnessione a internet, essi possono permettere l'identificazione dell'utente, per esempio il suo indirizzo IP, il suo indirizzo di posta elettronica, i destinatari delle comunicazioni, informazioni relative al materiale delle comunicazioni utilizzato e qualsiasi servizio aggiuntivo richiesto o utilizzato e il loro fornitore (*Benedik c. Slovenia*, 2018, § 96). Secondo la Corte, le informazioni relative a un abbonato associate a specifici indirizzi IP dinamici attribuiti in determinati periodi costituiscono dei dati personali. Essi non sono accessibili pubblicamente e non possono pertanto essere paragonati alle informazioni reperibili in un tradizionale elenco telefonico o in una banca dati pubblica dei numeri di immatricolazione dei veicoli (ibid., § 108).

47. L'acquisizione dei dati connessi alle comunicazioni nell'ambito di intercettazioni in massa non è necessariamente meno invasiva dell'acquisizione del contenuto delle comunicazioni (*Centrum för rättvisa c. Svezia* [GC], 2021, 277, e *Big Brother Watch e altri c. Regno Unito* [GC], 2021, § 363). L'intercettazione, la conservazione e la ricerca di dati connessi alle comunicazioni dovrebbero essere analizzate con riferimento alle medesime garanzie applicabili al contenuto. Detto ciò, in considerazione del differente carattere dei dati connessi alle comunicazioni e dei differenti modi in cui essi sono utilizzati da parte dei Servizi segreti, fintanto che sussistono le medesime garanzie, le disposizioni giuridiche che disciplinano il loro trattamento non devono essere necessariamente identiche sotto ogni aspetto a quelle che disciplinano il trattamento del contenuto delle comunicazioni (*Centrum för rättvisa c. Svezia* [GC], 2021, § 278; e *Big Brother Watch e altri c. Regno Unito* [GC], 2021, § 364).

48. Un'inderogabile esigenza di riservatezza dei dati relativi al traffico può, in alcune circostanze, rivelarsi incompatibile con l'articolo 8 se impedisce un'indagine penale effettiva, finalizzata a individuare e perseguire l'autore di un reato commesso mediante internet (*K.U. c. Finlandia,* 2008, § 49). La garanzia degli utenti di servizi di telecomunicazioni e di internet del rispetto della loro vita privata deve farsi da parte in occasione di altri legittimi imperativi, quali la prevenzione dei reati e la protezione dei diritti e delle libertà altrui (ibid., § 49).

iv. Campioni vocali

49. Le operazioni di "intercettazione mediante microspie" sono finalizzate a intercettare le conversazioni di una persona mediante l'installazione di dispositivi di ascolto in un locale privato (*Vetter c. Francia*, 2005, §§ 10, 20) o in luoghi pubblici (*P.G. e J.H. c. Regno Unito*, 2001, §§ 38, 63; *Allan c. Regno Unito*, 2002, § 35; *Doerga c. Paesi Bassi*, 2004, § 43; *Wisse c. Francia*, 2005, § 29).

50. La registrazione segreta della voce di una persona e il mantenimento di un registro permanente soggetto a una procedura di analisi finalizzata direttamente a identificare tale persona, nell'ambito di altri dati personali, costituisce un trattamento di dati personali che rappresenta un'ingerenza nel diritto della persona interessata al rispetto della sua vita privata (*P.G. e J.H. c. Regno Unito*, 2001, §§ 59-60). In un caso in cui non vi era alcuna legge nazionale che disciplinasse l'uso di dispositivi di ascolto occulti installati dalla Polizia nei propri uffici o in luoghi privati, la Corte ha riscontrato la violazione dell'articolo 8 (ibid., §§ 38, 63).

51. L'intercettazione di conversazioni mediante l'utilizzo di dispositivi di ascolto, come l'intercettazione di telefonate, rappresenta una grave ingerenza nel diritto della persona interessata al rispetto della sua vita privata (*Vetter c. Francia*, 2005, § 26). Deve pertanto essere basata su una "legge" particolarmente precisa: anche in questo campo, l'esistenza di norme chiare e dettagliate sembra indispensabile, specialmente perché le pertinenti procedure tecniche sono in continuo perfezionamento (ibid., § 26). Secondo la Corte, la "legge" deve fornire ai cittadini "adeguate garanzie" contro il medesimo tipo di abuso che potrebbe essere temuto in caso di intercettazioni telefoniche (ibid., § 26). Pertanto, dovranno essere definiti, in particolare, le categorie di persone che possono essere soggette a tale misura e il tipo di reati che potrebbero giustificarla; il tribunale dovrà

fissare un termine per l'esecuzione di tale misura; sarà necessario stabilire anche le condizioni per redigere i verbali delle conversazioni intercettate, le precauzioni da adottare per comunicare le registrazioni in stato intatto e completo, per un evetuale riesame da parte di un giudice e della difesa, e le circostanze in cui i nastri devono essere cancellati o distrutti, in partricolare successivamente a una decisione di archiviazione o di assoluzione (ibid., § 26, che rinvia ai criteri in materia di prove costituite da intercettazioni esposti nella causa *Kruslin c. Francia*, 1990, § 35).

52. La registrazione della voce di una persona, senza il minimo livello di protezione richiesta dallo Stato di diritto in una società democratica, costituirà violazione dell'articolo 8 (*Wisse c. Francia*, 2005, § 34 relativa alla registrazione e al successivo utilizzo delle conversazioni svoltesi nella sala visite di un carcere; *Allan c. Regno Unito*, 2002, § 36, relativa all'installazione di un dispositivo di ascolto nella cella di un carcere).

v. Dati di localizzazione GPS

53. I dati raccolti mediante un dispositivo GPS costituiscono dei dati personali nella misura in cui essi possono indicare il luogo in cui si trova una persona e i suoi spostamenti pubblici (*Uzun c. Germania*, 2010, §§ 51-52; *Florindo de Almeida Vasconcelos Gramaxo c. Portogallo*, 2022, § 95). Il trattamento e l'uso di tali dati può essere considerato un'ingerenza nel diritto dell'interessato al rispetto della vita privata (http://hudoc.echr.coe.int/eng?i=001-100344*Uzun c. Germania*, 2010, §§ 51-52; *Florindo de Almeida Vasconcelos Gramaxo c. Portogallo*, 2022, § 96). La sorveglianza mediante GPS deve per la sua stessa natura essere distinta da altri metodi di sorveglianza visiva o acustica che possono, di regola, interferire maggiormente nel diritto di una persona al rispetto della vita privata, in quanto rivelano un maggior numero di informazioni sul comportamento, le opinioni o i sentimenti di una persona (http://hudoc.echr.coe.int/eng?i=001-100344*Uzun c. Germania*, 2010, § 52).

54. Poiché tale tipo di misura deve essere considerato una minore ingerenza nella vita privata della persona interessata rispetto all'intercettazione delle sue conversazioni telefoniche, i criteri relativamente rigidi previsti e applicati nello specifico ambito delle intercettazioni telefoniche non sono di per sé applicabili alla sorveglianza mediante GPS degli spostamenti di una persona (ibid., § 66). Per esaminare se, in un dato caso, a una persona sottoposta a una misura di geolocalizzazione mediante GPS sia stata offerta un'adeguata protezione da ingerenze arbitrarie nell'esercizio dei suoi diritti di cui all'articolo 8, la Corte applicherà principi più generali nell'esame della prevedibilità della legge (ibid., § 66 e i rinvii citati nel § 63). L'emissione di un mandato da parte di un organo indipendente non è sempre necessaria e il successivo riesame giudiziario della sorveglianza mediante GPS fornirà sufficiente protezione dalle arbitrarietà (ibid., § 72).

55. La Corte ha ritenuto che l'installazione di un dispositivo di geolocalizzazione nel veicolo di una persona nell'ambito di un'indagine penale relativa al traffico di sostanze stupefacenti avesse violato l'articolo 8 in una causa in cui il diritto interno (la legge scritta e la giurisprudenza) all'epoca dei fatti non indicava con sufficiente chiarezza le modalità, e la misura, in cui le autorità potevano usare il loro potere discrezionale in tale campo (*Ben Faiza c. Francia*, 2018, §§ 58-61).

56. Tuttavia, in un'altra causa in cui la Corte ha eaminato la questione della raccolta dei dati personali di una persona mediante la geolocalizzazione e l'utilizzo dei dati in un procedimento penale nei suoi confronti, essa non ha riscontrato alcuna violazione dell'articolo 8 (*Uzun c. Germania*, 2010, §§ 60-74). Il riesame giudiziario e la possibilità di escludere le prove ottenute per mezzo di una sorveglianza mediante GPS illegale costituivano un'importante garanzia, in quanto dissuadevano gli inquirenti dal raccogliere prove con mezzi illegali (ibid., § 72). Nell'esame della proporzionalità dell'ingerenza si è tenuto conto anche del fatto che il diritto interno subordinava l'autorizzazione alla contestata misura di sorveglianza a condizioni molto stringenti, che la sorveglianza mediante GPS fosse stata disposta soltanto dopo che altri mezzi di indagine meno invasivi si erano dimostrati inefficaci, e che essa fosse stata svolta per un periodo relativamente breve (ibid., §§ 77-81).

57. Nella causa *Florindo de Almeida Vasconcelos Gramaxo c. Portogallo*, 2022 (§§ 95-96 e 105-125) il datore di lavoro del ricorrente aveva installato un sistema GPS nell'automobile di servizio del ricorrente al fine di controllare le distanze percorse durante la sua attività professionale e, se del caso, i suoi spostamenti privati. La Corte ha osservato che tale sistema aveva permesso di controllare gli spostamenti del veicolo in tempo reale: era quindi possibile localizzare geograficamente le persone o persone che si supponeva lo utilizzassero in un dato momento o in modo continuo. Secondo la Corte, tali informazioni costituivano dei dati personali. Essa ha inoltre sottolineato che i dipendenti non erano stati autorizzati a disattivare il sistema GPS, cosicché esso rimaneva attivo ventiquattro ore su ventiquattro, sette giorni a settimana, con il risultato che la sorveglianza era permanente e sistematica, il che costituiva chiaramente un'ingerenza nel diritto del ricorrente alla vita privata. Al medesimo tempo, la Corte ha ritenuto che i tribunali nazionali avessero soppesato attentamente gli interessi concorrenti in gioco vale a dire, il diritto del ricorrente al rispetto della sua vita privata e il diritto del suo datore di lavoro di assicurare il regolare funzionamento della società, tenendo conto del fine legittimo perseguito dalla stessa, vale a dire il diritto di controllare le proprie spese. La Corte non ha pertanto riscontrato alcuna violazione dell'articolo 8 della Convenzione.

vi. Fotografie

58. Il diritto alla tutela della propria immagine è uno degli elementi essenziali dello sviluppo personale e presuppone il diritto di controllare l'uso di tale immagine (*Reklos e Davourlis c. Grecia*, 2009, §§ 40-43). Tranne qualora una persona si sia esposta scientemente o accidentalmente alla possibilità di essere fotografata nell'ambito di un'attività suscettibile di essere registrata o riferita pubblicamente, l'effettiva tutela della propria immagine presuppone, in linea di principio, l'ottenimento del consenso della persona interessata nel momento in cui è scattata la fotografia e non semplicemente se e quando essa è pubblicata (ibid., §§ 37, 40). Tale principio non è tuttavia assoluto. La qualità di personaggio pubblico o che merita di essere pubblicato, può giustificare, in determinate circostanze, per motivi di interesse generale, la registrazione dell'immagine di una persona a sua insaputa e la sua diffusione senza il suo consenso[2].

59. Nel caso di persone arrestate o accusate di un reato, l'obiettiva utilità del fotosegnalamento da parte delle autorità successivamente all'arresto di una persona sospettata della commissione di un reato può rendere la conservazione delle fotografie "necessaria in una società democratica" al fine della prevenzione dei reati (*Suprunenko c. Russia* (dec.), 2018, §§ 63-65). Il mero fatto che un indagato sia fotografato e una sua fotografia sia inserita in una banca dati non comporta necessariamente uno stigma di sospetto o di colpevolezza (ibid., § 64). Nella causa *Murray c. Regno Unito* [GC], 1994 (§§ 92-93), lo scatto e la conservazione, senza il suo consenso, di una fotografia di una persona sospettata di un reato di terrorismo non erano stati sproporzionati al fine perseguito di contrastare il terrorismo, fine legittimo in una società democratica. Il fatto che le autorità registrassero e conservassero i dati personali fondamentali riguardanti la persona arrestata, o anche altre persone presenti al momento e nel luogo dell'arresto, non poteva essere considerato non rientrante nei limiti legittimi della procedura di indagine in materia di reati di terrorismo (ibid., § 93). La Corte ha inoltre dichiarato manifestamente infondato un ricorso concernente la conservazione nel sistema informatico del Ministero dell'Interno della fotografia del ricorrente, scattata dalle autorità al momento dell'arresto da parte della Polizia perché era sospettato della commissione di un reato (*Suprunenko c. Russia* (dec.), 2018, § 65). Secondo la Corte, benché le informazioni raccolte e conservate in tal modo nel computer della Polizia fossero di natura personale, esse non potevano essere considerate intime o sensibili (ibid., § 64).

[2] Si veda altresì la Guida all'articolo 10 della Convenzione (libertà di espressione) sulla pubblicazione di fotografie a fini giornalistici.

60. La Corte ha tuttavia riscontrato la violazione dell'articolo 8 se la aolizia aveva consegnato alla stampa, senza il preliminare consenso delle persone interessate, le fotografie di persone arrestate o accusate (*Sciacca c. Italia*, 2005, §§ 29-31; *Khoujine e altri c. Russia*, 2008, §§ 115-118), o se aveva invitato squadre televisive a filmare illegalmente un ricorrente nel posto di polizia e a trasmettere la sequenza per televisione (*Toma c. Romania*, 2009, §§ 90-93; *Khmel c. Russia*, 2013, § 41), o in un caso in cui l'affissione della fotografia di un ricorrente su un tabellone di persone ricercate non era previsto dalla legge (*Guiorgui Nikolaïchvili c. Georgia*, 2009, §§ 129-131).

61. Secondo la Corte, la conservazione per un periodo illimitato della fotografia di una persona sospettata della commissione di un reato, che non era stata ritenuta colpevole, comportava un rischio di stigmatizzazione più elevato della conservazione di dati relativi a persone che erano state condannate per un reato (*S. e Marper c. Regno Unito* [GC], 2008, § 122; *Gaughran c. Regno Unito*, 2020, §§ 82-84). La durata del periodo di conservazione non è necessariamente determinante nel valutare se uno Stato abbia ecceduto il margine di discrezionalità accettabile nello stabilire il regime pertinente per la conservazione di dati personali, bensì lo sono piuttosto l'esistenza e il funzionamento di alcune garanzie (ibid., § 88).

62. Le tecniche di riconoscimento facciale e di cartografia facciale che possono essere applicate oggigiorno diventano sempre più complesse e i tribunali nazionali devono tenere conto di ciò nell'esame della necessità di un'ingerenza nel diritto al rispetto della vita privata di una persona che è stata fotografata dalle autorità (ibid., §§ 67-70).

63. Nella causa *Gaughran c. Regno Unito*, 2020 (§§ 97-98), nella quale le autorità aveva deciso che la fotografia così come il profilo del DNA e le impronte digitali di una persona condannata per guida in stato di ebbrezza, dovessero essere conservati a tempo indeterminato, la Corte ha riscontrato la violazione dell'articolo 8. Nel decidere tale conservazione dei dati personali, senza tenere conto della gravità del reato e in assenza di qualsiasi reale possibilità di riesame, le autorità non erano pervenute a un giusto equilibrio degli interessi pubblici e privati concorrenti. Benché allo Stato fosse offerto un margine di discrezionalità leggermente più ampio in ordine alla conservazione di fotografie che a quella di profili del DNA (ibid., §§ 84, 96), tale margine ampliato non era sufficiente perché la conservazione di tali dati fosse proporzionata in qualsiasi circostanza, in particolare in assenza di garanzie pertinenti o di qualsiasi reale possibilità di riesame (ibid., § 96).

64. Nella causa *P.N. c. Germania*, 2020 (§§ 76-91) la Corte non ha riscontrato alcuna violazione dell'articolo 8 in relazione a una raccolta disposta dalla Polizia, successivamente all'apertura di un nuovo procedimento penale nei confronti di un individuo che era stato precedentemente condannato, di informazioni che lo identificavano, quali fotografie del suo volto e del suo corpo, specialmente dei tatuaggi, unitamente alle sue impronte digitali e palmari. In considerazione della relativamente limitata invadenza e durata della raccolta dei dati identificativi in questione, del limitato impatto della conservazione dei dati sulla vita quotidiana del ricorrente, della distruzione dei dati dopo cinque anni, e del fatto che i dati erano memorizzati in una banca dati della Polizia soggetta a garanzie e a un riesame individualizzato, la misura contestata aveva costituito un'ingerenza proporzionata nel diritto del ricorrente al rispetto della sua vita privata.

65. In un contesto differente, nella causa *Reklos e Davourlis c. Grecia*, 2009 (§§ 41-43), la Corte ha ritenuto che vi fosse stata violazione dell'articolo 8 in quanto le fotografie scattate a un neonato in una clinica e la loro conservazione da parte del fotografo in una forma che permetteva l'identificazione, con la possibilità di un successivo utilizzo, avevano avuto luogo contro la volontà dei genitori. Analogamente è stata riscontrata violazione nelle cause *Hájovský c. Slovacchia*, 2021 (§§ 46-49), riguardo alla pubblicazione nella stampa di immagini non sfocate del ricorrente, scattate a sua insaputa con dei pretesti, e *Volodina c. Russia (n. 2)*, 2021, § 68, concernente la mancata protezione di una donna, da parte delle autorità, dalla ripetuta ciberviolenza del marito, il quale aveva creato falsi profili a suo nome e aveva pubblicato le sue fotografie intime.

66. Nella causa *Vučina c. Croazia* (dec.), 2019 (§§ 34-51), il mero fatto che un nome che non era quello della ricorrente, che non aveva alcuna connotazione negativa, fosse stato indicato per errore nella didascalia di una fotografia su una rivista femminile non poteva essere considerato un'ingerenza particolarmente sostanziale nel diritto dell'interessata al rispetto della sua vita privata.

67. Nella causa *Von Hannover c. Germania (n. 2)* [GC], 2012 (§§ 114-126), il rifiuto da parte dei tribunali nazionali di proibire la pubblicazione di una fotografia di una coppia famosa, scattata all'insaputa della stessa non aveva costituito violazione dell'articolo 8, dato che i tribunali nazionali avevano soppesato attentamente il diritto della società editrice alla libertà di espressione, da una parte, e il diritto dei ricorrenti al rispetto della loro vita privata, dall'altra. Nel farlo essi avevano attribuito una fondamentale importanza alla questione di sapere se le fotografie, considerate alla luce degli articoli che le accompagnavano, avessero contribuito a un dibattito di interesse generale. Avevano anche esaminato le circostanze in cui erano state scattate le fotografie.

68. Nella causa *Kahn c. Germania*, 2016 (§§ 63-76) la Corte non ha riscontrato alcuna violazione dell'articolo 8 in una causa in cui un editore non era stato condannato al pagamento di una somma per avere violato il divieto di pubblicare le fotografie dei due figli di un ex portiere della squadra nazionale di calcio tedesca. La Corte ha chiarito che non era possibile dedurre dall'articolo 8 della Convenzione un principio secondo il quale, al fine di proteggere la vita privata di una persona in modo effettivo, l'ordine che imponeva a un editore di pagare una somma per non avere osservato l'ingiunzione che vietava la pubblicazione sarebbe stato sufficiente soltanto se la somma in questione fosse andata alla vittima. Ciò era vero purché lo Stato, nell'esercizio del suo margine di discrezionalità, avesse offerto alle parti lese altri ricorsi potenzialmente effettivi dei quali non era possibile affermare che limitassero in modo sproporzionato le opportunità di ottenere una riparazione per le asserite violazioni (ibid., § 75).

B. I due aspetti (negativo e positivo) della protezione dei dati

69. Benché la finalità principale dell'articolo 8 della Convenzione sia la protezione delle persone da ingerenze arbitrarie da parte di autorità pubbliche, o di organismi privati cui lo Stato ha delegato le responsabilità, nel loro diritto al rispetto della loro vita privata e familiare, del loro domicilio e della loro corrispondenza, esso può imporre allo Stato anche alcuni obblighi positivi per assicurare l'effettivo rispetto di tali diritti (*Bărbulescu c. Romania* [GC], 2017, § 108).

70. Se una misura che costituisce un'ingerenza nella protezione dei dati personali è adottata da una persona fisica o giuridica puramente nel settore privato, la Corte esaminerà la causa sotto il profilo degli obblighi positivi dello Stato (*Craxi c. Italia (n. 2)*, 2003, §§ 68-76; *Köpke c. Germania* (dec.), 2010; *Alkaya c. Turchia*, 2012, § 32; *Söderman c. Svezia* [GC], 2013, § 89; *Bărbulescu c. Romania* [GC], 2017, § 111; *López Ribalda e altri c. Spagna* [GC], 2019, § 111; *Buturugă c. Romania*, 2020, §§ 60-63; *Volodina c. Russia (n. 2*), 2021, §§ 58-68; *Florindo de Almeida Vasconcelos Gramaxo c. Portogallo*, 2022, § 111). Tuttavia, se una misura è stata adottata da un'entità pubblica (*Copland c. Regno Unito*, 2007, § 39; *Libert c. Francia,* 2018, § 41; *Drelon c. Francia*, 2022, § 85) o da un organo privato cui lo Stato ha delegato i suoi obblighi (*Vukota-Bojić c. Svizzera*, 2016, § 47), la Corte esaminerà la causa sotto il profilo dell'obbligo negativo dello Stato. La Corte dovrà verificare che l'ingerenza soddisfacesse i requisiti dell'articolo 8 § 2, vale a dire che fosse prevista dalla legge, perseguisse un fine legittimo e fosse necessaria in una società democratica. Tale questione sarà esaminata più dettagliatamente nella parte della presente Guida *infra* relativa ai Tre "criteri" in materia di protezione dei dati.

71. Nella causa *Vukota-Bojić c. Svizzera*, 2016 (§ 47) la Corte ha sottolineato che uno Stato non poteva esimersi dalla responsabilità derivanti dalla Convenzione delegando i suoi obblighi a organismi privati o a persone fisiche. Dato che la compagnia di assicurazione privata che aveva raccolto e memorizzato i dati personali, applicava il regime di assicurazione statale e che il regime interno la considerava

un'autorità pubblica, la compagnia doveva essere considerata un'autorità pubblica e gli atti compiuti da essa erano ascrivibili allo Stato convenuto (ibid., § 47).

72. Nella causa *Libert c. Francia,* 2018 (§§ 37-41), la Corte ha rigettato l'eccezione del Governo secondo la quale la Società nazionale delle Ferrovie (SNCF), datrice di lavoro del ricorrente, accusata di avere aperto dei file personali contenuti in un computer di lavoro, non poteva essere considerata un'autorità pubblica ai fini dell'articolo 8. Anche se il suo personale aveva un rapporto di lavoro di diritto privato, la società era una persona giuridica di diritto pubblico, sottoposta al controllo dello Stato e i suoi dirigenti erano nominati dallo Stato, e beneficiava quindi di un'implicita garanzia da parte dello Stato.

73. In una causa concernente la sorveglianza delle telefonate, delle e-mail e della connessione Internet di una dipendente scolastica, la Corte ha ritenuto che la questione dovesse essere analizzata in relazione all'obbligo negativo dello Stato di non commettere ingerenze nella vita privata e nella corrispondenza della ricorrente, in quanto l'istituto scolastico era un ente pubblico dei cui atti il Governo era responsabile ai fini della Convenzione (*Copland c. Regno Unito*, 2007, § 39).

74. Nella causa *Liebscher c. Austria*, 2021, il ricorrente ha lamentato l'obbligo di presentare l'intero accordo di divorzio (invece di un estratto di esso) al fine di ottenere il trasferimento della sua quota del patrimonio immobiliare alla sua ex moglie. Le informazioni contenute nell'accordo di divorzio comprendevano i nomi e i luoghi di residenza dei suoi figli minori e della sua ex moglie, l'importo dell'assegno alimentare che versava e gli accordi in materia di custodia, gli accordi relativi alla divisione dei beni (diversi dal patrimonio immobiliare) e un elenco dei redditi e dei beni del ricorrente. Il trasferimento dei beni, e quindi tutta la documentazione afferente, compreso l'accordo di divorzio, sarebbero stati registrati in un registro fondiario accessibile al pubblico e che poteva quindi essere consultato da terzi senza limitazioni. La Corte ha affrontato la causa dal punto di vista dell'obbligo positivo dello Stato di adottare misure finalizzate ad assicurare il rispetto della vita privata, tra cui sia la previsione di un quadro regolamentare che l'attuazione, se del caso, di misure specifiche (ibid., §§ 60-61).

75. Benché i confini tra gli obblighi positivi e quelìi negativi dello Stato ai sensi della Convenzione non si prestino a una definizione precisa, i principi applicabii sono tuttavia simili. In entrambi i contesti era necessario tenere conto in particolare del giusto equilibrio che doveva essere conseguito tra gli interessi concorrenti della persona e della comunità nel suo insieme, fatto salvo in ogni caso il margine di discrezionalità goduto dallo Stato (*Bărbulescu c. Romania* [GC], 2017, § 112).

76. Nei casi che sollevano la questione della protezione dei dati personali, la Corte ha ritenuto che il margine di discrezionalità dello Stato sia più ampio: se non vi è unanimità negli Stati membri del Consiglio d'Europa riguardo all'importanza dell'interesse in gioco, o sui migliori mezzi per tutelarlo (*Odièvre c. Francia* [GC], 2003, § 47; *Breyer c. Germania*, 2020, § 108); se i dati puramente finanziari in gioco non erano strettamente connessi all'identità del ricorrente (*G.S.B. c. Svizzera*, 2015, § 93); e, infine, in materia di sicurezza nazionale (*Leander c. Svezia*, 1987, § 59). Per contro, il margine di discrezionalità offerto alle autorità nazionali è stato ritenuto più esiguo se, per esempio, i dati personali soggetti a un trattamento automatizzato, che ne facilitava considerevolmente l'accesso e la diffusione, potevano nuocere alla reputazione di una persona e rendere più difficile la sua vita quotidiana (*Khelili c. Svizzera*, 2011, §§ 64, 70). La medesima considerazione è valida specialmente per la protezione di categorie di dati sensibili, in particolare informazioni relative al DNA, che contengono il patrimonio genetico e hanno notevole importanza sia per la persona interessata che per la sua famiglia (*S. e Marper c. Regno Unito* [GC], 2008, §§ 102-103).

77. Gli obblighi positivi inerenti di assicurare l'effettiva protezione dei diritti e delle libertà previsti dalla Convenzione possono riguardare, per esempio, l'obbligo di assicurare a una persona: l'accesso entro un termine ragionevole a informazioni memorizzate sistematicamente riguardo alla persona da parte dei vecchi Servizi segreti statali in relazione al suo remoto passato (*Haralambie c. Romania*, 2009, § 79; *Jarnea c. Romania*, 2011, § 50; *Joanna Szulc c. Polonia*, 2012, § 87); una "procedura

effettiva e accessibile" che permetta alla parte interessata di accedere a "qualsiasi informazione pertinente e appropriata", raccolta e memorizzata dalle autorità pubbliche al fine di ricevere le informazioni necessarie per conoscere e comprendere l'infanzia e l'iniziale sviluppo della persona (*Gaskin c. Regno Unito*, 1989, § 49), per scoprire la sua identità personale (*Odièvre c. Francia* [GC], 2003, § 42), o per individuare gli eventuali rischi per la salute cui era stata esposta (*Guerra e altri c. Italia,* 1998, § 60; *McGinley ed Egan c. Regno Unito*, 1998, § 101; *Roche c. Regno Unito* [GC], 2005, § 162).

78. La Corte ha tuttavia ritenuto che tali obblighi positivi non spettino alle autorità nazionali nel contesto di informazioni sensibili per la sicurezza nazionale, raccolte dalle autorità riguardo a una persona (*Leander c. Svezia*, 1987, § 51).

79. Pertanto nella causa *Kotilainen e altri c. Finlandia*, 2020 (§ 83), concernente l'uccisione di alunni a colpi di arma da fuoco in un istituto scolastico, la Corte ha ritenuto che l'obbligo positivo spettante alle autorità di proteggere le vite dei congiunti dei ricorrenti non si estendesse, ai sensi dell'aspetto sostanziale dell'articolo 2, a un obbligo per la Polizia di ottenere, prima delle uccisioni, le cartelle cliniche e militari dell'autore del reato, al fine di verificarne la salute mentale. L'accesso da parte della Polizia ai dati sanitari di una persona non può essere una questione di routine e deve rimanere soggetto a specifici requisiti di necessità e di giustificazione.

80. In alcune circostanze in cui sorge la questione dei dati personali, per esempio nel contesto di atti particolarmente gravi tra persone, l'effettivo godimento dei diritti previsti dalla Convenzione esige che lo Stato promulghi una legislazione specifica per proteggere tali diritti. Pertanto nella causa *Söderman c. Svezia* [GC], 2013 (§§ 86-117), la Corte ha riscontrato la violazione dell'articolo 8 in considerazione dell'assenza di chiare disposizioni legislative, che aveva comportato che l'atto isolato di filmare o fotografare una minore nuda, a sua insaputa, o senza il suo consenso, era rimasto impunito, lacuna della legge che non era stata compensata all'epoca da altre disposizioni penali, tenuto conto anche dell'inefficacia dei mezzi di ricorso civili (ibid., §§ 108-114). Analogamente, nella causa *K.U. c. Finlandia*, 2008 (§§ 49-50), è stata riscontrata la violazione dell'articolo 8 a causa dell'assenza di una base giuridica che consentisse alle autorità di obbligare un fornitore di accesso a internet a rivelare l'identità di una persona ricercata per avere pubblicato un messaggio indecente relativo a un minore su un sito di incontri. Il legislatore deve prevedere un quadro per conciliare i vari interessi concorrenti al fine di fornire una protezione in tale contesto. La causa *Khadija Ismayilova c. Azerbaigian*, 2019 (§§ 105-132) concerneva la registrazione segreta di una giornalista nella sua abitazione e la divulgazione pubblica dei video. In tale caso gli atti erano punibili ai sensi del diritto penale ed era stata aperta un'indagine penale. La Corte ha tuttavia ritenuto che le autorità non avessero adempiuto il loro obbligo positivo di assicurare una sufficiente protezione della vita privata della ricorrente, svolgendo un'indagine penale effettiva sulle gravi ingerenze nella sua vita privata (ibid., §§ 119-131). La causa *Volodina c. Russia (n. 2*), 2021, § 68, concerneva la doglianza della ricorrente secondo la quale le autorità non l'avevano protetta dalla ripetuta ciberviolenza del marito, il quale aveva creato profili falsi a suo nome, aveva pubblicato le sue fotografie intime, aveva seguito i suoi movimenti, e le aveva inviato minacce di morte mediante i social media. La Corte ha ritenuto, in particolare, che pur disponendo di strumenti giuridici per perseguire il marito della ricorrente, le autorità non avessero condotto un'indagine effettiva e non avessero mai previsto di adottare misure adeguate al fine di proteggerla. Esse non avevano quindi osservato il loro dovere di proteggerla da gravi abusi.

81. Per quanto riguarda atti meno gravi tra persone, come il controllo dei dipendenti nel luogo di lavoro, gli Stati possono scegliere se adottare o meno una legislazione specifica in materia di video-sorveglianza (*López Ribalda e altri c. Spagna* [GC], 2019, § 113; *Köpke c. Germania* (dec.), 2010) o di controllo della corrispondenza e delle comunicazioni non professionali dei dipendenti (*Bărbulescu c. Romania* [GC], 2017, § 119). Spetta tuttavia ai tribunali nazionali assicurare che l'attuazione da parte di un datore di lavoro di misure di sorveglianza, che interferiscono nel diritto dei dipendenti al rispetto della loro vita privata o della loro corrispondenza, sia proporzionata e accompagnata da garanzie

appropriate e adeguate contro gli abusi (*Köpke c. Germania* (dec.), 2010; *Bărbulescu c. Romania* [GC], 2017, § 120; *López Ribalda e altri c. Spagna* [GC], 2019, § 116).

82. In altre cause relative alla divulgazione di dati personali, la Corte ha ritenuto che lo Stato avesse l'obbligo positivo di indagare sulle asserite violazioni dell'articolo 8, sia se esse erano state commesse da privati che da autorità pubbliche. Pertanto, nella causa *Craxi c. Italia (n. 2)*, 2003 (§§ 68-76), concernene la lettura in udienza e la divulgazione da parte della stampa delle trascrizioni delle conversazioni telefoniche di un politico, intercettate nell'ambito di un procedimento penale per corruzione, la Corte ha ritenuto che le autorità avessero l'obbligo positivo di impedire che delle conversazioni private diventassero di dominio pubblico. Poiché la divulgazione delle conversazioni a mezzo stampa non era una diretta conseguenza di un atto compiuto dal pubblico ministero, ma era stata probabilmente causata dal malfunzionamento della cancelleria del tribunale nazionale, la Corte ha riscontrato la violazione dell'articolo 8, in quanto le autorità non avevano adottato le misure necessarie per assicurare l'effettiva protezione del diritto del ricorrente, prevedendo appropriate garanzie e svolgendo un'indagine effettiva.

83. Nella causa *Alkaya c. Turchia*, 2012 (§§ 30-40), la Corte ha concluso che la protezione offerta dalle autorità nazionali alle informazioni personali di una famosa attrice, della quale un giornale aveva rivelato l'indirizzo completo, fosse stata insufficiente. Non avendo riscontrato alcuna prova che sembrasse in grado di giustificare, per motivi di interesse generale, la decisione del giornale di divulgare il suo indirizzo, la Corte ha osservato che non sembrava che i tribunali nazionali avessero tenuto conto delle possibili ripercussioni sulla vita della ricorrente della pubblicazione del suo indirizzo personale su un giornale. Tale mancata valutazione da parte dei tribunali nazionali degli interessi concorrenti non poteva essere considerata conforme aglu obblighi positivi dello Stato di cui all'articolo 8.

84. Nel contesto della violenza domestica, la Corte ha ritenuto, nella causa *Buturugă c. Romania*, 2020 (§§ 73-78), in cui l'ex marito della ricorrente aveva consultato abusivamente i suoi account elettronici, compreso Facebook, e aveva copiato le sue conversazioni private, i suoi documenti e le sue fotografie, che le autorità avessero l'obbligo di indagare sulla violazione della riservatezza della corrispondenza della ricorrente. La Corte, riconoscendo che il ciberbullismo era stato considerato un aspetto della violenza nei confronti delle donne e delle ragazze, e che esso poteva assumere varie forme, compresa la ciberviolazione della vita privata, violando il computer della vittima e sottraendo, condividendo e manipolando dati e immagini, compresi particolari intimi, ha accettato che le autorità nazionali potevano tenere conto di atti quali controllare, accedere e salvare impropriamente la corrispondenza del coniuge, quando esse indagavano su casi di violenza domestica. Le accuse di violazione della riservatezza della propria corrispondenza esigevano che le autorità svolgessero un esame del merito al fine di acquisire una comprensione esauriente del fenomeno relativo a tutte le possibili forme di violenza domestica (ibid., §§ 76-77). Poiché tale esame non aveva avuto luogo, vi era stata violazione dell'articolo 8.

C. I tre "criteri" in materia di protezione dei dati

85. Il paragrafo 2 dell'articolo 8 indica le condizioni alle quali vi può essere un'ingerenza nel godimento del diritto protetto; tale ingerenza deve essere "prevista dalla legge", deve perseguire un "fine legittimo" e deve essere "necessaria in una società democratica".

1. La questione della legalità dell'ingerenza

86. La Corte ha esaminato in diverse cause la questione di sapere se il requisito, sancito dall'articolo 5 della Convenzione n. 108, secondo il quale i dati personali soggetti a trattamento automatizzato devono essere stati ottenuti o elaborati lealmente e legalmente, sia o non sia stato soddisfatto. In diverse cause la Corte ha riscontrato la violazione dell'articolo 8 soltanto a causa dell'assenza di una

base giuridica a livello nazionale per autorizzare misure in grado di interferire nei diritti pertinenti (*Taylor-Sabori c. Regno Unito*, 2002, §§ 17-19; *Radu c. Moldavia*, 2014, § 31; *Mockutė c. Lituania*, 2018, §§ 103-104; *M.D. e altri c. Spagna*, 2022, §§ 61-64).

87. In particolare, nella causa *Mockutė c. Lituania*, 2018 (§§ 103-104), la Corte ha osservato che né il Governo né i tribunali nazionali avevano indicato alcuna disposizione che avrebbe potuto costituire la base giuridica della comunicazione, da parte dell'ospedale psichiatrico, di informazioni sulla salute della ricorrente, che era maggiorenne, a sua madre e ai giornalisti. Nella causa *Taylor-Sabori c. Regno Unito*, 2002 (§§ 17-19), in cui il ricorrente era stato sottoposto a sorveglianza di polizia mediante la "clonazione" del suo cercapersone, non esisteva alcun sistema regolamentare per disciplinare l'intercettazione di messaggi del cercapersone trasmessi mediante un sistema di telecomunicazioni privato. Nella causa *Radu c. Repubblica di Moldavia*, 2014 (§ 31), la diffusione da parte di un ospedale pubblico di informazioni mediche sulla gravidanza, lo stato di salute della ricorrente e il trattamento da parte del suo datore di lavoro non era stata "prevista dalla legge". Nella causa *M.D. e altri c. Spagna*, 2022 (§§ 61-64), la Polizia aveva redatto un rapporto relativo a giudici e magistrati, che esercitavano le loro funzioni in Catalogna e che avevano firmato un manifesto nel quale avevano esposto il loro parere giuridico a favore alla possibilità che il popolo catalano esercitasse un cosiddetto "diritto di decidere", il rapporto rivelava dati personali, fotografie, informazioni professionali e opinioni politiche di alcuni di essi. La Corte ha osservato che la redazione del rapporto da parte della Polizia non era prevista dalla legge, e poiché le autorità pubbliche avevano utilizzato i dati personali per un fine diverso da quello che giustificava la raccolta, la mera esistenza del rapporto di Polizia, che era stato redatto in relazione a persone il cui comportamento non aveva implicato alcuna attività criminale, aveva costituito violazione dell'articolo 8 della Convenzione.

88. In altre cause la Corte ha riscontrato la violazione dell'articolo 8 in quanto il diritto interno, che avrebbe dovuto proteggere i dati personali, era inaccessibile o riservato (*Vasil Vasilev c. Bulgaria*, 2021, §§ 169-170; *Nuh Uzun e altri c. Turchia*, 2022, §§ 80-99) o non era sufficientemente chiaro e prevedibile (*Vukota-Bojić c. Svizzera*, 2016; *Ben Faiza c. Francia*, 2018, §§ 58-61; *Benedik c. Slovenia*, 2018*; Rotaru c. Romania* [GC], 2000; *Zoltán Varga c. Slovacchia*, 2021, § 162; *Haščák c. Slovacchia,* 2022, §§ 94-95). Pertanto, nella causa *Nuh Uzun e altri c. Turchia*, 2022, §§ 80-99, la corrispondenza dei detenuti era stata scannerizzata e caricata nel Server della rete giudiziaria nazionale sulla base di istruzioni impartite dal Ministero della Giustizia, indirizzate direttamente e specificamente ai pubblici ministeri e alle autorità carcerarie, che non erano state rese accessibili al pubblico in generale o ai ricorrenti in particolare. Nella causa *Vukota-Bojić c. Svizzera*, 2016, §§ 71-77, le disposizioni che costituivano la base della sorveglianza segreta cui era stata sottoposta la ricorrente dalla sua compagnia assicuratrice successivamente a un incidente stradale, non avevano indicato con sufficiente chiarezza la portata e le modalità di esercizio della discrezionalità conferita alle compagnie assicuratrici che agivano in qualità di autorità pubbliche nelle controversie assicurative, per condurre la sorveglianza segreta delle persone assicurate. Nella causa *Rotaru c. Romania* [GC], 2000 (§§ 57-62), concernente informazioni personali detenute dai Servizi segreti romeni, il diritto nazionale non definiva il tipo di informazioni che potevano essere trattate, le categorie di persone nei cui confronti potevano essere adottate misure di sorveglianza e in quali circostanze, o la procedura che doveva essere seguita. Nella causa *Benedik c. Slovenia*, 2018 (§ 132), alcune disposizioni giuridiche utilizzate dalla Polizia per ottenere i dati relativi a un abbonato associato a un indirizzo IP dinamico non erano chiare e non fornivano alcuna protezione dalle ingerenze arbitrarie, in quanto non esisteva alcuna garanzia contro gli abusi o alcun controllo indipendente dei poteri della Polizia in questione.

89. Per contro, in altre causa la Corte non ha riscontrato alcuna violazione dell'articolo 8, dopo avere concluso che il diritto interno fosse chiaro e prevedibile e offrisse sufficienti garanzie contro potenziali abusi (*Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia* [GC], 2017, § 154; *Ben Faiza c. Francia*, 2018, § 75). Nella causa *Ben Faiza c. Francia*, 2018 (§§ 70-76), un decreto giudiziario utilizzato per ottenere, da un fornitore di servizi di telefonia mobile, informazioni personali sul ricorrente che non concernevano il contenuto delle telefonate, era stato "previsto dalla legge". Tali

decreti giudiziari erano autorizzati e disciplinati dal pertinente quadro regolamentare e vi erano anche garanzie contro le arbitrarietà, in quanto tali decreti dovevano essere autorizzati anticipatamente da un pubblico ministero sotto pena di nullità, ed erano soggetti a riesame giudiziario, inoltre le informazioni ottenute potevano essere escluse dalle prove in caso di illegalità (ibid., § 73).

90. La Corte è pervenuta a una conclusione simile nella causa *Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia* [GC], 2017 (§ 154), concernente una decisione da parte della Commissione per la protezione dei dati, approvata dai tribunali, che proibiva la pubblicazione su vasta scala di dati fiscali. La formulazione della pertinente legislazione in materia di protezione dei dati e il modo in cui era stata applicata a seguito delle direttive impartite ai tribunali finlandesi dalla Corte di giustizia dell'Unione europea (CGUE), erano state sufficientemente prevedibili. Benché la causa fosse la prima di questo tipo ai sensi della Legge sui dati personali e il Tribunale amministrativo supremo avesse chiesto alla CGUE delle direttive sull'interpretazione della deroga prevista dalla Direttiva sulla protezione dei dati, ciò non aveva reso l'interpretazione e l'applicazione da parte dei tribunali interni della deroga giornalistica arbitraria o imprevedibile (ibid., § 150). Poiché le società ricorrenti Since erano delle imprese di media, esse avrebbero dovuto in quanto tali, essere consapevoli della possibilità che la raccolta massiva dei dati e la loro divulgazione su vasta scala avrebbero potuto non essere considerate "soltanto" un trattamento a fini giornalistici ai sensi delle pertinenti disposizioni del diritto finlandese e del diritto dell'Unione europea (ibid., § 151).

91. Infine, in altre cause la Corte ha ritenuto che il requisito che prevedeva che l'ingerenza fosse "prevista dalla legge" fosse connesso in modo talmente stretto al criterio secondo il quale essa dovesse essere "necessaria in una società democratica" che le due condizioni dovevano essere discusse insieme (*S. e Marper c. Regno Unito* [GC], 2008, § 99; *Kvasnica c. Slovacchia*, 2009, § 84; *Kennedy c. Regno Unito*, 2010, § 155).

92. Nello specifico contesto di misure di sorveglianza segreta, come l'intercettazione delle comunicazioni, la Corte ha ritenuto che la "prevedibilità" non possa essere intesa nel medesimo modo in cui lo è in molti altri campi. A suo avviso, essa non può significare che una persona debba essere in grado di prevedere quando è probabile che le autorità ricorrano a tali misure, in modo da potere adeguare conseguentemente il proprio comportamento (*Adomaitis c. Lituania*, 2022, § 83). Tuttavia, specialmente quando un potere conferito all'esecutivo è esercitato in segreto, i rischi di arbitrarietà sono evidenti. È pertanto essenziale che vi siano regole chiare e dettagliate sulle misure di sorveglianza segreta, specialmente perché la tecnologia utilizzabile diventa continuamente sempre più sofisticata. Il diritto interno deve essere sufficientemente chiaro al fine di fornire ai cittadini un'adeguata indicazione delle circostanze in cui, e delle condizioni alle quali, le autorità pubbliche sono autorizzate a ricorrere a simili misure (*Malone c. Regno Unito,* 1984, § 67; *Leander c. Svezia*, 1987, § 51; *Valenzuela Contreras c. Spagna,* 1998, § 46; *Weber e Saravia c. Germania* (dec.), 2006, § 93; *Association for European Integration and Human Rights ed Ekimdjiev c. Bulgaria*, 2007, § 75; *Roman Zakharov c. Russia* [GC], 2015, § 229). Inoltre, la legge deve indicare con sufficiente chiarezza la portata di una simile discrezionalità conferita alle autorità competenti e le modalità per esercitarla, al fine di offrire alle persone un'adeguata protezione dalle ingerenze arbitrarie (*Roman Zakharov c. Russia* [GC], 2015, § 230).

93. Nella sua giurisprudenza in materia di intercettazione delle comunicazioni nell'ambito di indagini penali la Corte ha determinato che, per impedire l'abuso di potere, la legge debba indicare almeno i seguenti sei elementi: la natura dei reati che possono dare luogo a un decreto di intercettazione; la definizione delle categorie di persone le cui comunicazioni possono essere intercettate; il termine per l'attuazione della misura; la procedura da seguire per l'esame, l'utilizzo e la memorizzazione dei dati raccolti; le precauzioni da adottare per la trasmissione dei dati ad altre parti; e le circostanze in cui i dati intercettati possono o devono essere cancellati o distrutti (*Huvig c. Francia*, 1990, § 34; *Valenzuela Contreras c. Spagna,* 1998, § 46; *Weber e Saravia c. Germania* (dec.), 2006, § 95; *Association for European Integration and Human Rights and Ekimdjiev c. Bulgaria*, 2007, § 76). Nella causa *Roman Zakharov c. Russia* [GC], 2015 (§ 238), ha confermato che tali medesime garanzie minime

si applicavano anche nei casi in cui l'intercettazione era stata eseguita per motivi di sicurezza nazionale; tuttavia, al fine di determinare se la legislazione contestata fosse incompatibile con l'articolo 8, la Corte ha tenuto conto anche dei seguenti fattori: le soluzioni previste per controllare l'esecuzione di misure di sorveglianza segreta, i meccanismi di notifica e i ricorsi previsti dal diritto nazionale[3].

94. Nel contesto della raccolta di dati personali da parte delle autorità e della loro memorizzazione in banche dati per fini connessi alla prevenzione o alla repressione di reati, la Corte ha dichiarato che è essenziale che esistano regole chiare e dettagliate che disciplinino la portata e l'applicazione di tali misure, unitamente a garanzie minime concernenti, *inter alia*, la durata, la memorizzazione, l'utilizzo, l'accesso di terzi, le procedure per preservare l'integrità e la riservatezza dei dati e le procedure per la loro distruzione, che forniscano quindi sufficienti granzie contro il rischio di abusi e di arbitrarietà (*S. e Marper c. Regno Unito* [GC], 2008, §§ 99, 103; *Nuh Uzun e altri c. Turchia*, 2022, § 86). La Corte ha riscontrato la violazione dell'articolo 8 in cause in cui il diritto interno non indicava con sufficiente chiarezza la portata e le modalità di esercizio della discrezionalità conferita alle autorità interne (*Shimovolos c. Russia*, 2011, § 70 ; *Dimitrov-Kazakov c. Bulgaria*, 2011, § 33). Nella causa *Shimovolos c. Russia*, 2011 (§ 69), la creazione e il mantenimento di una banca dati di sorveglianza che memorizza i dati personali, compresi quelli relativi agli spostamenti di un attivista in materia di diritti umani, e le procedure relative al suo funzionamento, erano disciplinati da un decreto ministeriale che non era mai stato pubblicato o reso accessibile al pubblico in altro modo. Nella causa *Dimitrov-Kazakov c. Bulgaria*, 2011 (§ 33), la registrazione di un individuo quale "delinquente" nei registri della Polizia era basata su un'istruzione non pubblica all'epoca dei fatti che era di carattere confidenziale ed era riservata, fino alla sua successiva desecretazione, a uso interno da parte del Ministero dell'Interno.

95. Nella causa *Catt c. Regno Unito*, 2019 (§§ 97, 106), la Corte ha sottolineato il rischio di ambiguità nella base giuridica utilizzata dalle autorità per la raccolta e la conservazione di dati personali, derivante da nozioni definite vagamente nel diritto interno.

2. La questione della legittimità del fine dell'ingerenza

96. In diverse cause la Corte ha esaminato la questione di sapere se il requisito, dichiarato nell'articolo 5 della Convenzione n. 108, che i dati personali sottoposti a trattamento automatizzato debbano essere stati raccolti per fini espliciti, determinati e legittimi, sia stato soddisfatto o meno. In tali cause, l'esame dei fini legittimi che possono giustificare un'ingerenza nell'esercizio dei diritti di cui all'articolo 8, elencati nel paragrafo 2, è alquanto succinta. Tali fini sono la protezione della sicurezza nazionale, la pubblica sicurezza e il benessere economico del Paese, la difesa dell'ordine e la prevenzione dei reati, la protezione della salute o della morale, o la protezione dei diritti o delle libertà altrui. La Corte conferma generalmente l'esistenza di uno o più di tali fini legittimi invocati dal Governo.

97. La Corte ha ritenuto, per esempio, che la memorizzazione in un registro segreto di Polizia di dati relativi alla vita privata delle persone, e il successivo utilizzo di tali dati nella verifica di candidati a posti importanti per la sicurezza nazionale, perseguissero un fine legittimo ai fini dell'articolo 8, vale a dire la protezione della sicurezza nazionale (*Leander c. Svezia*, 1987, § 49). La sorveglianza di un ricorrente mediante GPS, disposta da un pubblico ministero per un'indagine relativa a diversi atti di tentato omicidio dei quali un movimento terroristico aveva rivendicato la responsabilità, e al fine prevenire ulteriori attentati dinamitardi, aveva secondo la Corte tutelato gli interessi della sicurezza nazionale e della pubblica sicurezza, la prevenzione dei reati e la protezione dei diritti delle vittime (*Uzun c. Germania,* 2010, § 77).

[3] Si veda altresì la Guida all'articolo 8 della Convenzione (diritto al rispetto della vita privata e familiare) sul requisito della prevedibilità della legge in materia di intercettazione delle comunicazioni, intercettazioni telefoniche e sorveglianza segreta.

98. La Corte ha inoltre ritenuto che la trasmissione di dati bancari alle autorità di un altro Stato, ai sensi di un accordo bilaterale, perseguisse un fine legittimo, in quanto la misura serviva a proteggere il benessere economico del Paese (*G.S.B. c. Svizzera*, 2015, § 83). Dato che il settore bancario era un ramo economico di notevole importanza per lo Stato convenuto, la misura contestata, che faceva parte di un energico sforzo del Governo svizzero di dirimere il conflitto tra una banca (descritta come "un importante protagonista dell'economia svizzera che dava lavoro a un elevato numero di persone") e le autorità fiscali statunitensi, essa poteva essere considerata validamente un contributo alla protezione del benessere economico del Paese (ibid., § 83).

99. Rinviando a strumenti internazionali in base ai quali l'equità e la parità delle opportunità erano fondamentali nella lotta contro il doping, la Corte ha ritenuto che la protezione della salute e della morale giustificasse l'obbligo di accertare il luogo in cui si trovavano degli atleti, data la necessità di contrastare il doping nello sport (*National Federation of Sportspersons' Associations and Unions (FNASS) e altri c. Francia*, 2018, §§ 164-166). Secondo la Corte, ciò che il Governo aveva descritto come "morale", nell'ambito degli sforzi compiuti per assicurare una pari e significativa competizione negli sports, era connesso anche al fine legittimo della "protezione dei diritti e delle libertà altrui", poiché l'uso di agenti dopanti al fine di conseguire un vantaggio su altri atleti era una pericolosa incitazione agli atleti dilettanti, e in particolare ai giovani, a seguire l'esempio al fine di migliorare la loro prestazione, e privava gli spettatori della leale competizione che essi avevano il diritto di attendersi (ibid., § 166).

100. Nella causa *Ben Faiza c. Francia*, 2018 (§ 77), la Corte ha ritenuto che un decreto giudiziario utilizzato per ottenere, da un fornitore di servizi di telefonia mobile, informazioni personali sul ricorrente, che non concernevano il contenuto delle telefonate, mirasse ad accertare la verità nell'ambito di un procedimento penale relativo all'importazione di sostanze stupefacenti in una banda criminale organizzata, a un'associazione a delinquere e al riciclaggio. La misura aveva quindi perseguito i fini legittimi di difesa dell'ordine, di prevenzione dei reati e di protezione della salute pubblica.

101. L'intercettazione delle conversazioni telefoniche del ricorrente – che era direttore di un carcere, sospettato di corruzione – la memorizzazione di tali informazioni e la loro divulgazione nel corso del procedimento disciplinare, che avevano infine dato luogo al suo licenziamento, sono state considerate finalizzate a impedire atti di corruzione e a garantire la trasparenza e l'apertura del servizio pubblico, e avevano quindi perseguito i fini legittimi della difesa dell'ordine e della prevenzione dei reati, e della protezione dei diritti e delle libertà altrui nella causa *Adomaitis c. Lituania*, 2022 (§ 84).

102. Nella causa *López Ribalda e altri c. Spagna* [GC], 2019 (§§ 118, 123), l'interesse legittimo del datore di lavoro ad adottare misure finalizzate a scoprire e punire la persona, o le persone, responsabili di sospetti furti, al fine di assicurare la protezione dei beni della società e il suo regolare funzionamento, potevano giustificare misure che comportavano la video-sorveglianza dei dipendenti nel luogo di lavoro.

3. La questione della "necessità dell'ingerenza in una società democratica"

103. Per essere necessaria in una società democratica, una misura che interferisce nella protezione dei dati personali di cui all'articolo 8 deve soddisfare una "impellente esigenza sociale" e non deve essere sproporzionata al fine legittimo perseguito (*Z c. Finlandia*, 1997, § 94; *Khelili c. Svizzera*, 2011, § 62; *Vicent Del Campo c. Spagna*, 2018, § 46). I motivi invocati dal Governo devono essere pertinenti e sufficienti (*Z c. Finlandia*, 1997, § 94). Mentre spetta alle autorità nazionali compiere l'iniziale valutazione sotto tutti questi aspetti, la valutazione finale della necessità dell'ingerenza rimane soggetta al riesame della Corte per la conformità ai requisiti della Convenzione (*S. e Marper c. Regno Unito* [GC], 2008, § 101).

104. Nel contesto di atti particolarmente gravi tra persone in grado di interferire nei diritti di cui all'articolo 8, il riesame della Corte volto a stabilire se essi soddisfacessero il requisito della "necessità

in una società democratica" concerne il modo in cui lo Stato ha promulgato una specifica legislazione al fine di assicurare una sufficiente protezione di tali diritti (*K.U. c. Finlandia*, 2008, §§ 43-50; *Söderman c. Svezia* [GC], 2013, §§ 80-83). Quanto ad atti meno gravi tra persone, come la video-sorveglianza dei dipendenti nel luogo di lavoro, il riesame della Corte finalizzato a stabilire se la misura fosse "necessaria in una società democratica" concernerà le modalità con cui i tribunali nazionali hanno tenuto conto dei criteri stabiliti dalla Corte nella sua giurisprudenza, e che dimostrano quindi se siano stati soppesati gli interessi concorrenti (*López Ribalda e altri c. Spagna* [GC], 2019, §§ 116-117, § 122). Nel riesame di tali criteri, se uno di essi è assente le garanzie derivanti saranno ancora più importanti e possono compensare sufficientemente tale difetto (ibid., § 131).

105. Generalmente parlando, al fine di accertare se una misura che interferisce nella protezione nei dati personali di cui all'articolo 8 soddisfi la condizione della "necessità in una società democratica", la Corte ha esaminato se essa abbia osservato i requisiti elencati nell'articolo 5 della Convenzione n. 108, vale a dire e in particolare, il requisito di minimizzare la quantità dei dati raccolti, di assicurarne l'accuratezza, l'adeguatezza, la pertinenza e la non eccessività in relazione ai fini per i quali essi sono trattati, di limitare la durata della loro memorizzazione, di utilizzarli per i fini per i quali tali dati sono stati raccolti e di garantire la trasparenza nel loro trattamento.

a. Il requisito di minimizzare la quantità dei dati raccolti o registrati

106. In diverse cause la Corte ha esaminato la questione di sapere se i dati personali sottoposti a trattamento automatizzato fossero stati adeguati, pertinenti e non eccessivi in relazione ai fini per i quali erano stati registrati (*L.L. c. Francia*, 2006, §§ 45-46; *Vicent Del Campo c. Spagna*, 2018, § 51; *Khadija Ismayilova c. Azerbaigian*, 2019, § 147; *Kruglov e altri c. Russia*, 2020, § 132 *in fine*).

107. La Corte ha riscontrato la violazione dell'articolo 8: dopo avere osservato che, per quanto riguarda i dati conservati sui dispositivi elettronici dei ricorrenti che erano stati sequestrati, non sembrava che durante le perquisizioni fosse stato seguito alcun tipo di procedura di setacciatura per contenere al minimo la quantità di tali dati (*Kruglov e altri c. Russia*, 2020, § 132 *in fine*); per quanto riguarda una decisione giudiziaria che identificava il ricorrente, che non era parte del procedimento, quale autore di atti di molestie nel luogo di lavoro, mentre il giudice avrebbe potuto astenersi dal nominarlo, o avrebbe potuto riferirsi a lui semplicemente mediante le iniziali, al fine di evitare la stigmatizzazione (*Vicent Del Campo c. Spagna*, 2018, § 51); in un caso in cui i dati personali di una giornalista, che era stata filmata a sua insaputa nell'intimità della sua abitazione, erano stati divulgati, in modo considerato eccessivo e inutile, in un rapporto sullo stato di avanzamento di un'indagine (*Khadija Ismayilova c. Azerbaigian*, 2019, § 147).

108. Secondo la Corte, la compilazione di banche dati al fine di contribuire alla prevenzione e alla repressione di alcuni reati non può essere attuata in con una logica eccessiva per massimimizzare le informazioni memorizzate in esse (*B.B. c. Francia*, 2009, § 62; *Gardel c. Francia*, 2009, § 63; *M.B. c. Francia,* 2009, § 54). Senza il rispetto della necessaria proporzionalità in relazione ai fini legittimi attribuiti a tali meccanismi, i vantaggi che essi presentano sarebbero superati dalle gravi violazioni che essi causerebbero ai diritti e alle libertà che gli Stati devono garantire, ai sensi della Convenzione, alle persone sottoposte alla loro giurisdizione (*M. K. c. Francia*, 2013, § 35 ; *Aycaguer c. Francia*, 2017, § 34). Nell'ambito di un regime di conservazione indiscriminata e a tempo indeterminato, l'argomento secondo il quale "quanti più dati sono conservati, tanto più si prevengono i reati" sarebbe in pratica equivalente a giustificare la memorizzazione di informazioni relative all'intera popolazione e ai suoi congiunti defunti, il che è sicuramente eccessivo e irrilevante (*Gaughran c. Regno Unito*, 2020, § 89).

109. Nella causa *Catt c. Regno Unito*, 2019 (§ 122), l'assenza di effettive garanzie per assicurare la distruzione, in una banca dati della Polizia, di informazioni personali che rivelavano le opinioni politiche di un manifestante pacifico, quando la loro conservazione era diventata sproporzionata, aveva comportato la violazione dell'articolo 8.

b. Il requisito di accuratezza e di aggiornamento dei dati

110. La Corte ha giudicato diverse cause relative alla memorizzazione da parte delle autorità di dati che si erano dimostrati inaccurati, o la cui accuratezza era stata contestata dalla persona interessata (*Cemalettin Canlı c. Turchia*, 2008, §§ 34-37, sull'inaccuratezza di files della Polizia in un procedimento penale; *Rotaru c. Romania* [GC], 2000, § 36, sulla impossibilità per un individuo di contestare le informazioni raccolte dai servizi di sicurezza sulla sua asserita partecipazion a un movimento "legionario" nel suo lontano passato).

111. Le informazioni personali false o incomplete raccolte e conservate dalle autorità possono rendere la vita della persona interessata più difficile (*Khelili c. Svizzera*, 2011, § 64), possono rivelarsi diffamatorie (*Rotaru c. Romania* [GC], 2000, § 44) o possono eliminare alcune garanzie processuali previste dalla legge per proteggere i diritti della persona interessata quando tali dati possono essere trasmessi tra varie autorità (*Cemalettin Canlı c. Turchia*, 2008, §§ 42-43). La Corte ha inoltre sottolineato che era inopportuno raccogliere dati personali sulla base di una mera congettura, o di una mera presunzione senza alcuna base fattuale dimostrata (*Drelon c. Francia*, 2022, § 97).

112. Secondo la Corte, le autorità hanno il compito di dimostrare l'accuratezza dei dati memorizzati. Nella causa *Khelili c. Svizzera*, 2011 (§§ 66-70), in cui le incertezze circondavano una vaga e generica accusa di prostituzione illegale verbalizzata dalle autorità, la conservazione per anni del termine "prostituta" nei file della Polizia non era stata "necessaria in una società democratica", tenendo conto del comportamento contraddittorio delle autorità, del principio che spettava a tali medesime autorità dimostrare l'accuratezza di particolari dati, dell'esiguo margine di discrezionalità goduto dalle autorità nazionali in tale campo e della gravità dell'ingerenza nel diritto della ricorrente al rispetto della sua vita privata ai sensi dell'articolo 8. Analogamente, nella causa *Drelon c. Francia*, 2022, §§ 95-97, concernente il rifiuto, del Servizio francese di donazione del sangue, di accettare il ricorrente come donatore di sangue, sulla base della sua presunta omosessualità, la Corte ha osservato che la raccolta di dati personali dovrebbe avere una base fattuale precisa e accurata, mentre nel caso di specie era stata tratta una conclusione sulle pratiche sessuali del ricorrente soltanto perché egli aveva rifiutato di rispondere a domande sulla sua vita sessuale durante la visita medica preliminare alla donazione.

113. Nella causa *Anchev c. Bulgaria* (dec.), 2017 (§§ 112-115), in cui il ricorrente era stato sottoposto a tre indagini ed era stato segnalato, sulla base di materiale d'archivio, quale collaboratore dei vecchi Servizi di sicurezza ai sensi di una legge che imponeva di rendere noti i nominativi dei dipendenti pubblici che avevano collaborato con il regime comunista, la Corte ha rigettato la doglianza del ricorrente dopo avere osservato che egli era stato in grado di consultare gli archivi e successivamente di contestare pubblicamente la loro accuratezza sulla base di elementi concreti.

c. Il requisito che i dati non siano conservati più di quanto necessario per realizzare il fine per il quale sono stati registrati[4]

114. La questione della necessità di limitare la durata della conservazione dei dati personali è stata esaminata dalla Corte in diverse cause (*S. e Marper c. Regno Unito* [GC], 2008; *B.B. c. Francia*, 2009; *Gardel c. Francia*, 2009; *M.B. c. Francia,* 2009; *M.K. c. Francia*, 2013; *J.P.D. c. Francia* (dec.), 2014; *Peruzzo e Martens c. Germania* (dec.), 2013; *W. c. Paesi Bassi* (dec.), 2009; *Brunet c. Francia*, 2014; *Drelon c. Francia*, 2022, § 98). Un termine massimo di conservazione per trent'anni nella banca dati giudiziaria nazionale degli autori di reati sessuali, decorrente dalla scadenza della pena detentiva compresa tra i cinque e i quindici anni, per il reato di violenza sessuale, commesso nei confronti di una minore, non è stato considerato sproporzionato al fine legittimo perseguito mediante la

[4] Si veda altresì la parte *infra* della presente Guida relativa al periodo di conservazione dei dati.

memorizzazione dei dati, vale a dire la difesa dell'ordine e la prevenzione dei reati (*B.B. c. Francia*, 2009, §§ 67-68; *Gardel c. Francia*, 2009, §§ 68-69; *M.B. c. Francia*, 2009, §§ 59-60).

115. Tuttavia, la conservazione a tempo indeterminato in una banca dati nazionale delle impronte digitali, dei campioni cellulari, e dei profili del DNA di persone sospettate, ma non condannate per dei reati, a prescindere dalla natura o della gravità del reato del quale la persona era stata originariamente sospettata, e a prescindere dall'età, è stata ritenuta in violazione dell'articolo 8 (*S. e Marper c. Regno Unito* [GC], 2008, §§ 125-126). La conservazione a tempo indeterminato dei dati di una persona non condannata può essere particolarmente nociva in caso di minori, data la loro particolare situazione e l'importanza del loro sviluppo e della loro integrazione nella società (ibid., § 124).

116. L'assenza di un termine massimo di conservazione dei dati personali non è necessariamente incompatibile con l'articolo 8 (*Gaughran c. Regno Unito*, 2020, § 88; *Peruzzo e Martens c. Germania* (dec.), 2013, § 46), ma le garanzie processuali saranno vieppiù necessarie se la memorizzazione dei dati dipende interamente dalla diligenza delle autorità nell'assicurare che la sua durata sia proporzionata (ibid., § 46; *Aycaguer c. Francia*, 2017, §§ 44-46).

d. Il requisito di limitare l'utilizzo dei dati al fine per il quale sono stati registrati

117. La Corte ritiene che sia importante limitare l'uso dei dati al fine per i quali sono stati registrati. Pertanto, nella causa *Karabeyoğlu c. Turchia*, 2016 (§§ 112-121), l'utilizzo in un'indagine disciplinare di dati derivanti da intercettazioni telefoniche nel corso di un'indagine penale e, quindi, per un fine diverso da quello che aveva giustificato la loro raccolta, è stato ritenuto in violazione dell'articolo 8.

118. Nella causa *Surikov c. Ucraina*, 2017 (§§ 83-95), la conservazione a lungo termine di dati relativi alla salute mentale di un individuo, unitamente alla loro divulgazione e al loro utilizzo per fini che non erano connessi ai motivi che avevano inizialmente giustificato la loro raccolta, avevano costituito un'ingerenza sproporzionata nel diritto dell'interessato al rispetto della sua vita privata.

119. La questione del rischio dell'uomo improprio di informazioni personali è sorta anche nella causa *K.H. e altri c. Slovacchia*, 2009 (§§ 45-57), in cui le ricorrenti, otto donne di origine etnica Rom, che sospettavano di essere state sterilizzate durante un ricovero ospedaliero, hanno lamentato di non avere potuto ottenere copie delle loro cartelle cliniche. La Corte ha riscontrato la violazione dell'articolo 8, sottolineando che il rischio di abuso sostenuto dal Governo avrebbe potuto essere impedito mediante l'inserimento nel diritto interno di adeguate garanzie al fine di limitare rigorosamente le circostanze in cui tali dati potevano essere divulgati e l'ambito delle persone che avevano il diritto di accedere alle cartelle (ibid., § 56).

120. Per stabilire il confine dell'intimità della vita privata garantita dall'articolo 8, la Corte ha operato una distinzione tra la sorveglianza degli atti compiuti da un individuo in un luogo pubblico per fini di sicurezza, e la registrazione di tali atti utilizzati per altri fini, che eccede ciò che la persona interessata avrebbe potuto attendersi (*Peck c. Regno Unito*, 2003, §§ 59-62, relativa al fatto che il ricorrente era stato filmato in un luogo pubblico per motivi di sicurezza se la sequenza era divulgata ai media; *Perry c. Regno Unito*, 2003, §§ 41-42, su un sotterfugio utilizzato dalla Polizia al fine di identificare il ricorrente mediante la video-registrazione, che eccedeva i limiti del normale e prevedibile utilizzo di telecamere di sorveglianza nei posti di polizia).

e. Il requisito di trasparenza delle procedure di trattamento dei dati[5]

121. In diverse cause concernenti dati personali raccolti e memorizzati dalle autorità pubbliche, la Corte ha ritenuto che le autorità avessero l'obbligo positivo di fornire agli interessati una "procedura effettiva e accessibile" che consentisse agli stessi di accedere a "qualsiasi informazione pertinente e

[5] Si veda altresì la parte *infra* della presente Guida sul diritto di accesso ai propri dati.

appropriata ", che era necessaria, per esempio, per conoscere e comprendere la loro infanzia e il loro iniziale sviluppo (*Gaskin c. Regno Unito*, 1989, § 49), per scoprire la loro identità personale (*Odièvre c. Francia* [GC], 2003, §§ 41-49), per individuare i rischi per la salute cui erano stati esposti (*Roche c. Regno Unito* [GC], 2005, § 162; *Guerra e altri c. Italia,* 1998, § 60*; McGinley ed Egan c. Regno Unito*, 1998, § 101), o per ricostruire la loro storia personale durante un precedente regime totalitario (*Haralambie c. Romania*, 2009, § 93).

122. Tale requisito di trasparenza sarà meno rigido nell'ambito di informazioni sensibili per la sicurezza nazionale (*Leander c. Svezia*, 1987, § 51; *Segerstedt-Wiberg e altri c. Svezia*, 2006, § 102; *Dalea c. Francia* (dec.), 2010).

II. Protezione dei dati e diritto al rispetto della vita privata (articolo 8 della Convenzione)

Articolo 8 della **Convenzione**

"1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.

2. Non può esservi ingerenza di una autorità pubblica nell'esrcizio di tale diritto 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."

123. Al momento attuale la Corte ha trattato un notevole numero di operazioni relative a dati personali condotte dalle autorità o da vari enti privati, valutando se la "vita privata", il "domicilio" e/o la "corrispondenza" della persona interessata siano stati violati in modo incompatibile con l'articolo 8. In contesti differenti ha precisato il campo di applicazione di diversi diritti che le persone giuridiche e fisiche possono invocare per proteggere i loro dati personali.

A. Operazioni relative ai dati suscettibili di violare il diritto al rispetto della vita privata

124. Con lo sviluppo delle tecnologie, la raccolta, la memorizzazione e la divulgazione dei dati stanno assumendo un'ampia varietà di forme. In diversi casi la Corte ha esaminato se una o più operazioni di questo tipo avesse comportato un'ingerenza ingiustificata nel diritto della persona interessata al rispetto della propria vita privata.

1. Raccolta di dati personali

125. La Corte ha esaminato le operazioni di raccolta di dati personali in una varietà di contesti: per quanto riguarda la lotta contro la criminalità organizzata e il terrorismo mediante diversi sistemi di sorveglianza segreta creati dalle autorità; in ambito giudiziario relativamente a dati personali raccolti dalle autorità al fine di utilizzarli come prove; in ambito sanitario; nell'ambito della raccolta di dati nel luogo di lavoro, sia riguardo a datori di lavoro del settore pubblico che privato; e infine, nell'ambito degli obblighi giuridici di enti pubblici e privati di trasmettere alle autorità i dati personali di cui sono in possesso, al fine di tutelare un interesse pubblico generale.

a. Raccolta di dati da parte delle autorità mediante sorveglianza segreta[6]

126. La Corte ha trattato un notevole numero di cause concernente la questione della raccolta di dati personali mediante vari metodi di sorveglianza segreta. Qualunque sia il sistema di sorveglianza utilizzato dalle autorità, l'esistenza di adeguate e sufficienti garanzie contro gli abusi è essenziale. La Corte ritiene che i poteri di sorveglianza segreta dei cittadini siano tollerabili soltanto nella misura strettamente necessaria per salvaguardare le istituzioni democratiche (*Klass e altri c. Germania*, 1978, § 42; *Szabó e Vissy c. Ungheria*, 2016, §§ 72-73). Tale ingerenza deve essere sostenuta da motivi pertinenti e sufficienti e deve essere proporzionata al fine o ai fini legittimi perseguiti (*Segerstedt-Wiberg e altri c. Svezia*, § 88). La legislazione interna deve prevedee garanzie sufficientemente precise, efficaci e complete riguardo alla disposizione e all'esecuzione di misure di sorveglianza e al potenziale risarcimento (*Szabó e Vissy c. Ungheria*, 2016, § 89).

i. Intercettazioni telefoniche e conteggio

127. Nell'ambito giudiziario, la Corte ha riscontrato violazioni dell'articolo 8 nelle seguenti sfere: intercettazione telefonica e consegna alla Polizia delle registrazioni del conteggio (elenco dei numeri telefonici chiamati) (*Malone c. Regno Unito*, 1984, §§ 63-89); controllo e trascrizione di tutte le telefonate commerciali e private dei ricorrenti (*Huvig c. Francia*, 1990, §§ 24-35); controllo e registrazione di diverse conversazioni telefoniche del ricorrente, mediante l'intercettazione della linea telefonica di un terzo (*Kruslin c. Francia*, 1990, §§ 25-36); intercettazione telefonica di una persona mediante la linea telefonica di un terzo (*Lambert c. Francia*, 1998, §§ 21-41); controllo e registrazione da parte del pubblico ministero di una telefonata ricevuta da una persona, nel suo ufficio, da parte di un'altra persona che si trovava nell'ambasciata sovietica di Berna dell'epoca (*Amann c. Svizzera* [GC], 2000, §§ 45-62); intercettazioni telefoniche nell'ambito di un'indagine preliminare (*Prado Bugallo c. Spagna,* 2003, §§ 28-33); controllo delle conversazioni telefoniche nell'ambito di un procedimento penale e successiva pubblicazione delle stesse da parte della stampa (*Craxi c. Italia (n. 2)*, 2003, §§ 57-84); inserimento nel fascicolo del ricorrente della trascrizione di un'intercettazione telefonica svolta nell'ambito di un procedimento nel quale egli non era coinvolto (*Matheron c. Francia*, 2005, §§ 27-44); controllo delle telefonate da parte delle autorità, in assenza di un'autorizzazione da parte del pubblico ministero emessa nei confronti dell'indagato e in assenza di una legislazione che prevedesse sufficienti garanzie contro le arbitrarietà (*Dumitru Popescu c. Romania (n. 2)*, 2007, §§ 61-86); intercettazione delle telefonate fatte da un avvocato per delle indagini penali (*Kvasnica c. Slovacchia*, 2009, §§ 80-89); insufficienti garanzie contro le arbitrarietà nelle disposizioni nazionali in materia di intercettazioni telefoniche (*Dragojević c. Croazia*, 2015, §§ 85-102; *Liblik e altri c. Estonia*, 2019, §§ 132-143); assenza di adeguate garanzie giudiziarie (*Moskalev c. Russia*, 2017, §§ 35-45); assenza di un controllo efficace della registrazione di telefonate nell'ambito di un procedimento penale (*Pruteanu c. Romania*, 2015, §§ 41-58); controllo di telefonate effettuate mediante un telefono cellulare (*Šantare e Labazņikovs c. Lettonia*, 2016, §§ 56-63); assenza ingiustificata di notifica *ex post* di una misura di intercettazione temporanea del telefono cellulare (*Cevat Özel c. Turchia,* 2016, §§ 29-37); e controllo preventivo delle telefonate (*Mustafa Sezgin Tanrıkulu c. Turchia,* 2017, §§ 45-66); potere praticamente illimitato dei Servizi segreti nello svolgimento della sorveglianza di un individuo e degli incontri svoltisi nell'appartamento di sua proprietà, in assenza di sufficienti garanzie giuridiche (*Zoltán Varga c. Slovacchia*, 2021, §§ 170-171), il che incideva aleatoriamente su un'altra persona senza che a quest'ultima fosse fornita alcuna garanzia ai sensi del diritto interno (*Haščák c. Slovacchia,* 2022, § 95); e intercettazione, registrazione e trascrizione di una conversazione telefonica intercorsa tra un avvocato e un suo assistito, che era un ex ministro della difesa, sottoposto a sorveglianza segreta in relazione a un'indagine penale (*Vasil Vasilev c. Bulgaria*, 2021, §§ 167-181).

[6] Si veda altresì la Guida all'articolo 8 della Convenzione (diritto al rispetto della vita privata e familiare).

128. La Corte non ha riscontrato violazione dell'articolo 8 in relazione a intercettazioni telefoniche autorizzate per decisione giudiziaria, nella consapevolezza che la necessità di tale misura era stata valutata dai tribunali (*İrfan Güzel c. Turchia*, 2017, §§ 78-89).

129. La Corte non riscontrato alcuna violazione dell'articolo 8 anche nei seguenti casi: verbalizzazione da parte della Polizia di numeri telefonici contattati da un individuo mediante il conteggio del suo telefono (*P.G. e J.H. c. Regno Unito*, 2001, §§ 42-51); intercettazione delle linee telefoniche di un giudice nell'ambito di indagini penali relative a un'organizzazione illegale, della quale si sospettava che egli fosse membro, contribuente o favoreggiatore (*Karabeyoğlu c. Turchia*, 2016, §§ 74-111); e intercettazione delle comunicazioni telefoniche del direttore di un carcere nell'ambito di un'indagine penale sulla sua sospetta attività di corruzione in carcere per profitto personale, benché l'indagine fosse stata infine archiviata sulla base dell'assenza di prove incriminanti (*Adomaitis c. Lituania*, 2022, §§ 81-90).

130. Diversi ricorsi sono stati dichiarati manifestamente infondati, in relazione a: intercettazioni telefoniche nell'ambito di attività di intelligence preventive da parte della Polizia (*Deveci c. Turchia* (dec.), 2022); intercettazioni telefoniche nell'ambito di un'indagine preliminare (*Greuter c. Paesi Bassi* (dec.), 2002); intercettazioni telefoniche nell'ambito di un'indagine penale quale uno dei principali metodi investigativi per facilitare la dimostrazione della partecipazione di alcune persone a un'importante rete di traffico di sostanze stupefacenti (*Coban c. Spagna* (dec.), 2006); e controllo delle conversazioni telefoniche effettuate da un membro del Parlamento europeo, accusato di appropriazione indebita di beni sociali e inapplicabiità in tale caso del trattamento particolare riservato ai deputati nazionali (*Marchiani c. Francia* (dec.), 2008).

131. Nel contesto carcerario, la registrazione e la memorizzazione illegali da parte delle autorità carcerarie, delle telefonate di un detenuto e il loro successivo utilizzo come prove per condannare il detenuto per un ulteriore reato, avevano violato l'articolo 8, nella causa *Doerga c. Paesi Bassi*, 2004 (§§ 43-54).

132. In diversi altri campi la Corte ha riscontrato violazioni dell'articolo 8 in relazione a: un sistema automatico di controllo di tutta la corrispondenza e delle telefonate effettuate da minori detenuti in un istituto penale di istruzione, che escludeva qualsiasi genere di riservatezza riguardo ai tipi degli scambi controllati (*D.L. c. Bulgaria*, 2006, §§ 100-116); l'intercettazione autorizzata dal Ministero della Difesa delle comunicazioni in uscita di organizzazioni operanti nel campo delle libertà civili (*Liberty e altri c. Regno Unito*, 2008, §§ 56-70); la mera esistenza di una legislzione che permette il controllo delle telecomunicazioni da parte di un'organizzazione non governativa moldava specializzata nella rappresentanza dei ricorrenti dinanzi alla Corte (*Iordachi e altri c. Moldavia*, 2009, §§ 29-54); la fuga nei media e la teletrasmissione di una conversazione privata registrata con l'approvazione delle autorità sulla linea telefonica di un politico indagato dalle autorità inquirenti (*Drakšas c. Lituania*, 2012, § 62); le lacune nel quadro giuridico che disciplinava il controllo segreto delle telefonate effettuate mediante telefono cellulare, compiuto dagli operatori della rete di telefonia mobile, che permetteva al Servizio di sicurezza federale di intercettare qualsiasi tipo di comunicazione telefonica senza preliminare autorizzazione giudiziaria (*Roman Zakharov c. Russia* [GC], 2015, §§ 163-305); l'uso in un'indagine disciplinare dei dati relativi a intercettazioni telefoniche provenienti da un'indagine penale (*Karabeyoğlu c. Turchia*, 2016, §§ 112-121); e l'uso in un procedimento disciplinare nei confronti di un avvocato della trascrizione di una conversazione con un suo assistito il cui telefono era stato intercettato (*Versini-Campinchi e Crasnianski c. Francia*, 2016, §§ 49-84). Per contro, l'uso, nel procedimento disciplinare nei confronti del direttore di un carcere, delle informazioni ricevute mediante le intercettazioni telefoniche svolte nell'ambito di un'indagine penale relativa alla sua sospetta corruzione è stato considerato proporzionato (*Adomaitis c. Lituania*, 2022, § 87).

ii. Intercettazione dei messaggi del cercapersone

133. Nella causa *Taylor-Sabori c. Regno Unito,* 2002, §§ 18-19, nell'ambito di un procedimento giudiziario, l'intercettazione da parte della Polizia dei messaggi del cercapersone del ricorrente e il successivo rinvio a essi quale base per una condanna sono stati considerati in violazione dell'articolo 8, in assenza di disposizioni giuridiche che regolamentassero tale intercettazione.

iii. Audio-sorveglianza e video-sorveglianza

134. La Corte ha riscontrato la violazione dell'articolo 8 in un caso in cui la registrazione di una conversazione, utilizzando un dispositivo di radiotrasmissione, nell'ambito di un'operazione segreta di Polizia, non era stata accompagnata da adeguate garanzie processuali (*Bykov c. Russia* [GC], 2009, §§ 81, 83; *Oleynik c. Russia*, 2016, §§ 75-79).

135. La Corte ha operato una distinzione tra il controllo degli atti compiuti da un individuo in un luogo pubblico, per fini di sicurezza, e la registrazione di tali atti per altri fini, eccedente quanto la persona avrebbe potuto possibilmente prevedere (*Peck c. Regno Unito*, 2003, §§ 59-62; *Perry c. Regno Unito*, 2003, §§ 41-42), al fine di stabilire il rigido confine tra la vita privata garantita ai sensi dell'articolo 8 nella sfera delle misure di sorveglianza segreta e l'intercettazione delle comunicazioni da parte delle autorità statali.

136. Nell'ambito giudiziario, la Corte ha riscontrato violazioni dell'articolo 8 nei seguenti casi: la registrazione delle voci dei ricorrenti accusati di un reato e ristretti nelle loro celle in un posto di polizia (*P.G. e J.H. c. Regno Unito*, 2001, §§ 56-63); il fatto di filmare, ai fini dell'identificazione, un indagato in un posto di polizia utilizzando una telecamera segreta a circuito chiuso (*Perry c. Regno Unito*, 2003, §§ 36-49); la registrazione da parte della Polizia, mediante un dispositivo di ascolto installato nell'abitazione di un terzo, cui il ricorrente aveva fatto visita, di una conversazione non provocata e spontanea, durante la quale il ricorrente aveva ammesso di avere partecipato all'importazione di sostanze stupefacenti (*Khan c. Regno Unito*, 2000, §§ 25-28); la collocazione di microspie da parte della Polizia in locali privati nell'ambito di un'indagine giudiziaria (*Vetter c. Francia*, 2005, §§ 20-27); la registrazione di una conversazione mediante un dispositivo di ascolto, impiantato su una persona da parte delle autorità di Polizia, e il successivo utilizzo di tale registrazione durante il processo, anche se non si trattava dell'unica prova incriminante (*Heglas c. Repubblica ceca*, 2007, §§ 71-76); e la registrazione delle comunicazioni da parte di una persona nell'ambito e a vantaggio di un'indagine ufficiale, di natura penale o di altra natura, con la collaborazione e l'assistenza tecnica delle autorità investigative statali (*Van Vondel c. Paesi Bassi*, 2007, §§ 47-55).

137. Nel contesto carcerario, la Corte ha riscontrato violazioni dell'articolo 8 nei seguenti casi: l'uso da parte delle autorità di dispositivi di registrazione video e audio, installati segretamente nella cella del ricorrente e nelle zone del carcere adibite alle visite, nonché sulla persona di un compagno di reclusione, che facilitavano la registrazione di dichiarazioni del ricorrente non spontanee e provocate (*Allan c. Regno Unito*, 2002, §§ 35-36); la registrazione delle conversazioni tra i detenuti e le loro famiglie nelle sale visita di un carcere (*Wisse c. Francia*, 2005, §§ 28-34); la sorveglianza segreta delle consultazioni di un detenuto con il suo difensore (*R.E. c. Regno Unito*, 2015, §§ 115-143); e la video-sorveglianza ventiquattro ore su ventiquattro dei detenuti nelle loro celle, mediante una telecamera segreta a circuito chiuso (*Gorlov e altri c. Russia*, 2019, §§ 83-100).

138. La Corte non ha riscontrato alcuna violazione dell'articolo 8 relativa alla sorveglianza segreta delle consultazioni di un detenuto con la persona nominata per assisterlo, in quanto persona vulnerabile, dopo il suo arresto (*R.E. c. Regno Unito*, 2015, §§ 154-168). Le disposizini relative alla sorveglianza, nella misura in cui erano connesse alla possibile sorveglianza delle consultazioni tra i detenuti e degli adulti qualificati, erano state accompagnate da adeguate garanzie contro gli abusi.

139. In contesti differenti in cui i dati in questione erano stati raccolti mediante telecamere occultate, la Corte ha riscontrato violazioni dell'articolo 8 in relazione a: la trasmissione ai media del video

ottenuto mediante una telecamera nascosta a circuito chiusio, che aveva filmato una persona che tentava di suicidarsi in un luogo pubblico (*Peck c. Regno Unito*, 2003, §§ 57-87); la diffusione per televisione dell'immagine non sfocata e non velata di un individuo, ottenuta mediante una telecamera occultata (*Bremner c. Turchia*, 2015, §§ 71-85); la video-sorveglianza segreta di una giornalista nella sua abitazione e la diffusione pubblica dei video (*Khadija Ismayilova c. Azerbaigian*, 2019, §§ 108-132). Si vedano altresì i paragrafi 232-234 e 151-157 della presente Guida.

iv. Geolocalizzazione di veicolo mediante GPS[7]

140. Nella causa *Uzun c. Germania*, 2010 (§§ 49-81) la sorveglianza mediante GPS di un individuo sospettato di terrorismo non aveva costituito violazione dell'articolo 8. Per contro, nella causa *Ben Faiza c. Francia*, 2018 (§§ 53-61), l'installazione di un dispositivo di geolocalizzazione in un veicolo e l'uso dei dati ottenuti in tal modo, che avevano fornito agli investigatori informazioni in tempo reale circa gli spostamenti del ricorrente e avevano permesso a essi di arrestarlo, sono stati considerati in violazione dell'articolo 8.

v. Sorveglianza da parte di investigatori privati

141. Nella causa *Vukota-Bojić c. Svizzera*, 2016 (§§ 52-78), la Corte ha riscontrato la violazione dell'articolo 8 in relazione alla sorveglianza illecita da parte di investigatori privati delle attività di una persona che percepiva prestazioni assistenziali contestate. Il diritto interno non aveva indicato con sufficiente chiarezza la portata e le modalità di esercizio della discrezionalità conferita alle compagnie assicuratrici, che agivano in qualità di autorità pubbliche, nelle controversie in materia assicurativa per svolgere una sorveglianza segreta degli assicurati.

vi. Controllo della corrispondenza

142. Nel contesto carcerario, la Corte ha riscontrato violazioni dell'articolo 8 riguardo a: l'intercettazione e l'apertura della corrispondenza di un detenuto (*Lavents c. Lettonia*, 2002, §§ 136-137); l'apertura della corrispondenza di un detenuto, anche in caso di malfunzionamento del servizio postale all'interno del carcere (*Demirtepe c. Francia*, 1999, §§ 26-28; *Valašinas c. Lituania*, 2001, §§ 128-130); l'intercettazione e la censura della corrispondenza di un detenuto (*Silver e altri c. Regno Unito*, 1983, §§ 84-105; *Labita c. Italia* [GC], 2000, §§ 176-184; *Niedbała c. Polonia*, 2000, §§ 78-84; *Messina c. Italia (n. 2)*, 2000, §§ 78-83); l'intercettazione delle lettere di detenuti al loro difensore (*Ekinci e Akalın c. Turchia*, 2007, §§ 37-48); l'intercettazione della corrispondenza di detenuti con i loro difensori e con la Commissione europea dei diritti umani (*Campbell c. Regno Unito*, 1992, §§ 32-54; *A.B. c. Paesi Bassi*, 2002, §§ 81-94); l'apertura di una lettera inviata a un detenuto dalla Commissione (*Peers c. Grecia*, 2001, §§ 81-84); la sorveglianza della corrispondenza di un detenuto con il suo medico (*Szuluk c. Regno Unito*, 2009, §§ 47-55); la prassi di scannerizzare e caricare la corrispondenza privata dei detenuti, sia in entrata che in uscita, sul Server della rete giudiziaria nazionale (*Nuh Uzun e altri c. Turchia*, 2022, §§ 80-99). Per contro, nella causa *Erdem c. Germania*, 2001 (§§ 53-70), non è stata riscontrata alcuna violazione dell'articolo 8 in relazione all'intercettazione della corrispondenza tra un detenuto sospettato di terrorismo e il suo difensore.

143. In un contesto differente, è stata riscontrata la violazione dell'articolo 8 in un caso in cui la corrispondenza di un fallito era stata aperta e copiata su un file dal curatore fallimentare (*Foxley c. Regno Unito*, 2000, §§ 27-47).

[7] Si veda altresì la sezione della Guida *supra* relativa ai Dati di localizzazione GPS.

vii. Operazioni di sorveglianza segreta, spionaggio e sorveglianza di massa

144. Nella causa *Roman Zakharov c. Russia* [GC], 2015 (§§ 171-172) la Corte ha stabilito che un ricorrente poteva affermare di essere vittima di una violazione causata dalla mera esistenza di misure di sorveglianza segreta o di una legislazione che permette tali misure, se sono soddisfatte determinate misure, e che l'approccio adottato nella causa *Kennedy c. Regno Unito*, 2010 (§ 124) era il più adatto alla necessità di assicurare che la segretezza delle misure di sorveglianza non comportasse che tali misure fossero effettivamente inattaccabili e sfuggissero al controllo delle autorità giudiziarie nazionali e della Corte. Nella causa *Ekimdzhiev e altri c. Bulgaria*, 2022 (§ 262-277 e 371-384) la Corte ha ammesso, sulla base dei principi elaborati nella causa *Roman Zakharov c. Russia* [GC], 2015 (§ 171), che i ricorrenti, due avvocati e due organizzazioni non governative legate a essi, potevano sostenere di essere vittime di un'ingerenza nei loro diritti di cui all'articolo 8, in ragione della mera esistenza di una legislazione o di prassi interne che permettevano la sorveglianza segreta, nonché di leggi che disciplinavano l'accesso da parte delle autorità a dati di comunicazioni conservati.

145. La Corte ha riscontrato violazioni dell'articolo 8 nei seguenti casi: se ai sensi della Legge sui mezzi di sorveglianza speciale l'associazione ricorrente poteva essere sottoposta in qualsiasi momento a misure di sorveglianza senza notifica (*Association for European Integration and Human Rights and Ekimdzhiev c. Bulgaria*, 2007, §§ 69-94); l'intercettazione e la registrazione di una conversazione mediante un dispositivo di radiotrasmissione nell'ambito di un'operazione segreta della Polizia senza alcuna garanzia processuale (*Bykov c. Russia* [GC], 2009, §§ 72-83); la registrazione di conversazioni nell'ambito di un "esperimento operativo" condotto per iniziativa del Servizio di sicurezza federale in modo non "previsto dalla legge" (*Oleynik c. Russia*, 2016, §§ 74-79); l'intercettazione autorizzata da parte del Ministero della Difesa delle comunicazioni in uscita di organizzazioni operanti nel campo delle libertà civili (*Liberty e altri c. Regno Unito*, 2008, §§ 55-70); la memorizzazione di registrazioni e la sorveglianza da parte della Polizia di un ricorrente a causa della sua appartenenza a un'organizzazione per i diritti umani (*Shimovolos c. Russia*, 2011, §§ 64-71); la legislazione in materia di sorveglianza segreta che istituiva un'unità operativa speciale per la lotta al terrorismo, senza adeguate garanzie contro gli abusi (*Szabó e Vissy c. Ungheria*, 2016, §§ 52-89); la memorizzazione di informazioni raccolte mediante sorveglianza segreta (*Rotaru c. Romania* [GC], 2000, §§ 45-63; *Associazione «21 dicembre 1989» e altri c. Romania*, 2011, §§ 169-177); varie carenze nel quadro giuridico nazionale che disciplinava la sorveglianza segreta delle comunicazioni di telefonia mobile (*Roman Zakharov c. Russia* [GC], 2015, §§ 163-305); e un regime di intercettazione di massa delle comunicazioni, che non conteneva sufficienti garanzie "da un estremo all'altro" per offrire una protezione adeguata ed effettiva dalle arbitrarietà e dal rischio di abusi, benché siano state individuate alcune solide garanzie (*Centrum för rättvisa c. Svezia* [GC], 2021, §§ 365-374, e *Big Brother Watch e altri c. Regno Unito* [GC], 2021, §§ 424-427). La Corte ha riscontrato la violazione dell'articolo 8 anche nella causa *Ekimdzhiev e altri c. Bulgaria*, 2022 (§§ 356-359 e 419-421), osservando, in particolare, che benché notevolmente migliorata successivamente all'esame svolto nella causa *Association for European Integration and Human Rights and Ekimdzhiev c. Bulgaria*, 2007, l'applicazione nella pratica delle leggi che disciplinavano la sorveglianza segreta difettava ancora per diversi aspetti delle minime garanzie contro le arbitrarietà e gli abusi. È pervenuta a una conclusione analoga in relazione alle leggi che disciplinavano la conservazione dei dati di comunicazione e il loro successivo utilizzo da parte delle autorità.

146. La Corte non ha riscontrato alcuna violazione dell'articolo 8 nei seguenti casi: l'utilizzo di un agente infiltrato, unitamente all'intercettazione della linea telefonica del ricorrente, accusato di traffico di sostanze stupefacenti (*Lüdi c. Svizzera*, 1992, §§ 38-41); un regime che autorizzava la sorveglianza segreta della corrispondenza, della posta e delle comunicazioni telefoniche generali della popolazione (*Klass e altri c. Germania*, 1978, §§ 39-60); e un quadro legislativo che autorizzava l'intercettazione delle comunicazioni interne al fine di contrastare il terrorismo e gravi reati (*Kennedy c. Regno Unito*, 2010, §§ 151-170).

147. La Corte ha dichiarato manifestamente infondata la causa *Weber e Saravia c. Germania* (dec.), 2006 (§§ 143-153) relativa alla sorveglianza strategica delle telecomunicazioni, causa che faceva seguito alla causa *Klass e altri c. Germania*, 1978.

b. Raccolta di dati da parte dei datori di lavoro nel luogo di lavoro

148. La Corte ha valutato ai sensi dell'articolo 8 la questione della raccolta di dati personali nel luogo di lavoro da parte di datori di lavoro del settore pubblico (*Halford c. Regno Unito*, 1997, §§ 49, 45; *Antović e Mirković c. Montenegro*, 2017, § 58; *Libert c. Francia*, 2018, § 41) o privato (*Köpke c. Germania* (dec.), 2010; *Bărbulescu c. Romania* [GC], 2017, § 109; e *López Ribalda e altri c. Spagna* [GC], 2019, § 109). In alcuni casi l'operazione di raccolta dei dati era stata svolta all'insaputa degli interessati, mediante una sorveglianza che era stata tenuta segreta, o totalmente (*Halford c. Regno Unito*, 1997, § 49; *Copland c. Regno Unito,* 2007, § 45; *Bărbulescu c. Romania* [GC], 2017, § 78), o parzialmente (*López Ribalda e altri c. Spagna* [GC], 2019, § 93), mentre in altri casi i dati erano stati raccolti con la piena consapevolezza dei dipendenti interessati (*Antović e Mirković c. Montenegro*, 2017, § 44).

149. I dati personali da raccogliere derivanti da: sorveglianza di telefonate non professionali da locali di lavoro (*Halford c. Regno Unito*, 1997, § 44); controllo dell'uso del telefono, della posta elettronica e di internet sul luogo di lavoro (*Copland c. Regno Unito*, 2007, §§ 44-49); controllo dell'uso di internet e della messaggistica istantanea (Yahoo) (*Bărbulescu c. Romania* [GC], 2017, § 74); apertura di file memorizzati da un dipendente su un computer fornito dal suo datore di lavoro a fini lavorativi (*Libert c. Francia*, 2018, § 25); fotografie scattate mediante la video-registrazione che mostravano il comportamento nel luogo di lavoro di un dipendente identificato o identificabile (*Köpke c. Germania* (dec.), 2010; *Antović e Mirković c. Montenegro*, 2017, § 44; *López Ribalda e altri c. Spagna* [GC], 2019, § 92); o il controllo, per mezzo di un sistema GPS, delle distanze percorse da un dipendente mediante un veicolo della società nel corso della sua attività professionale e, se del caso, negli spostamenti privati (*Florindo de Almeida Vasconcelos Gramaxo c. Portogallo*, 2022, §§ 94-96).

150. Nella prime due sentenze pronunciate in questo ambito (*Halford c. Regno Unito*, 1997, § 44, e *Copland c. Regno Unito*, 2007, § 41), la Corte ha ritenuto che le telefonate non professionali effettuate dai locali dell'azienda siano a prima vista comprese nelle nozioni di "vita privata" e di "corrispondenza" ai fini dell'articolo 8. Ha ritenuto anche che le e-mail inviate dal lavoro dovrebbero essere analogamente tutelate ai sensi dell'articolo 8, così come le informazioni tratte dal controllo dell'uso personale di internet (*Copland c. Regno Unito*, 2007, § 41). Successivamente, la Corte ha inoltre precisato che anche i dati chiaramente identificati come privati e memorizzati da un dipendente in un computer, fornitogli dal suo datore di lavoro a fini lavorativi, potrebbero essere compresi nella nozione di "vita privata" (*Libert c. Francia*, 2018, § 25). Inoltre, anche una video-registrazione realizzata in segreto, che mostrava il comportamento di un dipendente nel luogo di lavoro, senza avviso, incide sulla "vita privata" (*Köpke c. Germania* (dec.), 2010). Successivamente, la Corte non ha riscontrato alcun motivo per discostarsi da questa conclusione, sia se la video-sorveglianza di dipendenti nel luogo di lavoro era segreta che se non lo era (*Antović e Mirković c. Montenegro*, 2017, § 44; *López Ribalda e altri c. Spagna* [GC], 2019, § 93).

151. Nelle cause *Halford c. Regno Unito*, 1997 (§§ 50-51) e *Copland c. Regno Unito,* 2007 (§ 48), la Corte ha ritenuto che in assenza, all'epoca dei fatti, di una disposizione giuridica interna che autorizzava la raccolta di dati personali provenienti, rispettivamente, dalle telefonate non professionali dei dipendenti e dai messaggi di posta elettronica inviati dal luogo di lavoro, l'ingerenza che ne derivava nel loro diritto al rispetto della loro vita privata non fosse stata "prevista dalla legge". Nella causa *Köpke c. Germania* (dec.), 2010, la Corte ha dichiarato manifestamente infondata una doglianza relativa a un datore di lavoro che aveva raccolto con l'aiuto di un'agenzia di investigazioni privata, utilizzando la video-sorveglianza segreta, dati relativi alla cassiera di un supermercato, sospettata di furto. Benché all'epoca dei fatti le condizioni alle quali un datore di lavoro poteva ricorrere alla video-sorveglianza di un dipendente non fossero state ancora stabilite dalla legislazione,

la giurisprudenza del Tribunale federale del lavoro aveva elaborato importanti garanzie contro le ingerenze arbitrarie nel diritto dei dipendenti al rispetto della loro vita privata.

152. L'esistenza del ragionevole sospetto della commissione di gravi irregolarità e la portata delle perdite individuate nella fattispecie possono costituire una giustificazione convincente per l'attuazione da parte di datori di lavoro di una raccolta di dati personali nel luogo di lavoro (*López Ribalda e altri c. Spagna* [GC], 2019, § 134). Per contro, meri sospetti di appropriazione indebita o di qualsiasi altra irregolarità da parte dei dipendenti non possono giustificare l'installazione da parte del datore di lavoro di una video-sorveglianza segreta (ibid., § 134).

153. Nella causa *Bărbulescu c. Romania* [GC], 2017 (§ 121) la Corte ha definito un certo numero di criteri da soddisfare in relazione a misure volte a controllare la corrispondenza e le comunicazioni dei dipendenti nel luogo di lavoro, affinché esse non violino l'articolo 8. In tale contesto, le autorità nazionali devono rispondere alle seguenti domande: era il dipendente informato della possibilità che il datore di lavoro avrebbe potuto adottare misure volte a controllare la corrispondenza e altre comunicazioni, e dell'attuazione di tali misure? Quale era la portata del controllo svolto dal datore di lavoro e del livello di intrusione nella vita privata del dipendente? Aveva il datore di lavoro fornito motivi legittimi che giustificassero il controllo delle comunicazioni del dipendente? Sarebbe stato possibile istituire un sistema di sorveglianza basato su metodi e misure meno invasivi dell'accesso diretto alle comunicazioni del dipendente? Quali erano state le conseguenze del controllo per il dipendente sottoposto a esso? Erano state fornite al dipendente adeguate garanzie, specialmente se le operazioni di controllo da parte del datore di lavoro erano di natura invasiva? E infine, le autorità nazionali dovrebbero assicurare che un dipendente le cui comunicazioni sono state controllate abbia accesso a un ricorso dinanzi a un organo giudiziario competente a determinare, almeno sostanzialmente, in quale modo fossero stati osservati i criteri delineati sopra e se le misure contestate fossero lecite (ibid., § 122).

154. Successivamente, nella causa *López Ribalda e altri c. Spagna* [GC], 2019 (§ 116), la Corte ha sottolineato che tali criteri erano trasponibili alle misure di video-sorveglianza attuate da un datore di lavoro nel luogo di lavoro. Nella causa *Florindo de Almeida Vasconcelos Gramaxo c. Portogallo*, 2022 (§ 115), la Corte ha inoltre applicato i suddetti criteri nell'ambito del controllo da parte di un datore di lavoro mediante un sistema GPS delle distanze percorse da un dipendente con il veicolo della società.

155. La Corte ha riscontrato violazioni dell'articolo 8 in casi in cui ha rilevato che i tribunali nazionali non avevano assicurato che l'attuazione di misure di sorveglianza da parte di un datore di lavoro fosse proporzionata e accompagnata da adeguate e sufficienti garanzie. Nella causa *Bărbulescu c. Romania* [GC], 2017 (§§ 108-141), i tribunali nazionali non avevano determinato i motivi specifici che avevano giustificato l'attuazione di misure di sorveglianza, se il datore di lavoro avrebbe potuto ricorrere a misure meno invasive per la vita privata e la corrispondenza del dipendente, o se il dipendente fosse stato informato anticipatamente dal suo datore di lavoro del possibile controllo delle sue comunicazioni. Per contro, nella causa *Libert c. Francia*, 2018 (§§ 37-53) la Corte non ha riscontrato alcuna violazione dell'articolo 8 in relazione all'apertura di file personali memorizzati in un computer di lavoro, il cui contenuto pornografico aveva fornito la base del licenziamento del dipendente. Ha osservato che il diritto interno, come interpretato e applicato dal tribunale nazionale, aveva compreso adeguate garanzie contro le arbitrarietà, in particolare il fatto che il datore di lavoro avesse potuto aprire i file contrassegnati come "personali" soltanto alla presenza del dipendente.

156. Secondo la Corte, soltanto un'esigenza preponderante relativa alla protezione di importanti interessi pubblici o privati avrebbe potuto giustificare la mancata fornitura da parte del datore di lavoro di informazioni preliminari sulle misure che avrebbero potuto violare la protezione dei dati personali dei dipendenti (*López Ribalda e altri c. Spagna* [GC], 2019, § 133). Prima di attuare misure finalizzate alla raccolta dei loro dati, i datori di lavoro avrebbero dovuto informare i dipendenti interessati dell'esistenza e delle condizioni di tale raccolta dei dati, anche se soltanto in modo generale (ibid., § 131). L'esigenza di trasparenza e il conseguente diritto di informazione sono fondamentali, in

particolare nell'ambito dei rapporti di lavoro, nei quali il datore di lavoro ha notevoli poteri nei confronti dei dipendenti, e dovrebbe essere evitato qualsiasi abuso di tali poteri. Tuttavia, la fornitura di informazioni all'individuo controllato e le loro portata costituiscono soltanto uno dei criteri di cui si deve tenere conto per valutare la proporzionalità di una misura di questo tipo in un dato caso. Tuttavia, in assenza di tali informazioni, le garanzie derivanti dagli altri criteri saranno ancora più importanti (ibid., § 131).

157. Se non sono state fornite preliminari informazioni, è importante accertare se i dipendenti che sono stati sottoposti a sorveglianza avessero avuto a disposizione ricorsi interni, finalizzati specificamente ad assicurare un'effettiva protezione del diritto al rispetto della vita privata. Nell'ambito delle misure imposte ai dipendenti nel luogo di lavoro, tale protezione può essere assicurata mediante vari mezzi, che possono riguardare il diritto del lavoro ma anche il diritto civile, amministrativo o penale (ibid., § 136).

158. Per quanto riguarda specificamente la video-sorveglianza dei dipendenti, nella causa *López Ribalda e altri c. Spagna* [GC], 2019 (§ 125) la Corte ha sottolineato che è necessario distinguere, nell'analisi di una misura di video-sorveglianza, i vari luoghi in cui è stato svolto il controllo, alla luce della tutela della vita privata che un dipendente poteva ragionevolmente attendersi. Tale aspettativa è molto elevata nei luoghi che sono privati per natura, come i gabinetti o gli spogliatoi, dove è giustificata una maggiore protezione, o perfino un divieto totale della video-sorveglianza (ibid., §§ 125, 61, 65, che citano i pertinenti strumenti internazionali). Essa rimane alta in spazi di lavoro chiusi come gli uffici, ed è manifestamente inferiore in luoghi visibili o accessibili ai colleghi o al pubblico generale (ibid. , § 125).

159. A tale riguardo, nella causa *Köpke c. Germania* (dec.), 2010, la Corte ha dichiarato irricevibile in quanto manifestamente infondata la doglianza sollevata dalla ricorrente, una cassiera di un supermercato, concernente una misura di video-sorveglianza segreta attuata dal suo datore di lavoro con l'aiuto di un'agenzia di investigazioni privata. La Corte ha osservato in particolare che la misura contestata era stata limitata nel tempo (due settimane) e aveva riguardato soltanto la zona accessibile al pubblico che circondava la cassa, che i dati del video ottenuti erano stati trattati da un limitato numero di persone che lavoravano per l'agenzia di investigazioni e dal personale del datore di lavoro, e che erano stati utilizzati soltanto nell'ambito del procedimento di licenziamento della ricorrente e nel procedimento dinanzi ai tribunali del lavoro.

160. Per contro, nella sentenza relativa alla causa *Antović e Mirković c. Montenegro*, 2017 (§§ 55-60), la Corte ha riscontrato la violazione dell'articolo 8, in quanto l'asserita violazione della vita privata dei ricorrenti, due docenti universitari, in conseguenza dell'installazione di un sistema di video-sorveglianza nelle aule universitarie in cui essi svolgevano le lezioni, non era prevista dalla legge.

161. Nella causa *López Ribalda e altri c. Spagna* [GC], 2019 (§ 137), la Corte non ha riscontrato alcuna violazione dell'articolo 8 in relazione alla video-sorveglianza parzialmente visibile e parzialmente segreta dei cassieri e degli assistenti alle vendite di un supermercato, tenuto conto, *inter alia,* delle notevoli garanzie fornite dalla legislazione spagnola, tra cui i rimedi dei quali i ricorrenti non si erano avvalsi.

162. Analogamente, la causa *Florindo de Almeida Vasconcelos Gramaxo c. Portogallo*, 2022 (§§ 105-125) concerneva il licenziamento del ricorrente sulla base dei dati del chilometraggio registrati per mezzo di un sistema GPS installato sul veicolo della sua società da parte del suo datore di lavoro. La Corte non ha riscontrato alcuna violazione dell'articolo 8, avendo considerato che i tribunali nazionali avessero bilanciato attentamente gli interessi concorrenti in gioco vale a dire, il diritto del ricorrente al rispetto della sua vita privata e il diritto del suo datore di lavoro di assicurare la regolare gestione della società, tenendo conto del fine legittimo perseguito dalla società, vale a dire il diritto di controllare le sue spese.

c. Raccolta di dati al fine dell'utilizzo come prove in procedimenti giudiziari

163. La raccolta di prove reali nell'ambito di procedimenti giudiziarie solleva questioni connesse alla protezione dei dati personali degli individui, qualunque sia il loro status nel procedimento in questione, quello di parti, di testimoni o di terzi.

i. Perquisizioni e sequestri

164. In diverse cause la Corte ha sottolineato che gli Stati contraenti avrebbero potuto considerare necessario ricorrere a misure quali le perquisizioni e i sequestri al fine di ottenere le prove materiali di alcuni reati (*Vasylchuk c. Ucraina*, 2013, § 79; *K.S. e M.S. c. Germania*, 2016, § 43). In tali casi, l'esame delle misure verte sulla pertinenza e sull'adeguatezza dei motivi forniti per giustificarle, nonché sull'osservanza del principio della loro proporzionalità al fine perseguito (*Smirnov c. Russia*, 2007, § 44). La gravità del reato che ha provocato la perquisizione e il sequestro, le circostanze in cui è stato emesso il provvedimento, in particolare se fosse disponibile all'epoca qualsiasi ulteriore prova, il contenuto e la portata del provvedimento, tenuto conto in particolare della natura dei luoghi perquisiti e delle garanzie attuate al fine di contenere l'impatto della misura entro limiti ragionevoli, le modalità di conduzione della perquisizione e la portata delle possibili ripercussioni sul rispetto per la vita privata della persona interessata, sono tutti importanti criteri di cui si deve tenere conto nel bilanciare i vari interessi concorrenti (ibid., § 44; *Modestou c. Grecia*, 2017, § 42 e i rinvii ivi citati). La Corte esige anche che il diritto interno preveda adeguate e sufficienti garanzie contro le arbitrarietà (*Vinci Construction et GTM Génie Civil et Services c. Francia*, 2015, § 66; *Modestou c. Grecia*, 2017, § 43). Tali garanzie comprendono l'esistenza di misure di un "effettivo controllo" delle misure che interferiscono con l'articolo 8 (ibid., § 42).

165. Nella causa *Trabajo Rueda c. Spagna*, 2017 (§§ 44-47), il sequestro del computer personale del ricorrente, che aveva permesso alla Polizia di accedere a tutti i file personali memorizzati nel computer, in quanto esso conteneva materiale pedopornografico, era stato condiderato in violazione dell'articolo 8. La Corte non era convinta dell'urgenza della situazione che aveva richiesto che la Polizia sequestrasse i file contenuti nel computer personale del ricorrente e che accedesse a tutti i dati memorizzati senza ottenere la preliminare autorizzazione giudiziaria richiesta normalmente, benché tale autorizzazione avrebbe potuto essere ottenuta molto rapidamente.

166. Nella causa *K.S. e M.S. c. Germania*, 2016 (§§ 32-58), la Corte non ha riscontrato alcuna violazione dell'articolo 8 in relazione alla perquisizione dell'abitazione dei ricorrenti in virtù di un mandato emesso sulla base di informazioni comprendenti dati personali copiati illecitamente da un dipendente bancario e venduti successivamente ai Servizi segreti, relativi ai loro beni in una banca all'estero. La legislazione e la prassi tedesche prevedevano garanzie adeguate ed effettive contro gli abusi. Inoltre, i tribunali nazionali non avevano ecceduto il loro margine di discrezionalità nel basare il mandato di perquisizione su dati provenienti dall'estero. In particolare, la Corte ha attribuito particolare importanza al fatto che all'epoca dell'emissione del mandato di perquisizione, la serie di dati pertinenti era una delle poche acquistate dalle autorità tedesche (ibid., § 51). Né il mero fatto che non esista una regola assoluta secondo la quale le prove che sono state acquisite in violazione delle regole procedurali non possono essere utilizzate nei procedimenti penali, comporta che le autorità abbiano ottenuto deliberatamente i dati in violazione del diritto internazionale o del diritto interno (ibid., § 51). Inoltre, il supporto informatico dei dati conteneva informazioni concernenti la situazione finanziaria dei ricorrenti, che essi erano obbligati a presentare alle autorità tributarie nazionali, ma nessun dato strettamente legato alla loro identità (ibid., § 53; si raffronti *G.S.B. c. Svizzera*, 2015, § 93, concernente la trasmissione di dati bancari alle autorità tributarie di un altro Stato ai sensi di un accordo bilaterale).

167. Le perquisizioni condotte nei locali di un'impresa, finalizzate a raccogliere prove reali sollevano questioni relative alla protezione dei suoi dati, sotto il profilo del diritto al rispetto della sua "corrispondenza" e del suo "domicilio", garantiti ai sensi dell'articolo 8. Per esempio, nella causa *Bernh*

Larsen Holding AS e altri c. Norvegia, 2013 (§§ 104-175) la Corte non ha riscontrato alcuna violazione dell'articolo 8 in relazione a una decisione che ordinava a una società di fornire una copia integrale di tutti i dati del server informatico che essa condivideva con altre società. Benché non fosse prevista alcuna preliminare autorizzazione giudiziaria, la Corte ha tenuto conto delle garanzie effettive e adeguate contro gli abusi, degli interessi sia delle società che dei loro dipendenti, e dell'interesse pubblico a un controllo fiscale efficace (ibid., §§ 172-175). Per contro, la Corte ha rilevato la violazione dell'articolo 8 nella causa *DELTA PEKÁRNY a.s. c. Repubblica ceca*, 2014 (§§ 92-93), concernente un'ispezione nei locali di un'impresa, finalizzata a ottenere le prove dell'esistenza di un accordo illegale sui prezzi in violazione delle norme in materia di concorrenza. La Corte ha rinviato all'assenza di una preliminare autorizzazione da parte di un giudice, di un effettivo riesame *post hoc* della necessità della misura e della regolamentazione della eventuale distruzione dei dati ottenuti.

168. Nella causa *Buck c. Germania*, 2005 (§§ 30-53), la perquisizione dei locali professionali e residenziali del ricorrente in relazione a un reato in materia di circolazione stradale, commesso da un terzo, aveva costituito violazione dell'articolo 8. Tenuto conto delle particolari circostanze della causa, in particolare del fatto che la perquisizione e il sequestro in questione erano stati disposti in relazione a una lieve violazione di un regolamento, commessa presumibilmente da un terzo e che essi concernevano i locali residenziali privati del ricorrente, la Corte ha concluso che l'ingerenza non potesse essere considerata proporzionata ai fini legittimi perseguiti (ibid., § 52).

169. Riguardo alle perquisizioni dei locali professionali di giornalisti, dei loro domicili e delle loro automobili private (in alcuni casi), e dei sequestri in massa, ai fini di individuare le loro fonti, la Corte ha riscontrato la violazione dell'articolo 8 nella causa *Ernst e altri c. Belgio*, 2003 (§§ 110-117). In relazione alle azioni per lottare contro le violazioni della segretezza delle indagini giudiziarie, la legislazione e la prassi degli Stati contraenti, che possono prevedere le perquisizioni domiciliari e i sequestri domiciliari, devono prevedere garanzie adeguate e sufficienti contro gli abusi. Nel caso di specie la situazione era stata differente, poiché non erano state formulate accuse nei confronti dei ricorrenti e i vari mandati di perquisizione erano stati redatti in termini ampi, senza fornire informazioni sull'indagine contestata, sui precisi locali che dovevano essere perquisiti o sugli oggetti che dovevano essere sequestrati, lasciando quindi agli investigatori ampi spazi di manovra. Inoltre, i ricorrenti non erano mai stati informati dei reali motivi delle perquisizioni (si veda altresì il paragrafo 327 *infra* concernente la violazione dell'articolo 10 in questa causa).

170. Per quanto riguarda i sequestri svolti negli studi legali, essi devono essere sempre accompagnati da particolari garanzie processuali in grado di proteggere la riservatezza dei dati che è alla base del rapporto di fiducia tra un avvocato e il suo assistito[8]. Nella causa *Kırdök e altri c. Turchia*, 2019 (§§ 52-58), il sequestro dei dati elettronici di diversi avvocati da parte delle autorità giudiziarie, ai fini del procedimento penale nei confronti di un altro avvocato, che condivideva lo studio di tali avvocati, e il rifiuto di restituire i dati o di distruggerli avevano costituito violazione dell'articolo 8. La Corte ha attribuito importnza al fatto che, nel corso della perquisizione, non fosse stata notata alcuna procedura di filtraggio dei documenti elettronici o dei dati tutelati dal segreto professionale. Inoltre, il rifiuto di consegnare i dati sequestrati in quanto poiché essi non erano stati ancora trascritti non vi era modo di accertare a chi appartenessero, non era chiaramente prescritto dalla legge e violava l'essenza stessa del segreto professionale, che esigeva la riservatezza di tali dati.

171. Nella causa *Kruglov e altri c. Russia*, 2020 (§§ 123-138), la Corte ha stabilito che i sequestri di computer e di hard drive contenenti informazioni personali e documenti tutelati dal segreto professionale dei ricorrenti, che erano avvocati di professione, o dei loro assistiti, durante le perquisizioni condotte dalla Polizia nelle loro abitazioni e nei loro uffici, senza alcun filtraggio dei dati sequestrati, avevano violato l'articolo 8. In particolare, l'esistenza di una preliminare autorizzazione

[8] Si veda altresì la Guida all'articolo 8 della Convenzione (diritto al rispetto della vita privata e familiare) per ulteriori dettagli sulle garanzie procedurali applicabili ai sequestri svolti negli studi legali.

giudiziaria ha un effetto limitato, in quanto i tribunali nazionali non hanno mai tentato di bilanciare l'obbligo di proteggere la riservatezza dei dati e le esigenze delle indagini penali, per esempio esaminando la possibilità di ottenere informazioni da altre fonti (ibid. , §§ 126-129).

172. La Corte ha riscontrato la violazione dell'articolo 8 anche nella causa *Smirnov c. Russia*, 2007 (§§ 36-49), concernente la perquisizione e il sequestro di numerosi documenti e dell'unità centrale del computer di un avvocato, nell'abitazione dell'avvocato, senza alcuna giustificazione o garanzia; nella causa *Wieser and Bicos Beteiligungen GmbH c. Austria*, 2007 (§§ 42-68), concernente le perquisizioni e il sequestro dei dati elettronici di un avvocato in violazione delle garanzie processuali previste dalla legge; nella causa *Robathin c. Austria*, 2012 (§ 52), relativa un'autorizzazione di perquisizione e sequestro di tutti i dati elettronici memorizzati in uno studio legale, motivata in modo insufficiente; e nella causa *Särgava c. Estonia*, 2021 (§§ 107-108), concernente le garanzie processuali che sono state considerate insufficienti a proteggere i dati tutelati dal segreto professionale successivamente al sequestro e poi all'esame del computer e del telefono cellulare di un avvocato.

173. Nella causa *Vinci Construction et GTM Génie Civil et Services c. Francia*, 2015 (§§ 69-81), la Corte ha riscontrato la violazione dell'articolo 8 in relazione al sequestro e alla perquisizione di dati informatici appartenenti a delle società, tra cui messaggi elettronici tutelati dalla riservatezza dei rapporti tra un difensore e un suo assistito. Il Tribunale di primo grado, pur riconoscendo la presenza della corrispondenza di un avvocato tra i documenti sequestrati dagli inquirenti, aveva meramente valutato la legittimità del quadro formale dei sequestri contestati, senza svolgere il necessario esame particolareggiato.

174. Nella causa *André e altri c. Francia*, 2008 (§§ 37-49), una perquisizione "domiciliare" e il sequestro di documenti in uno studio legale da parte di agenti del fisco, al fine di ottenere prove contro una società sua cliente aveva costituito violazione dell'articolo 8. La perquisizione in questione era finalizzata a scoprire presso i ricorrenti, puramente nella loro qualità di avvocati della società sospettata di frode, documenti in grado di stabilire l'esistenza di tale frode da parte della società e di utilizzare tali documenti come prove contro di essa. I ricorrenti non erano stati accusati o sospettati in alcuna fase di avere commesso un reato, o di essere coinvolti nella frode commessa dalla società loro cliente (ibid., § 46).

175. Un secondo sequestro, effettuato cinque minuti dopo la restituzione di materiale confiscato illegalmente, aveva costituito violazione dell'articolo 8 nella causa *Visy c. Slovacchia*, 2018 (§§ 33-47). Il ricorrente era stato privato di qualsiasi effettiva garanzia contro le arbitrarietà e gli abusi in relazione al secondo sequestro.

176. Nella causa *Sher a altri c. Regno Unito*, 2015 (§§ 171-176), in materia di terrorismo, la Corte ha dovuto esaminare la questione di un mandato di perquisizione estendibile in casi di sospetto di attività terroristiche. La Corte ha ritenuto che la complessità inerente a tali casi potesse giustificare una perquisizione basata su termini più ampi di quelli che sarebbero stati diversamente ammissibili. Imporre ai sensi dell'articolo 8 l'obbligo che il mandato di perquisizione individui dettagliatamente la la precisa natura degli oggetti che devono essere ricercati e sequestrati potrebbe compromettere gravemente l'efficacia di un'indagine, nella quale potrebbero essere in gioco numerose vite. In casi di questa natura, deve essere permessa alla Polizia una certa elasticità per valutare, sulla base di quanto scoperto durante la perquisizione, quali oggetti potrebbero essere connessi alle attività terroristiche e per sequestrarli al fine di un ulteriore esame (ibid., § 74).

177. Nella causa *Ivashchenko c. Russia*, 2018 (§§ 59-95), i poteri delle autorità doganali di consultare e copiare i dati elettronici delle persone avevano costituito violazione dell'articolo 8, data l'assenza di ragionevoli sospetti della commissione di irregolarità. La copiatura dei dati personali e professionali del ricorrente, seguita dalla comunicazione degli stessi al fine di una perizia, e la conservazione di tali dati per circa due anni, aveva ecceduto quelle che avrebbero potuto essere considerate delle procedure di "routine" non invasive, per le quali era generalmente prestato il consenso. Il ricorrente non era stato in grado di scegliere se desiderasse presentare sé stesso e i suoi beni alla dogana e a

un'eventuale ispezione doganale. (Si veda altresì *Gillan e Quinton c. Regno Unito,* 2010, §§ 61-67, concernente i poteri di fermare e perquisire le persone senza alcun motivo plausibile di sospettare che esse avessero commesso un reato, che costituiva violazione dell'articolo 8. La Corte ha sottolineato che la natura pubblica della perquisizione, durante la quale il fatto di esporre informazioni personali ad altre persone causava imbarazzo, poteva perfino, in alcuni casi, aggravare la gravità dell'ingerenza nella vita privata della persona, a causa dell'elemento dell'umiliazione e dell'imbarazzo. La discrezionalità di cui godevano gli agenti della Polizia era una fonte di preoccupazione: non soltanto essi non erano tenuti a dimostrare l'esistenza di un plausibile sospetto, ma essi non erano tenuti neanche a sospettare soggettivamente nulla riguardo alla persona fermata e perquisita).

ii. Interventi medici obbligatori ai fini del prelievo di campioni cellulari

178. In generale, l'utilizzo di vari interventi medici obbligatori ai fini del prelievo di campioni cellulari, quali le analisi ematiche e i campioni salivari, non era di per sé proibito nell'ambito dell'acquisizione di prove nei procedimenti civili o penali (*Caruana c. Malta* (dec.), 2018, § 41).

179. Nella causa *Mikulić c. Croazia*, 2002 (§ 64), la Corte ha ritenuto che l'assenza di qualsiasi misura procedurale per obbligare il presunto padre a sottoporsi all'esame del DNA fosse conforme al principio di proporzionalità soltanto se erano previsti mezzi alternativi per determinare la domanda di accertamento della paternità. La Corte ha riscontrato la violazione dell'articolo 8 in quanto il diritto interno non prevedeva tali mezzi, condannando quindi la ricorrente a un'ulteriore prolungata incertezza riguardo alla sua identità personale, a causa del rifiuto del suo presunto padre di sottoporsi all'esame del DNA (ibid., §§ 65-66).

180. Nella causa *Mifsud c. Malta*, 2019 (§§ 61-78), un decreto giudiziario emesso nei confronti del ricorrente che disponeva che si sottoponesse contro la sua volontà a un test genetico, nell'ambito di un procedimento per l'accertamento della paternità, ai sensi del diritto maltese, non aveva violato l'articolo 8. Prima di ordinare al ricorrente di sottoporsi all'esame del DNA, i giudici nazionali avevano effettuato la necessaria ponderazione degli interessi concorrenti nella causa, nell'ambito di un procedimento giudiziario al quale il ricorrente aveva partecipato, rappresentato da un difensore di propria scelta, e nel quale i suoi diritti processuali erano stati rispettati su un piano di parità con la parte avversaria. I giudici nazionali erano pervenuti a un giusto equilibrio tra l'interesse della presunta figlia del ricorrente a ottenere l'accertamento della paternità e quello del ricorrente a non sottoporsi all'esame del DNA (ibid., § 77). Il processo decisionale era stto complessivamente equo e aveva tutelato debitamente gli interessi del ricorrente, garantiti dall'articolo 8.

181. Nella causa *Boljević c. Serbia*, 2020 (§§ 50-56), la Corte ha stabilito che il rigetto per prescrizione da parte dei giudici nazionali di una domanda di riesame di una decisione definitiva emessa quarantuno anni prima, che accoglieva l'azione di un uomo che contestava la paternità, in un'epoca in cui l'esame del DNA non esisteva ancora, avesse violato l'articolo 8. La Corte ha ritenuto che la salvaguardia della certezza giuridica non potesse costituire di per sé un motivo sufficiente per privare il ricorrente del diritto di conoscere la verità su un importante aspetto della sua identità personale, senza soppesare gli interessi concorrenti nella causa. La legislazione interna in materia di termini per la riapertura di un procedimento aveva impedito alle autorità di compiere tale ponderazione, tenuto conto delle circostanze molto particolari del caso del ricorrente, vale a dire che il ricorrente aveva appreso della sentenza definitiva concernente la paternità del suo presunto padre soltanto successivamente al decesso di quest'ultimo. La Corte ha ritenuto che la vita privata di un defunto non possa essere compromessa da una domanda di prelievo di un campione del DNA, presentata successivamente al suo decesso. La Corte era pervenuta precedentemente alla medesima decisione nella causa *Succession Kresten Filtenborg Mortensen c. Danimarca* (dec.), 2006, concernente l'esumazione di una salma al fine di eseguire esami genetici, e *Jäggi c. Svizzera*, 2006 (§ 42), in cui il rifiuto da parte dei giudici di autorizzare l'esame del DNA di una persona deceduta richiesto dall'asserito figlio di quest'ultima, al fine di accertare l'identità del padre biologico aveva costituito violazione dell'articolo 8 (ibid., §§ 34-44).

182. Nella causa *Caruana c. Malta* (dec.), 2018 (§§ 28-42), la Corte ha dichiarato manifestamente infondata una doglianza relativa all'obbligo imposto alla moglie di un presunto omicida di fornire dei campioni salivari. La Corte ha ritenuto che il prelievo di un campione salivare fosse un lieve intervento, che causava raramente lesioni personali o sofferenza fisica o mentale. L'omicidio era in grave reato, e quindi era sia ragionevole che necessario raccogliere quante più prove possibile (ibid., § 41). La Corte ha inoltre operato una distinzione tra la situazione di un testimone e quella di un imputato, il cui rifiuto di sottoporsi a una simile misura nell'ambito di un procedimento penale avrebbe potuto incidere sulla eventuale dichiarazione di colpevolezza e sulle sanzioni connesse (ibid., § 40).

183. Nella causa *Dragan Petrović c. Serbia*, 2020 (§§ 79-84), il prelievo di un campione salivare nell'ambito di un'indagine per omicidio aveva costituito violazione dell'articolo 8, a causa dell'assenza di disposizioni giuridiche prevedibili. Il fatto che il ricorrente avesse accettato di consegnare un campione della sua saliva agli agenti della Polizia non aveva rilevanza al fine di stabilire se egli avesse subito un'ingerenza nella sua vita privata o meno, in quanto egli lo aveva fatto soltanto perché era stato minacciato che altrimenti gli sarebbe stato prelevato con la forza un campione salivare o ematico (ibid., § 79).

184. La Corte ha riscontrato la violazione dell'articolo 8 in caso di raccolta di dati medici di Testimoni di Geova che avevano rifiutato trasfusioni di sangue (*Avilkina e altri c. Russia*, 2013); si veda altresì il paragrafo 188 supra.

185. Violazioni dell'articolo 8 sono state constatate anche in caso di espianto di organi dai corpi di persone decedute ai fini del trapianto senza il consenso e all'insaputa dei prossimi congiunti della persona deceduta (*Petrova c. Lettonia*, 2014, §§ 87-98), e in una situazione di imprecisione della legislazione interna in materia di consenso dei prossimi congunti al prelievo di tessuti dal corpo di una persona deceduta (*Elberte c. Lettonia*, 2015, §§ 105-117).

d. Raccolta di dati personali in ambito medico

186. La Corte ha trattato la questione della raccolta di dati sensibili in ambito medico. Nella causa *L.H. c. Lettonia*, 2014 (§§ 47-60), la raccolta dei dati medici di un paziente di un ospedale pubblico da parte di un organismo statale ("l'organismo") responsabile del controllo della qualità delle cure mediche è stata considerata non conforme all'articolo 8, in assenza di una legislazione formulata con precisione che offrisse un'adeguata tutela giuridica contro le arbitrarietà. L'organismo aveva raccolto i dati in questione per un periodo di sette anni, indiscriminatamente, senza alcuna precedente valutazione volta a stabilire se i dati sarebbero stati "potenzialmente determinanti", "pertinenti" o "importanti" per raggiungere l'obiettivo dell'indagine. L'organismo non era tenuto a chiedere e a ottenere il consenso del ricorrente alla raccolta dei suoi dati (ibid., § 53). La portata dei dati privati che potevano essere raccolti non era limitata in alcun modo (ibid., § 57). Inoltre, non sembrava che la pertinenza e la sufficienza dei motivi per raccogliere le informazioni fossero state esaminate in alcuna fase dei procedimenti interni (ibid., § 57). In tale contesto, la Corte ha ritenuto che fosse meno pertinente stabilire se l'organismo avesse o meno un obbligo legale di mantenere la riservatezza dei dati personali (ibid., § 58).

187. Nella causa *Surikov c. Ucraina*, 2017 (§§ 75-95), la raccolta e la conservazione di dati personali concernenti la salute mentale di una persona per un protratto periodo, nonché la comunicazione e l'utilizzo di tali dati per un fine non connesso con gli iniziali motivi della loro raccolta, avevano costituito un'ingerenza sproporzionata nel diritto dell'interessato al rispetto della sua vita privata, in violazione dell'articolo 8. Benché i datori di lavoro potessero avere un legittimo interesse a ottenere informazioni concernenti la salute mentale e fisica dei loro dipendenti, in particolare nell'ambito dell'assegnazione a essi di determinate funzioni lavorative connesse a specifiche abilità, responsabilità o competenze, la raccolta e il trattamento delle informazioni pertinenti dovevano essere leciti e tali da conseguire un giusto equilibrio tra gli interessi del datore di lavoro e le preoccupazioni relative alla vita privata del candidato al pertinente posto (ibid., § 91).

188. Nella causa *Z c. Finlandia*, 1997 (§§ 106-110), la Corte non ha riscontrato alcuna violazione dell'articolo 8 relativamente al sequestro di cartelle cliniche e al loro inserimento nel fascicolo investigativo senza il preliminare consenso della paziente, nell'ambito di un procedimento penale nei confronti di suo marito. Non vi era stata alcuna irregolarità nel processo decisionale, ed esistevano dei ricorsi per impugnare il sequestro e annullare il termine indicato nel decreto relativo alla riservatezza.

189. La causa *Drelon c. Francia*, 2022 (§§ 79-100) concerneva il tentativo del ricorrente di donare il sangue in un luogo di raccolta del Servizio francese di donazione del sangue e il rifiuto di quest'ultimo di accettarlo quale donatore di sangue sulla base della sua presunta omosessualità. Benché il ricorrente avesse rifiutato di rispondere a domande relative alla sua vita sessuale durante la visita medica preliminare alla donazione, i dati comprendevano la specifica controindicazione alla donazione del sangue da parte di uomini che avevano avuto rapporti sessuali con altri uomini. Avendo preso atto della natura sensibile dei suddetti dati, la Corte ha ammesso che la raccolta e la conservazione di essi fossero basati su motivi pertinenti e sufficienti, vale a dire la protezione della salute e l'importanza di assicurare la sicurezza del sangue. Al medesimo tempo, essa ha osservato che i dati raccolti erano basati su una mera congettura priva di qualsiasi base fattuale dimostrata. Ha rilevato anche l'eccessiva durata della conservazione dei dati, che permetteva che i dati fossero utilizzati ripetutamente nei confronti del ricorrente, comportando la sua automatica esclusione dalla donazione del sangue. Rinviando a tali elementi, la Corte ha constatato la violazione dell'articolo 8 della Convenzione.

e. Comunicazione obbligatoria di dati personali

190. La Corte ha valutato in diverse occasioni l'obbligo degli operatori di telefonia mobile, dei fornitori di servizi internet, delle banche, degli atleti di alto livello, e degli ospedali di fornire alle autorità i dati personali di cui sono in possesso ai sensi di una legge o di un decreto emesso dalle autorità.

191. Quanto all'azione di contrasto della criminalità organizzata e del terrorismo, la Corte ha ammesso che i metodi investigativi devono essere adattati alla moderna tecnologia delle comunicazioni. Nella causa *Breyer c. Germania*, 2020 (§§ 81-110), l'obbligo legale per gli operatori di telefonia mobile di registrare i dati personali degli utenti di carte SIM prepagate e di metterli a disposizione delle autorità, ai sensi della Legge sulle telecomunicazioni, che autorizzava varie autorità pubbliche a chiedere l'estrazione e la comunicazione di tali dati senza alcuna necessità di una decisione giudiziaria o di una notifica alle persone interessate, non è stata ritenuta contraria all'articolo 8. Era stata memorizzata soltanto una limitata quantità di dati e non era stato memorizzato alcun dato concernente comunicazioni individuali; l'ingerenza era stata pertanto veramente minima (ibid., §§ 92-95). Vi erano state anche diverse garanzie: l'assicurazione della sicurezza tecnica, la limitata durata della memorizzazione, la limitazione dei dati alle informazioni necessarie per individuare chiaramente l'abbonato in questione; le possibilità di una futura consultazione e utilizzazione dei dati memorizzati; la sorveglianza da parte di un'autorità indipendente; e le possibilità di ricorso per chiunque ritenesse che fossero stati violati i suoi diritti, benché il livello di riesame e di controllo non fossero un elemento decisivo nella valutazione della proporzionalità della raccolta e della memorizzazione di un insieme di dati così limitato (ibid. , §§ 96-107).

192. Per contro, la Corte ha ritenuto che l'imposizione dell'obbligo legale ai fornitori di servizi internet di estrarre i dati di connessione memorizzati di un loro abbonato e di trasmetterli alla Polizia costituisse violazione dell'articolo 8 in quanto le disposizioni giuridiche invocate dalla Polizia non erano chiare e non fornivano alcuna protezione contro un'ingerenza arbitraria, in particolare in assenza di un controllo indipendente dei poteri della Polizia in questione (*Benedik c. Slovenia*, 2018, §§ 132-134).

193. Nella causa *Sommer c. Germania*, 2017 (§ 63), l'ispezione di un conto bancario di un avvocato aveva costituito violazione dell'articolo 8 in considerazione della soglia minima necessaria per ispezionare il conto bancario del ricorrente, dell'ampia portata delle domande di informazione, della successiva divulgazione e della continua memorizzazione delle informazioni personali del ricorrente, nonché dell'insufficienza delle garanzie procedurali.

194. Nella causa *Avilkina e altri c. Russia*, 2013 (§ 54), concernente la raccolta di dati medici relativi a dei Testimoni di Geova che avevano rifiutato le trasfusioni di sangue, la Corte ha ritenuto che la raccolta da parte degli inquirenti dei dati dei ricorrenti presso l'istituto sanitario che li aveva curati, senza informare gli interessati o dare loro la possibilità di opporsi, fosse stata incompatibile con l'articolo 8. La Procura aveva avuto altre possibilità per dare seguito alle denunce che le erano state presentate nei confronti dell'organizzazione religiosa in questione, quali l'interrogatorio delle persone interessate o la richiesta del loro consenso (ibid., § 48).

195. Nella causa *National Federation of Sportspersons' Associations and Unions (FNASS) e altri c. Francia*, 2018 (§§ 155-191), l'obbligo legale di reperibilità imposto ad atleti di alto livello facenti parte di un "gruppo sottoposto a controllo", al fine di svolgere test antidoping senza preavviso nell'ambito della lotta contro il doping, che comportava pesanti sanzioni in caso di inosservanza entro un periodo di diciotto mesi consecutivi, non è stato considerato contrario all'articolo 8. Senza sottovalutare l'impatto dell'obbligo della reperibilità sulla vita privata dei ricorrenti, la Corte ha ritenuto che la riduzione o l'eliminazione degli obblighi imposti ad atleti di alto livello avrebbe potuto comportare l'aumento dei pericoli del doping per la loro salute e per quella dell'intera comunità sportiva, e avrebbe contrastato con l'unanimità europea e internazionale riguardo alla necessità di esami senza preavviso (ibid. , § 191).

196. Nella causa *Aycaguer c. Francia*, 2017 (§§ 45-47), la Corte ha riscontrato la violazione dell'articolo 8, in quanto la condanna penale del ricorrente per avere rifiutato di sottoporsi a un esame biologico obbligatorio al fine di registrare il profilo del suo DNA nella banca dati computerizzata delle persone condannate, non poteva essere considerata una misura necessaria in una società democratica. Il ricorrente aveva compiuto le azioni che avevano condotto all'ordine di sottoporsi a un esame obbligatorio del DNA in un contesto politico/sindacale, esse riguardavano semplici ombrellate dirette contro dei gendarmi che non erano stati identificati, per le quali era stato condannato a due mesi di reclusione, con la sospensione della pena. La banca dati nazionale computerizzata del DNA non prevedeva tuttavia alcuna differenziazione sulla base della gravità del reato commesso, nonostante la notevole disparità delle situazioni che potevano potenzialmente sorgere, come dimostra la situazione del ricorrente (ibid., § 43). Infine, il ricorrente non aveva avuto accesso a una procedura per cancellare i dati memorizzati (tale procedura era prevista soltanto per le persone sospettate di un reato, e non per le persone già condannate) (ibid., § 43).

2. Conservazione di dati personali

197. La memorizzazione da parte di un'autorità pubblica di informazioni relative alla vita privata di un individuo, a prescindere dalla modalità di ottenimento di tali informazioni, costituisce un'ingerenza nel diritto al rispetto della vita privata della persona interessata ai sensi dell'articolo 8, indipendentemente dal fatto che i dati siano successivamente utilizzati o meno (*Amman c. Svizzera* [GC], 2000, § 69; *Rotaru c. Romania* [GC], 2000, § 46; *S. e Marper c. Regno Unito* [GC], 2008, § 67; *M.K. c. Francia*, 2013, § 29; *Aycaguer c. Francia*, 2017 § 33). Il carattere intrinsecamente privato di tali informazioni esige che la Corte svolga un rigoroso esame di qualsiasi misura statale che ne autorizza la conservazione e l'utilizzo da parte delle autorità senza il consenso della persona interessata (*S. e Marper c. Regno Unito* [GC], 2008, § 104).

a. Memorizzazione di dati personali al fine della prevenzione dei reati

198. L'interesse delle persone interessate e della comunità nel suo insieme a proteggere i dati personali, tra cui le impronte digitali e le informazioni relative al DNA, può essere superato dall'interesse legittimo di prevenire i reati (*S. e Marper c. Regno Unito* [GC], 2008, § 104). Al fine di proteggere come devono la loro popolazione, le autorità nazionali possono istituire legittimamente delle banche dati come mezzo effettivo per contribuire a punire e a prevenire determinati reati, compresi quelli di tipo più grave, quali i reati sessuali (*B.B. c. Francia*, 2009, § 62; *Gardel c. Francia*,

2009, § 63; *M.B. c. Francia,* 2009, § 54). Mentre l'iniziale acquisizione di tali informazioni persegue il fine di collegare una particolare persona al particolare reato della quale è sospettata, la loro conservazione persegue il fine più ampio di facilitare l'identificazione di futuri delinquenti (*S. e Marper c. Regno Unito* [GC], 2008, § 100). La Corte non può mettere in discussione il fine preventivo di tali registri (*Gardel c. Francia*, 2009, § 63; *B.B. c. Francia*, 2009, § 62; *M.B. c. Francia,* 2009, § 54). La lotta contro la criminalità, e in particolare contro la criminalità organizzata e il terrorismo, che è una delle sfide che affrontano attualmente le società europee, dipende in larga misura dall'utilizzo di moderne tecniche scientifiche di indagine e di identificazione (*S. e Marper c. Regno Unito* [GC], 2008, § 105). Al medesimo tempo, poiché la protezione dei dati personali è di fondamentale importanza per il godimento da parte di una persona del suo diritto al rispetto della vita privata e familiare, garantito dall'articolo 8 della Convenzione, il diritto interno deve offrire garanzie adeguate per impedire qualsiasi utilizzo dei dati personali incompatibile con le garanzie di questo articolo (ibid. , § 103).

199. La Corte ha esaminato diverse cause relative alla registrazione in banche dati finalizzate alla repressione e alla prevenzione dei reati dei dati personali di persone condannate per reati di lieve entità (*M.K. c. Francia*, 2013, §§ 6, 8, 41; *Aycaguer c. Francia*, 2017, §§ 8, 43), per gravi reati (*B.B. c. Francia*, 2009, §§ 6, 62; *Gardel c. Francia*, 2009, §§ 8, 9, 63; *M.B. c. Francia,* 2009, §§ 6, 54; *Peruzzo e Martens c. Germania* (dec.), 2013, §§ 6, 12, 37-38; *Trajkovski e Chipovski c. Macedonia del Nord*, 2020, §§ 6, 12), o per reati che non erano né di lieve entità né particolarmente gravi (*P.N. c. Germania*, 2020, §§ 6, 81). Altre cause riguardavano la memorizzazione, in banche dati finalizzate alla repressione e alla prevenzione dei reati, dei dati personali di individui che erano stati sospettati della commissione di reati, ma che erano stati infine prosciolti (*S. e Marper c. Regno Unito* [GC], 2007, §§ 10, 11, 113; *M.K. c. Francia*, 2013, §§ 7, 9, 42; *Brunet c. Francia*, 2014, §§ 6, 7, 40), assolti (*S. e Marper c. Regno Unito* [GC], 2008, §§ 10, 113), o semplicemente ammoniti dopo il procedimento, senza riportare condanne (*M.M. c. Regno Unito*, 2012, §§ 7-9). Infine, altre cause riguardavano le misure preventive che comportavano la memorizzazione di dati personali negli archivi della Polizia, sulla base di meri sospetti (*Shimovolos c. Russia*, 2011, § 16; *Khelili c. Svizzera*, 2011, §§ 8, 9, 59; *Catt c. Regno Unito*, 2019, §§ 6, 14, 119).

200. I fattori esposti in prosieguo sono importanti nell'esame della necessità di memorizzare dati personali per fini di polizia.

i. Indiscriminata e indifferenziata natura dei dati memorizzati

201. In diverse cause la Corte ha messo in discussione l'ampia portata del regime di memorizzazione dei dati istituito dalle autorità, che non aveva operato una distinzione sulla base della natura o del livello di gravità del reato che aveva dato luogo alla condanna (*M.K. c. Francia*, 2013, § 41; *Aycaguer c. Francia,* 2017, § 43; *Gaughran c. Regno Unito*, 2020, § 94), o a seconda del fatto che la persona interessata fosse stata condannata, assolta, prosciolta o semplicemente ammonita, dopo essere stata sospettata della commissione di un reato (*S. e Marper c. Regno Unito* [GC], 2008, § 119; *M.M. c. Regno Unito*, 2012, § 198; *M.K. c. Francia*, 2013, § 42*; Brunet c. Francia*, 2014, § 41). La Corte ritiene che i dispositivi predisposti dalle autorità per contribuire alla repressione e alla prevenzione di alcuni reati non possano essere attuati nell'ambito di un eccessivo sforzo per massimizzare le informazioni memorizzate in essi. Invero, senza il rispetto della necessaria proporzionalità nei confronti degli obiettivi legittimi attribuiti a tali meccanismi, i vantaggi che essi presentano sarebbero superati dalle gravi violazioni che causerebbero ai diritti e alle libertà che gli Stati devono garantire ai sensi della Convenzione alle persone sottoposte alla loro giurisdizione (*M.K. c. Francia,* 2013, § 35 ; *Aycaguer c. Francia,* 2017, § 34).

202. Nella causa *S. e Marper c. Regno Unito* [GC], 2008 (§§ 119, 125), una banca dati in cui era possibile raccogliere e memorizzare impronte digitali, campioni biologici e profili del DNA di qualsiasi persona sospettata, ma non condannata, per dei reati, a prescindere dall'età, dalla natura e dalla gravità dei reati, senza un termine o un riesame indipendente della giustificazione della conservazione dei dati sulla base di criteri definiti, aveva dato luogo alla constatazione di violazione dell'articolo 8. Il

carattere generale e indiscriminato di tale regime non rispecchiava un giusto equilibrio tra i concorrenti interessi pubblici e privati in gioco.

203. Vi è un rischio di stigmatizzazione se persone che non sono state condannate per un reato e che hanno diritto alla presunzione di innocenza sono trattate allo stesso modo di persone condannate (*S. e Marper c. Regno Unito* [GC], 2008, § 122). Benché la conservazione di dati privati concernenti persone sospettate di un reato, ma che sono state assolte o prosciolte, non possa essere equiparata all'espressione di sospetti, l'impressione che esse hanno di non essere trattate come se fossero innocenti è rafforzata dal fatto che i loro dati sono conservati a tempo indeterminto allo stesso modo dei dati relativi alle persone condannate, mentre i dati relativi alle persone che non sono mai state sospettate di un reato devono essere distrutti (ibid., § 122). Pertanto, il fatto che una persona abbia beneficiato di una scarcerazione dopo essere stata sospettata di un reato giustifica che sia trattata in modo diverso da una persona condannata (ibid., § 122; si veda altresì, nel medesimo senso, *M.K. c. Francia*, 2013, § 42; *Brunet c. Francia*, 2014, § 40). Pertanto, nella causa *Brunet c. Francia*, 2014 (§ 40), in cui il ricorrente aveva beneficiato di una decisione di archiviazione successivamente a una mediazione, la Corte ha messo in discussione la natura indiscriminata dei dati personali registrati negli archivi delle autorità, senza operare alcuna distinzione tra le persone condannate e quelle che avevano beneficiato di un'archiviazione. Nella causa *Aycaguer c. Francia,* 2017 (§§ 42-43), in cui i dati personali erano stati raccolti e conservati a seguito di una condanna per reati che non erano particolarmente gravi, la Corte ha messo in discussione l'ampia portata della raccolta di dati personali da parte delle autorità, che non avevano operato alcuna distinzione sulla base del livello di gravità del reato che aveva dato luogo alla condanna, nonostante l'ampia gamma di situazioni suscettibili di sorgere nell'ambito dell'applicazione della legge. Secondo la Corte gli atti che avevano dato luogo alla condanna del ricorrente, delle mere ombrellate dirette contro dei gendarmi in un contesto politico/sindacale, non erano paragonabili agli atti classificati come reati particolarmente gravi, quali i reati sessuali, il terrorismo, i crimini contro l'umanità o la tratta di esseri umani.

204. Nella causa *M.M. c. Regno Unito*, 2012 (§§ 187-207), la registrazione a vita nel casellario giudiziale di un ammonimento relativo a una persona, dopo che la stessa era scomparsa per un giorno con il nipote, un bambino, sperando di impedire la sua partenza per l'Australia successivamente alla rottura del matrimonio di suo figlio, aveva dato luogo alla constatazione di violazione dell'articolo 8. La Corte ha contestato la portata estremamente ampia del regime di conservazione dei dati, comprendente non soltanto le condanne bensì anche decisioni diverse dalle condanne quali gli avvisi, gli ammonimenti e le reprimende, nonché una notevole quantità di dati supplementari registrati dalla polizia in virtù di una direttiva generale che prevedeva che i dati dovessero essere conservati fino al compimento del centesimo anno da parte della oersona interessata (ibid., § 202). La Corte ha ritenuto che quanto più era ampia la portata del regime di conservazione, e quindi quanto più era ampia la quantità e la sensibilità dei dati conservati e che potevano essere rivelati, tanto più era importante il contenuto delle garanzie che dovevano essere applicate nelle varie fasi cruciali del successivo trattamento dei dati (ibid., § 200). Lo stesso valeva per la causa *Gaughran c. Regno Unito,* 2020 (§§ 94-97), concernente la memorizzazione a tempo indeterminato dei dati biometrici e delle fotografie del ricorrente, condannato per guida in stato di ebrezza, che aveva costituito violazione dell'articolo 8.

205. La conservazione dei dati di persone non condannate può essere particolarmente nociva se si tratta di minori, data la loro particolare situazione e l'importanza del loro sviluppo e della loro integrazione nella società. Dovrebbe essere prestata particolare attenzione alla protezione dei minorenni da qualsiasi pregiudizio di tale tipo (*S. e Marper c. Regno Unito* [GC], 2008, § 124).

ii. Periodo di conservazione dei dati

206. La durata del periodo per il quale le autorità decidono di memorizzare i dati personali di una persona è un aspetto importante, benché non determinante, di cui tenere conto nel valutare se la memorizzazione di dati personali in un registro o in una banca dati per fini di polizia sia proporzionata,

o meno, al fine legittimo perseguito. La Corte ha riscontrato violazioni dell'articolo 8 in cause concernenti:

- la memorizzazione a tempo indeterminato delle impronte digitali e dei dati del DNA di persone sostettate di un reato, ma i cui procedimenti si erano conclusi con una decisione di archiviazione o con un'assoluzione (*S. e Marper c. Regno Unito* [GC], 2008);
- la memorizzazione a tempo indeterminato dei profili del DNA, delle impronte digitali e delle fotografie di una persona riconosciuta colpevole di un reato, anche dopo che la sua condanna era stata cancellata dal casellario giudiziale allo scadere del termine previsto dalla legge (*Gaughran c. Regno Unito*, 2020);
- la conservazione a vita in un casellario giudiziale di qualsiasi condanna, assoluzione, ammonimento, avviso e reprimenda relativi a una persona (*M.M. c. Regno Unito*, 2012);
- la memorizzazione a tempo indeterminato dei profili del DNA di persone condannate per furto aggravato (*Trajkovski e Chipovski c. Macedonia del Nord*, 2020);
- la conservazione per un massimo di quaranta anni dei dati personali di una persona condannata per un reato di lieve entità (*Ayçaguer c. Francia*, 2017);
- la conservazione per un massimo di venti anni delle impronte digitali di una persona sospettata, ma non condannata, per furto di libri (*M. K. c. Francia*, 2013);
- la conservazione per un massimo di venti anni dei dati personali di un individuo in conseguenza di una denuncia per violenza nei confronti della sua compagna, archiviata a seguito di mediazione (*Brunet c. Francia*, 2014);
- la conservazione fino al 2278 dei dati personali relativi alla presunta omosessualità del ricorrente, raccolti nel 2004 (*Drelon c. Francia*, 2022).

207. Per contro, la Corte non ha riscontrato alcuna violazione dell'articolo 8 in diverse cause concernenti la memorizzazione per un massimo di trenta anni dei dati personali di individui condannati per aggressioni sessuali, dopodiché i dati sono stati automaticamente cancellati,in quanto erano state introdotte delle procedure per consentire la cancellazione dei dati appena essi non erano più pertinenti (*B.B. c. Francia*, 2009, § 67; *Gardel c. Francia*, 2009, § 69; *M.B. c. Francia,* 2009, § 59). La Corte ha inoltre dichiarato manifestamente infondata una causa concernente la conservazione a tempo indeterminato dei dati personali di individui condannati per gravi reati, accompagnata da riesami a intervalli regolari non superiori a dieci anni, per determinare se la memorizzazione continuasse a essere necessaria (*Peruzzo e Martens c. Germania* (dec.), 2013, §§ 44-49). Nella causa *P.N. c. Germania*, 2020 (§§ 87-90), la Corte non ha riscontrato alcuna violazione dell'articolo 8 in relazione alla conservazione per cinque anni, salve le garanzie e un riesame individualizzato, dei dati personali di un recidivo al fine della sua identificazione a seguito dell'avvio di un nuovo procedimento penale nei suoi confronti.

208. In relazione ai regimi di conservazione dei dati biometrici di persone condannate, la durata del periodo di conservazione non è necessariamente determinante nel valutare se uno Stato abbia ecceduto l'accettabile margine di discrezionalità quando ha istituito il pertinente regime – essendo determinante l'esistenza e il funzionamento di alcune garanzie (*Gaughran c. Regno Unito*, 2020, § 88). Quando gli Stati stessi fissano dei termini di conservazione dei dati biometrici delle persone condannate, o invero decidono che la conservazione dei dati debba essere a tempo indeterminato, essi si collocano al limite del loro margine di discrezionalità e devono garantire l'esistenza di alcune garanzie effettive (ibid.*,* § 88). L'esistenza o l'assenza di un riesame indipendente della giustificazione della conservazione delle informazioni sulla base di precisi criteri quali la gravità del reato, la forza del sospetto nei confronti della persona, le precedenti condanne e qualsiasi altra particolare circostanza, costituiscono un'importante garanzia per assicurare la proporzionalità dei termini di conservazione dei dati (ibid.*,* § 94; *S. e Marper c. Regno Unito* [GC], 2008, § 119; *B.B. c. Francia*, 2009, § 68; *Gardel c. Francia*, 2009, § 69; *M.B. c. Francia,* 2009, § 60).

209. L'assenza di un termine massimo di conservazione dei dati personali non è necessariamente incompatibile con l'articolo 8 (*Peruzzo e Martens c. Germania* (dec.), 2013, § 46; *Gaughran c. Regno Unito*, 2020, § 88), ma le garanzie procedurali sono particolarmente necessarie se la memorizzazione dei dati dipende interamente dalla diligenza con la quale le autorità assicurano la proporzionalità del termine di conservazione dei dati (*Peruzzo e Martens c. Germania* (dec.), 2013, § 46; *Ayçaguer c. Francia*, 2017, § 38).

210. Nella causa *Peruzzo e Martens c. Germania* (dec.), 2013 (§ 44) concernente la conservazione a tempo indeterminato dei dati biometrici di persone condannate per gravi reati e suscettibili di recidiva, la Corte era soddisfatta di constatare che il diritto interno imponeva al Tribunale penale federale di controllare a intervalli regolari, di non oltre dieci anni, se la memorizzazione dei dati continuasse a essere necessaria o se i dati potessero essere cancellati, tenuto conto in ciascun caso del fine della conservazione dei dati, nonché della natura e della gravità delle circostanze di ciascun caso in cui i dati personali erano stati registrati (ibid., § 46). La Corte ha ritenuto che la durata degli intervalli non fosse stata irragionevole, dato che i profili del DNA potevano essere ottenuti soltanto dalle persone condannate per reati che raggiungevano una specifica soglia di gravità (ibid. , §§ 48-49).

211. Nella causa *Gaughran c. Regno Unito*, 2020 (§ 96), il carattere illimitato della memorizzazione delle impronte digitali, dei profili del DNA e della fotografia di una persona riconosciuta colpevole di guida in stato di ebbrezza, aveva dato luogo alla constatazione di violazione dell'articolo 8. Le autorità non avevano tenuto conto della gravità del reato commesso, o della continua necessità di conservare i suddetti dati a tempo indeterminato, né avevano fornito alcuna reale possibilità di riesame (ibid., § 96).

212. Un termine massimo di memorizzazione dei dati personali previsto dal diritto interno può essere in pratica più affine a una norma che a un reale termine, se le possibilità di accettazione di una domanda di cancellazione dei dati prima della scadenza del termine previsto dalla legge sono meramente ipotetiche (*M. K. c. Francia*, 2013, §§ 44-47; *Brunet c. Francia*, 2014, §§ 41-45; *Ayçaguer c. Francia*, 2017, §§ 44-46). La Corte ha riscontrato la violazione dell'articolo 8 in diverse cause in cui l'ordinamento nazionale prevedeva termini massimi di conservazione di venti o venticinque anni per reati oggetto di procedimenti che erano stati archiviati (*M. K. c. Francia*, 2013, §§ 44-47; *Brunet c. Francia*, 2014, §§ 41-45), e perfino un termine massimo di memorizzazione di quaranta anni nel caso di un reato non particolarmente grave ma che aveva dato luogo a una condanna (*Ayçaguer c. Francia*, 2017, § 42).

213. Nella causa *Catt c. Regno Unito*, 2019 (§ 120), la conservazione per almeno sei anni dei dati personali del ricorrente in una banca dati della Polizia in materia di estremismo, termine dopo il quale essa sarebbe stata sottoposta a un riesame programmato, aveva dato luogo alla constatazione di violazione dell'articolo 8. Il ricorrente aveva dovuto dipendere del tutto dalla diligenza delle autorità nell'attuazione di garanzie altamente elastiche previste dal codice di condotta applicabile, per garantire la proporzionalità del termine di conservazione dei dati. L'assenza di garanzie per agevolare la cancellazione dei dati appena il termine di conservazione diventava sproporzionato è particolarmente preoccupante se i dati che rivelano opinioni politiche, che beneficiano di un accresciuto livello di protezione, sono conservati a tempo indeterminato (ibid., §§ 122-123).

214. La causa *M.M. c. Regno Unito*, 2012 concerneva le conseguenze delle modifiche della politica del termine di conservazione dei dati personali in un casellario giudiziale sulle prospettive di impiego dell'interessato (§ 204). La Corte ritiene improbabile che la raccolta indiscriminata e incondizionata dei dati relativi ai precedenti penali soddisfi i requisiti dell'articolo 8 data l'assenza di chiare e particolareggiate disposizioni giuridiche che spieghino le garanzie applicabili ed espongano le regole che disciplinano, *inter alia*, la durata della memorizzazione di tali dati (ibid., § 199).

215. Si veda altresì, in un ambito differente, il termine decennale fissato da un tribunale in materia di riservatezza delle prove prodotte nel corso di procedimenti contenenti dati medici tali da rivelare l'identità e la sieropositività all'HIV di una persona nella causa *Z c. Finlandia*, 1997 (§§ 111-113). In tale

causa il termine decennale di riservatezza contrastava con i desideri e gli interessi delle parti del procedimento, e la produzione, in assenza del consenso della ricorrente, delle informazioni in questione aveva già causato una grave ingerenza nel diritto al rispetto della sua vita privata e familiare. L'ulteriore ingerenza che ella avrebbe subito se le informazioni mediche fossero state rese pubblicamente accessibili dopo dieci anni non era giustificata da alcun motivo imperativo.

iii. Garanzie relative alla distruzione o alla cancellazione dei dati memorizzati [9]

216. Secondo la Corte, la cancellazione dei dati da una banca dati nella quale essi erano stati memorizzati per fini di polizia non era particolarmente onerosa (*Catt c. Regno Unito*, 2019*,* § 127). La creazione da parte del Governo di una banca dati che non permette di riesaminare o modificare facilmente i dati contenuti in essa, e il successivo utilizzo di tale sviluppo quale giustificazione per rifiutare di eliminare delle informazioni da tale banca dati contrasterebbe del tutto con l'esigenza di proteggere la vita privata di cui all'articolo 8 (ibid.*,* § 127).

217. La disponibilità a livello nazionale di una procedura giudiziaria per eliminare i dati, che preveda un riesame indipendente della giustificazione della conservazione delle informazioni secondo criteri definiti, e offra garanzie adeguate ed effettive del diritto al rispetto della vita privata della persona interessata, è un importante fattore nel bilanciare i vari interessi concorrenti (*S. e Marper c. Regno Unito* [GC], 2008, § 119; *Gardel c. Francia*, 2009, § 69).

218. La Corte non ha riscontrato alcuna violazione dell'articolo 8 in cause in cui, benché i dati fossero stati conservati per "lunghi" periodi, fino a trenta anni (*B.B. c. Francia*, 2009, §§ 66, 68; *Gardel c. Francia*, 2009, §§ 67, 69; *M.B. c. Francia,* 2009, §§ 58, 60), o perfino a tempo indeterminato (*Peruzzo e Martens c. Germania* (dec.), 2013, § 46), la persona interessata aveva beneficiato di una procedura giudiziaria che garantiva un riesame indipendente della giustificazione della memorizzazione dei suoi dati secondo criteri definiti, che le permettevano di ottenere la cancellazione dei dati prima della scadenza del termine massimo prescritto dalla legge, o, in caso di conservazione dei dati a tempo indeterminato, appena tale conservazione non era più pertinente (si veda, *a contrario*, *S. e Marper c. Regno Unito* [GC], 2008, § 119).

219. Pertanto nelle cause *B.B. c. Francia*, 2009 (§ 68), *Gardel c. Francia*, 2009 (§ 69), e *M.B. c. Francia,* 2009 (§ 60), la Corte ha stabilito che la procedura giudiziaria per ottenere l'eliminazione dei dati, che la persona interessata poteva iniziare presentando una semplice domanda al pubblico ministero, le cui decisioni potevano essere impugnate, prevedesse un riesame indipendente della giustificazione della conservazione delle informazioni secondo criteri definiti e offrisse garanzie adeguate ed effettive. Si veda altresì il paragrafo 204 *supra*, relativo alla causa *Peruzzo e Martens c. Germania* (dec.), 2013 (§ 44).

220. Nella causa *P.N. c. Germania*, 2020 (§§ 81, 88) concernente la memorizzazione dei dati personali di un delinquente maggiorenne i cui reati non erano di lieve entità né particolarmente gravi, la regola che prevedeva che tali dati fossero cancellati decorsi cinque anni in assenza, entro tale termine, di nuove indagini penali nei confronti della persona interessata, non è stata considerata in violazione dell'articolo 8. Esisteva una possibilità di riesame da parte delle autorità di polizia, suscettibile di riesame giudiziario, della necessità di conservare ulteriormente i dati in questione, e il ricorrente poteva quindi ottenere l'eliminazione dei suoi dati se il suo comportamento aveva dimostrato che i dati non erano più necessari a fini di polizia (ibid.*,* § 88).

221. L'assenza di effettive garanzie che permettano la cancellazione di dati personali che non sono più pertinenti agli iniziali fini è particolarmente preoccupante per quanto riguarda categorie sensibili di dati personali che esigono un accresciuto livello di protezione (*Catt c. Regno Unito*, 2019*,* § 123).

[9] Si veda altresì la Sezione *supra* sul diritto alla cancellazione dei dati (diritto all'oblio).

222. La possibilità di cancellazione dei dati ai sensi del diritto interno è una garanzia "teorica e illusoria", piuttosto che "pratica ed effettiva", se il diritto di presentare in qualsiasi momento una domanda tesa a ottenere tale cancellazione strideva con gli interessi dei Servizi investigativi di disporre di un casellario contenente il maggior numero di riferimenti possibile e se gli interessi concorrenti in gioco erano contraddittori, anche soltanto parzialmente (*M.K. c. Francia,* 2013, § 44). La garanzia della cancellazione dei dati ha un impatto limitato anche se le autorità rifiutano, successivamente a una domanda da parte della persona interessata di cancellazione dei suoi dati o di fornire spiegazioni riguardo al proseguimento della conservazione (*Catt c. Regno Unito*, 2019, § 122). Lo stesso può dirsi se le domande di cancellazione sono accolte soltanto in circostanze eccezionali, o sono rigettate se la persona interessata ha ammesso di avere commesso un reato e i dati sono esatti (*M.M. c. Regno Unito*, 2012, § 202).

223. La Corte ritiene che anche le persone che sono state condannate per un reato dovrebbero, come le persone che sono state assolte o prosciolte, disporre di un mezzo pratico per presentare una domanda di cancellazione dei dati registrati (*B.B. c. Francia*, 2009*,* § 68*; Brunet c. Francia*, 2014, §§ 41-43; *Ayçaguer c. Francia*, 2017, § 44). Nella causa *Ayçaguer c. Francia*, 2017 (§ 44), in cui una procedura di cancellazione dei dati era accessibile soltanto alle persone sospettate della commissione di un reato e non alle persone condannate, la Corte ha constatato la violazione dell'articolo 8. La Corte ha ritenuto che, in ragione della sua durata e dell'assenza della possibilità di cancellazione, le disposizioni relative alla memorizzazione dei profili del DNA nella banca dati nazionale non avessero conseguito un giusto equilibrio tra i concorrenti interessi pubblici e privati (ibid.*,* § 45).

224. Nella causa *Khelili c. Svizzera*, 2011 (§§ 68-70) la Corte ha riscontrato la violazione dell'articolo 8, dopo avere sottolineato le incertezze e le difficoltà provate dalla ricorrente nei suoi tentativi di ottenere la cancellazione della menzione di "prostituta" nella sezione "occupazione" del registro della Polizia, in quanto ella non era mai stata condannata per l'illecito esercizio della prostituzione. La Corte ha osservato che non era mai stato affermato che la cancellazione nel registro della polizia della menzione contestata fosse stata impossibile o difficile per motivi tecnici (ibid.*,* § 68).

iv. Garanzie finalizzate a disciplinare l'accesso di terzi e a proteggere l'integrità e la riservatezza dei dati

225. La Corte ha esaminato in diverse occasioni la questione di sapere se il diritto interno applicabile comprendesse garanzie in grado di proteggere efficientemente dall'uso scorretto e dall'abuso i dati personali memorizzati in banche dati ufficiali (*S. e Marper c. Regno Unito* [GC], 2008, § 103; *B.B. c. Francia*, 2009, § 61; *Gardel c. Francia*, 2009 § 62; *M.M. c. Regno Unito*, 2012, § 195; *M.K. c. Francia,* 2013, § 35; *Brunet c. Francia*, 2014, § 35; *Ayçaguer c. Francia*, 2017, § 38). Ha osservato che tali garanzie esistevano se, per esempio,

- soltanto autorità tenute alla riservatezza potevano consultare i dati registrati (*B.B. c. Francia*, 2009, § 69; *Peruzzo e Martens c. Germania* (dec.), 2013, § 47);
- i dati registrati erano soggetti a procedure ben definite di consultazione, concernenti le persone autorizzate a consultare la banca dati (*M.K. c. Francia,* 2013, § 37; si veda, *a contrario*, *Khelili c. Svizzera*, 2011, § 64);
- l'identità di una persona alla quale era stato prelevato un campione di DNA non era stata divulgata agli esperti responsabili della profilazione del DNA; questi ultimi erano anche tenuti ad adottare misure adeguate per impedire qualsiasi uso non autorizzato del materiale cellulare esaminato (*Peruzzo e Martens c. Germania* (dec.), 2013, § 45); il materiale cellulare stesso doveva essere immediatamente distrutto appena non era più necessario al fine di stabilire il profilo del DNA, e soltanto i profili del DNA estratti da tale materiale cellulare potevano essere conservati nella banca dati dell'Ufficio federale della Polizia criminale (ibid.*,* § 45); inoltre i profili del DNA conservati potevano essere divulgati soltanto alle autorità

competenti ai fini dei procedimenti penali, della prevenzione di pericoli e dell'assistenza giudiziaria internazionale (ibid., § 47).

226. Nella causa *Gardel c. Francia*, 2009 (§ 70), in cui le regole relative all'uso del registro e la sfera delle autorità pubbliche che potevano accedervi era stata ampliata in diverse occasioni e non era più limitata alle autorità giudiziarie e alla Polizia, poiché anche gli organi amministrativi vi accedono attualmente, la Corte era soddisfatta di osservare che il registro poteva essere consultato soltanto dalle autorità tenute alla riservatezza,e in circostanze definite in modo preciso.

227. Nella causa *P.N. c. Germania*, 2020 (§ 89), non vi era alcun elemento indicante che i dati identificativi di un delinquente maggiorenne memorizzati dalla Polizia per un massimo di cinque anni non fossero sufficientemente protetti dagli abusi quali l'accesso o la diffusione non autorizzati.

228. Per contro, nella causa *M.M. c. Regno Unito*, 2012 (§ 204), concernente la conservazione vita natural durante di un ammonimento nel casellario giudiziale di una persona e la divulgazione di tali dati a un futuro datore di lavoro nell'ambito della ricerca di un impiego, la Corte ha messo in discussione le lacune della procedura che disciplinava l'accesso di terzi al casellario giudiziale di persone alla ricerca di un impiego, che non permetteva di valutare, in qualsiasi fase, la pertinenza dei dati conservati nel casellario centrale all'impiego cercato, o della misura in cui la persona interessata poteva dare l'impressione di continuare a rappresentare un rischio.

b. Conservazione di dati sanitari

229. La Corte ha trattato la questione della memorizzazione di dati sanitari sensibili. Nella causa *Malanicheva c. Russia* (dec.), 2016 (§§ 13, 15-18), la Corte ha ritenuto che l'efficiente funzionamento degli istituti di cura e del processo decisionale giudiziario esigesse la memorizzazione e la condivisione dei dati pertinenti. Ha rigettato in quanto manifestamente infondate le doglianze concernenti la registrazione del nome della ricorrente nel registro ospedaliero delle persone affette da disturbi psichiatrici e gli asseritamente erronei riferimenti a vari aspetti della sua salute mentale nelle successive comunicazioni interne tra gli istituti di cura e nelle loro osservazioni dinanzi ai tribunali. Non vi era alcun elemento indicante che le informazioni registrate in questione fossero state rese accessibili al pubblico, o fossero state utilizzate per fini diversi da quello della decisione delle cure mediche più appropriate per la persona interessata.

230. Precedentemente, la Commissione aveva dichiarato manifestamente infondato e rigettato un ricorso concernente la registrazione nel registro di un ospedale psichiatrico di dati relativi al ricovero coatto di una paziente, che i tribunali nazionali avevano dichiarato illegale (*Yvonne Chave nata Jullien c. Francia*, 1991). La Commissione ha ritenuto che la registrazione di informazioni concernenti i pazienti mentali sia funzionale non soltanto all'interesse legittimo di assicurare l'efficiente gestione del Servizio ospedaliero pubblico, bensì anche a quello di tutelare i diritti dei pazienti stessi, in quanto contribuiva a prevenire il rischio di internamento arbitrario, ed era un mezzo di indagine a disposizione delle autorità amministrative o giudiziarie responsabii della vigilanza sugli istituti psichiatrici. Nella fattispecie, i dati personali della ricorrente annotati sul registro dell'ospedale psichiatrico erano stati protetti da appropriate regole di riservatezza.

231. Si veda altresì il paragrafo 182 *supra* relativo alla violazione dell'articolo 8 nella causa *Surikov c. Ucraina*, 2017 (§ 75-95).

c. Memorizzazione online di dati personali a fini giornalistici

232. Nella causa *M.L. e W.W. c. Germania*, 2018 (§ 90), la Corte ha dichiarato che la stampa aveva un ruolo secondario, ma ciononostante prezioso nella conservazione di archivi contenenti notizie che erano state precedentemente pubblicate e nel metterle a disposizione del pubblico. A tale riguardo, gli archivi su internet contribuiscono notevolmente a conservare le notizie e le informazioni e a renderle disponibili, in quanto esse costituiscono un'importante fonte per l'istruzione e la ricerca

storica, in particolare perché esse sono immediatamente accessibili al pubblico e sono generalmente gratuite (*Times Newspapers Ltd c. Regno Unito (nn. 1 e 2)*, 2009, §§ 27, 45; *Węgrzynowski e Smolczewski c. Polonia*, 2013, § 59).

3. Divulgazione di dati personali

233. La Corte ha valutato in diverse cause misure che comportavano la divulgazione, da parte del responsabile del trattamento, dei dati personali di un individuo:

- a un'altra persona fisica o giuridica (*Mockutė c. Lituania*, 2018, §§ 99-100, relativa alla trasmissione da parte di un ospedale di informazioni sullo stato di salute di una paziente a un suo familiare e ai giornalisti; *Y. c. Turchia* (dec.), 2015, §§ 70-72, concernente la divulgazione da parte dell'equipaggio di un'ambulanza al personale ospedaliero di informazioni circa la sieropositività di un paziente all'HIV; *Radu c. Repubblica di Moldavia*, 2014, § 27, concernente la divulgazione da parte di un ospedale di informazioni mediche sullo stato di salute di una paziente al suo datore di lavoro; *M.C. c. Regno Unito*, 2021, § 46 concernente la divulgazione da parte delle autorità di informazioni relative ai precedenti penali della ricorrente a un potenziale datore di lavoro);
- a un'autorità pubblica (*M.S. c. Svezia*, 1997, § 35, concernente la divulgazione da parte di un reparto ginecologico di informazioni mediche relative a una paziente alla Cassa di sicurezza sociale; *P.T. c. Repubblica di Moldavia*, 2020, §§ 5-6, 29-31, concernente il superfluo inserimento di dati medici sensibili in un certificato medico che doveva essere prodotto in vari contesti);
- al pubblico (*Hájovský c. Slovacchia*, 2021 §§ 46-49, relativa alla comunicazione in un telegiornale di informazioni che identificavano un individuo e contenevano una sua fotografia non sfocata, scattata segretamente e mediante un falso pretesto; *Peck c. Regno Unito*, 2003, § 63, relativa alla trasmissione ai media di un video proveniente da una televisione a circuito chiuso che mostrava una persona che tentava di suicidarsi in un luogo pubblico; *Bremner c. Turchia*, 2015, §§ 71-85, concernente la diffusione televisiva dell'immagine non sfocata, e non sfumata, di un individuo filmato mediante una telecamera nascosta; *Khadija Ismayilova c. Azerbaigian*, 2019, §§ 108-132, concernente la video-registrazione segreta di una giornalista nella sua abitazione privata e la pubblica diffusione dei video; *Z c. Finlandia*, 1997, §§ 70-71, concernente la divulgazione in una decisione giudiziaria trasmessa alla stampa dell'identità e dello stato di salute di un individuo; *Apostu c. Romania*, 2015, §§ 121-132, sulla divulgazione alla stampa di prove tratte da un fascicolo istruttorio; *Montera c. Italia* (dec.), 2002, concernente la diffusione pubblica di un rapporto da parte di una commissione parlamentare relativo alla vita privata e alla deontologia professionale di un magistrato; *Von Hannover c. Germania*, 2004, §§ 61-81, sulla pubblicazione sulla stampa scandalistica di fotografie relative alla vita privata di una principessa; *Polanco Torres e Movilla Polanco c. Spagna*, 2010, §§ 44-54, concernente un articolo della stampa basato sulle dichiarazioni di un ex contabile, che accusava la moglie di un alto magistrato di essere coinvolta in operazioni illecite con una specifica società; *Alkaya c. Turchia*, 2012, §§ 30-31, concernente la divulgazione da parte di un quotidiano a grande tiratura dell'indirizzo postale completo di una famosa attrice; *Mityanin e Leonov c. Russia*, 2018, §§ 111-121, relativa alla divulgazione sulla stampa della fotografia di un individuo sospettato, accompagnata da dichiarazioni che lo accusavano di vari reati di lieve entità e gravi; e *Bogomolova c. Russia*, 2017, §§ 54-58, concernente la pubblicazione della fotografia di un minore sulla copertina di un opuscolo intitolato "I bambini hanno bisogno di una famiglia", pubblicato da un Centro per il sostegno psicologico, medico e sociale).

a. Impatto del preliminare consenso

234. Il preliminare consenso da parte delle persone interessate alla trasmissione, alla divulgazione o alla pubblicazione dei loro dati è un elemento importante, benché non determinante, in un dato caso, per stabilire se tali operazioni costituiscano un'ingerenza nel loro diritto al rispetto della vita privata (*M.S. c. Svezia*, 1997, §§ 31, 35; *M.M. c. Regno Unito*, 2012, §§ 186, 189) o se esse possono essere considerate "previste dalla legge" ai sensi dell'articolo 8 § 2 (*Radu c. Repubblica di Moldavia*, 2014, § 27; *Mockutė c. Lituania*, 2018, § 101). La Corte ha riscontrato la violazione dell'articolo 8 in diverse cause in cui la divulgazione di dati personali da parte del responsabile del trattamento era avvenuta senza il consenso della persona interessata (*Radu c. Repubblica di Moldavia*, 2014, §§ 30, 32; *Mockutė c. Lituania*, 2018, §§ 103, 106; *Peck c. Regno Unito*, 2003, §§ 85-87; *Sõro c. Estonia*, 2015, §§ 17-19, 64).

235. Per essere valido, il consenso della persona interessata deve essere informato e inequivoco (*M.S. c. Svezia n*, 1997, § 32; *Konovalova c. Russia*, 2014, §§ 47-48). In una causa concernente la comunicazione della cartella clinica di una persona da un organo pubblico (il reparto di ginecologia di un ospedale) a un altro (la Cassa della sicurezza sociale) senza il consenso dell'interessata, si trattava di stabilire se, instaurando un'azione risarcitoria, l'interessata avesse rinunciato al suo diritto alla riservatezza dei dati (*M.S. c. Svezia*, 1997, §§ 31-32). La Corte ha stabilito che, poiché la divulgazione dei dati non era dipesa soltanto dal fatto che la ricorrente avesse presentato una domanda di risarcimento, bensì anche da diversi fattori dei quali ella non aveva il controllo, dalla sua domanda di risarcimento non si poteva desumere che ella avesse rinunciato inequivocabilmente al suo diritto al rispetto della vita privata in relazione alla cartella clinica. Conseguentemente, l'articolo 8 era applicabile.

236. Il fatto che i dati personali degli individui siano divulgati su loro richiesta, o con il loro consenso, non li priva della protezione offerta dall'articolo 8, se essi non hanno alcuna reale possibilità di scelta, per esempio se un datore di lavoro insiste per la divulgazione di dati personali memorizzati nel casellario giudiziale di una persona alla ricerca di un impiego (*M.M. c. Regno Unito*, 2012, § 189). In quest'ultimo caso, *M.M. c. Regno Unito*, 2012 (§§ 187-207), in cui la ricorrente aveva chiesto la divulgazione a un potenziale datore di lavoro di informazioni relative a un ammonimento, registrato nel suo casellario giudiziale, la Corte ha riscontrato la violazione dell'articolo 8 a causa dell'assenza di sufficienti garanzie nel regime di conservazione e di divulgazione di dati del casellario giudiziale, che non aveva previsto una valutazione, in qualsiasi fase, della pertinenza consentita dei dati all'impiego ricercato, o della misura in cui era possibile ritenere che la persona interessata continuasse a rappresentare un rischio (ibid., § 204). Nella causa *M.C. c. Regno Unito*, 2021, §§ 47-57, la Corte ha preso atto delle modifiche legislative introdotte successivamente alla sentenza *M.M. c. Regno Unito* e ha ritenuto che un regime recentemente introdotto riguardo alla divulgazione di informazioni relative ai precedenti penali fosse compatibile con i pertinenti requisiti dell'articolo 8: esso distingueva in diversi modi i differenti tipi di reati; permetteva di conoscere con certezza, in qualsiasi momento, quali precedenti condanne sarebbero state divulgate; e fissava un termine definito e limitato per la divulgazione, che sarebbe variato in funzione dell'età dell'autore del reato e della percepita gravità del reato.

237. Non è sempre possibile ottenere il consenso della persona interessata, per esempio se le sequenze di telecamere a circuito chiuso installate dalle autorità lungo la strada per facilitare l'identificazione degli autori di reati e prevenirli, contengono le immagini di numerose persone (*Peck c. Regno Unito*, 2003, § 81). Secondo la Corte, un sistema di telecamere a circuito chiuso, le cui immagini possono essere divulgate sulla base del consenso, potrebbe in pratica compromettere qualsiasi azione finalizzata a favorire l'efficacia del sistema di telecamere a circuito chiuso, nella scoperta e nella prevenzione dei reati, ruolo reso ancora più efficace dalla pubblicità del sistema di telecamere a circuito chiuso e dei vantaggi che esso presenta (ibid., § 81). In tali circostanze, o se le persone le cui immagini sono contenute in sequenze di telecamere a circuito chiuso rifiutano di acconsentire alla divulgazione delle loro immagini, il responsabile del trattamento dovrebbe

considerare altre soluzioni, come la mascheratura delle immagini prima della divulgazione (ibid., § 82) o assicurando che le immagini siano mascherate dai destinatari, in modo appropriato e adeguato (ibid., § 83).

238. Nella causa *Peck c. Regno Unito*, 2003 (§ 87), la comunicazione da parte di un consiglio comunale in un comunicato stampa per i media di immagini di una televisione a circuito chiuso, che filmava un individuo che tentava di suicidarsi in un luogo pubblico, aveva costituito violazione dell'articolo 8. La Corte ha ritenuto che, poiché la sequenza in questione era chiaramente concentrata e riguardava un solo individuo, l'operatore della televisione a circuito chiuso, che aveva avvisato la Polizia e ne aveva osservato l'intervento, avrebbe potuto chiedere alla Polizia informazioni per identificare l'identità del ricorrente e chiedere in tal modo il suo consenso alla divulgazione (ibid., § 81).

239. Nella causa *Bremner c. Turchia*, 2015 (§§ 71-85), la diffusione, in un documentario televisivo filmato mediante una telecamera nascosta, di un'immagine non sfocata e non sfumata di un individuo è stata considerata contraria all'articolo 8. Per quanto riguarda, in particolare, il fatto che il ricorrente non fosse famoso, non vi era alcun elemento che suggerisse che la suddetta trasmissione avesse un inerente valore informativo o fosse stata utilizzata correttamente e adeguatamente.

240. Inoltre, visto l'effetto dissuasivo al quale l'obbligo di una preliminare notifica rischia di dare luogo, i significativi dubbi riguardo all'efficacia di un obbligo di preliminare notifica, e l'ampio margine di discrezionalità goduto dalle autorità nazionali in questo campo, nella causa *Mosley c. Regno Unito*, 2011 (§ 132), la Corte ha ritenuto che l'articolo 8 non imponesse un obbligo legalmente vincolante di informare una persona prima di pubblicare informazioni sulla sua vita privata.

241. In alcune situazioni la divulgazione a uno stretto congiunto di dati relativi alla salute mentale di una persona, senza il suo consenso, può costituire violazione del diritto al rispetto della sua vita privata. Nella causa *Mockutė c. Lituania*, 2018 (§ 100), la Corte ha ritenuto che la divulgazione alla madre di una paziente di informazioni relative alla salute di sua figlia maggiorenne, senza il consenso di quest'ultima, in considerazione della tensione del rapporto tra le due adulte, fosse stata incompatibile con il diritto garantito ai sensi dell'articolo 8.

242. Per quanto riguarda persone arrestate o processate, la Corte ha riscontrato violazioni dell'articolo 8 nel caso in cui i Servizi di Polizia avessero consegnato alla stampa le fotografie dei ricorrenti senza il loro consenso (*Sciacca c. Italia*, 2005, §§ 29-31; *Khuzhin e altri c. Russia*, 2008, §§ 115-118), se avevano invitato squadre televisive a filmare un ricorrente in un posto di polizia, senza il consenso dello stesso, al fine di diffondere le immagini in televisione (*Toma c. Romania*, 2009, §§ 90-93; *Khmel c. Russia*, 2013, § 41), o ina una causa in cui l'affissione della fotografia del ricorrente nella bacheca delle "persone ricercate" non era prevista dalla legge (*Guiorgui Nikolaïchvili c. Georgia*, 2009, §§ 129-131).

243. Il mancato ottenimento del preliminare consenso della persona interessata alla trasmissione, alla divulgazione o alla pubblicazione dei suoi dati, non costituisce necessariamente violazione dell'articolo 8 se sussistono altre legittime preoccupazioni. quali la necessità di indagare riguardo a dei reati e assicurare la pubblicità dei procedimenti giudiziari (*Avilkina e altri c. Russia,* 2013, § 45; *Z c. Finlandia*, 1997, § 97), e la necessità di proteggere la salute pubblica (*Y. c. Turchia* (dec.), 2015, § 74), la sicurezza nazionale (*Anchev c. Bulgaria* (dec.), 2017, § 100) o il benessere economico di un Paese (*M.S. c. Svezia*, 1997, § 38).

b. Divulgazione di dati personali nell'ambito di procedimenti giudiziari

244. In diverse cause la Corte ha esaminato le misure adottate dalle autorità nell'ambito di procedimenti giudiziari che hanno dato luogo alla divulgazione di dati personali delle parti o di terzi, quali:

- la riproduzione da parte di un tribunale, in una sentenza di divorzio, di un estratto della cartella clinica personale (*L.L. c. Francia*, 2006, § 46), e un provvedimento che limitava a dieci

anni il termine di riservatezza delle prove, contenenti dati medici, prodotte (*Z c. Finlandia*, 1997, §§ 112-113);

- la divulgazione di dati psichiatrici riservati relativi a un ricorrente durante una pubblica udienza (*Panteleyenko c. Ucraina*, 2006, § 57), e la verifica di un certificato medico prodotto a sostegno di una domanda di rinvio (*Stokłosa c. Polonia* (dec.) 2021, §§ 43-44;
- la divulgazione dell'identità e della sieropositività all'HIV di un individuo in una sentenza comunicata alla stampa (*Z c. Finlandia*, 1997, § 113);
- la divulgazione dell'identità completa di un terzo in una sentenza, senza informarlo preliminarmente (*Vicent Del Campo c. Spagna*, 2018, §§ 47-51);
- l'utilizzo di un linguaggio e di argomenti che rivelano, in una sentenza, i dati personali della vittima, che trasmettono stereotipi sul ruolo delle donne e in grado di ostacolare l'effettiva protezione delle vittime di violenza sessuale, nonostante un soddisfacente quadro legislativo (*J.L. c. Italia*, 2021, §§ 136-142).

245. Secondo la Corte, la necessità di proteggere la riservatezza di alcuni tipi di dati personali può essere a volte superata dall'interesse per le indagini e il perseguimento dei reati e la pubblicità dei procedimenti giudiziari (*Avilkina e altri c. Russia,* 2013, § 45; *Z c. Finlandia*, 1997, § 97). Alle competenti autorità nazionali dovrebbe essere accordata una certa elasticità nel conseguire un giusto equilibrio tra, da una parte, la tutela della pubblicità dei procedimenti giudiziari, necessaria per sostenere la fiducia nei tribunali, e dall'altra, gli interessi di una parte o di un terzo al mantenimento della riservatezza dei suoi dati (*C.C. c. Spagna*, 2009, § 35). Qualsiasi misura in grado di rendere pubblici i dati personali di un individuo, sia egli parte o terzo in un procedimento giudiziario, dovrebbe rispondere a un'impellente esigenza sociale (*Vicent Del Campo c. Spagna*, 2018, § 46) e dovrebbe essere limitata, per quanto possibile, a quanto reso strettamente necessario dalle specifiche caratteristiche del procedimento (*L.L. c. Francia*, 2006, § 45).

246. Al fine di determinare, in un dato caso, se vi siano motivi sufficienti per divulgare, nel testo di una decisione giudiziaria, l'identità di un individuo e altri dati personali su quest'ultimo, è importante stabilire se, ai sensi del diritto e della prassi interni, sarebbero state possibili altre misure meno invasive. Ciò comprende la possibilità che un tribunale ometta di menzionare nella sentenza qualsiasi nome che permetta di identificare l'interessato (*Z c. Finlandia*, 1997, § 113; *Vicent Del Campo c. Spagna*, 2018, § 50), mantenere riservata per un certo periodo la motivazione completa e pubblicare invece una versione ridotta della motivazione e del dispositivo e un'indicazione succinta della legislazione applicata (*Z c. Finlandia*, 1997, § 113), o limitare l'accesso al testo di una sentenza, o a determinate parti di essa (*Vicent Del Campo c. Spagna*, 2018, § 50). La Corte ritiene che tali misure siano generalmente considerate in grado di ridurre l'impatto di una sentenza sul diritto dell'interessato alla protezione della sua vita privata.

247. Nella causa *Panteleyenko c. Ucraina,* 2006 (§ 82), la Corte ha ritenuto che anche la celebrazione di un'udienza a porte chiuse avrebbe contribuito a impedire la divulgazione pubblica, durante una pubblica udienza, di informazioni riservate relative alla salute mentale di una persona, ottenute da un ospedale psichiatrico e sulle cure psichiatriche cui era stata sottoposta in tale luogo, ance se ciò non avrebbe necessariamente impedito che tali informazioni fossero portate all'attenzione delle parti e fossero inserite nel fascicolo.

248. Nella causa *Frâncu c. Romania*, 2020 (§§ 72-73), la mancata assicurazione da parte di una corte di appello della riservatezza delle informazioni mediche relative al ricorrente, mediante il rigetto di una richiesta di celebrare un'udienza a porte chiuse, in una causa nei confronti di un sindaco in materia di corruzione, era stata ritenuta contraria all'articolo 8. Secondo la Corte, limitandosi a dichiarare, senza ulteriori spiegazioni, che il caso del ricorrente non corrispondeva ad "alcuna situazione" esposta nel codice di procedura penale relativa ai procedimenti svolti a porte chiuse, tale corte non era pervenuta a un giusto equilibrio tra l'interesse generale di assicurare la trasparenza dei procedimenti giudiziari e l'interesse del litigante di conservare la riservatezza dei dati relativi al suo stato di salute.

Anche supponendo che la notorietà di un imputato possa essere uno dei fattori di cui tenere conto nell'analisi della proporzionalità di una domanda, tesa a ottenere la celebrazione di un'udienza a porte chiuse, nella fattispecie la corte di appello non aveva svolto alcuna valutazione personalizzata della proporzionalità di tale misura.

249. Nella causa *Khadija Ismayilova c. Azerbaigian*, 2019 (§§ 105-132), la Corte ha stabilito che la divulgazione da parte delle autorità inquirenti di informazioni private comprendenti dati personali sensibili quali il nome e l'indirizzo della ricorrente, una giornalista professionista, nonchè i nomi dei suoi amici, dei suoi congiunti e dei suoi colleghi in un comunicato-stampa che pretendeva di fornire un rapporto sul progresso di un'indagine penale, avesse costituito violazione dell'articolo 8 (ibid., §§ 142-150).

250. Nella causa *M.P. c. Portogallo*, 2021, §§ 48-49, la produzione da parte dell'ex marito della ricorrente, senza il consenso di quest'ultima, nell'ambito di una causa di divorzio, di messaggi di posta elettronica scambiati da sua moglie su un sito di incontri, al quale sembrava che ella gli avesse dato accesso, non aveva comportato la violazione dell'articolo 8, in quanto il Tribunale per la famiglia non aveva infine tenuto conto di essi e il pubblico accesso ai dati in tale tipo di procedimento era, in ogni caso, limitato.

251. Nella causa *J.S. c. Regno Unito* (dec.), 2015 (§§ 71-73), la Corte ha rigettato in quanto manifestamente infondata una doglianza relativa alla divulgazione in un comunicato-stampa della Procura di informazioni personali che non eccedevano quanto fornito generalmente ai media in risposta a delle domande su un procedimento giudiziario, e non avevano divulgato il nome del ricorrente, la sua età o l'istituto scolastico che frequentava (era un minore accusato di avere aggredito un insegnante), né alcuna altra informazione personale.

252. Nella causa *L.L. c. Francia*, 2006 (§§ 46), in cui il giudice aveva invocato, quale base alternativa e secondaria, nell'ambito di una causa di divorzio, la corrispondenza privata tra un medico specialista e il medico che curava il ricorrente, contenente un documento medico riservato, il fatto che il giudice o l'investigatore avrebbero potuto escludere i dati medici in questione dalla motivazione della sentenza, potendo comunque giungere alla medesima conclusione, era un importante fattore di cui si doveva tenere conto. Poiché chiunque avrebbe potuto ottenere una copia della motivazione della decisione senza dovere dimostrare un particolare interesse, l'ingerenza subita dal ricorrente nel suo diritto al rispetto della sua vita privata non era stata giustificata, in considerazione del fondamentale ruolo svolto dalla protezione dei dati personali, nonostante il fatto che il procedimento tra le parti di un divorzio non fosse pubblico e la decisione valida opponibile a terzi contenesse soltanto il dispositivo (ibid., §§ 47, 33).

253. Nella causa *Vicent Del Campo c. Spagna*, 2018 (§§ 53, 56), il fatto che il ricorrente, terzo in un procedimento giudiziario, fosse stato privato di qualsiasi possibilità di chiedere a un tribunale, prima della pronuncia della sentenza, di astenersi dal comunicare la sua identità, aveva costituito violazione dell'articolo 8. Il ricorrente non era stato informato, interrogato, citato a comparire o informato in qualsiasi modo.

254. In una causa in cui i tribunali nazionali avevano limitato a tre anni il periodo di riservatezza dei documenti contenuti nel fascicolo che rivelavano l'identità e la sieropositività della ricorrente all'HIV, la Corte ha riscontrato la violazione dell'articolo 8, in quanto le autorità giudiziarie avevano attribuito un peso insufficiente all'interesse di proteggere i dati personali delle parti e di terzi che potevano essere compromessi (*Z c. Finlandia*, 1997, §§ 111-112). Ha ritenuto che la grave ingerenza nel diritto diritto della ricorrente al rispetto della sua vita privata, causata dalla produzione in un procedimento giudiziario, senza avervi acconsentito, di informazioni relative al suo stato di salute, sarebbe stata ulteriormente aggravata se le informazioni mediche in questione fossero state rese accessibili al pubblico dopo dieci anni (ibid., § 112). Per contro, nella causa *Y. c. Turchia* (dec.), 2015 (§§ 81-82), il fatto che l'identità e la sieropositività del ricorrente all'HIV fossero state rivelate in una sola decisione di incompetenza emessa da un tribunale amministrativo, che non era stata pubblicata o resa pubblica

in alcun altro modo, e non era accessibile al pubblico, mentre nessuna altra decisione emessa nell'ambito del medesimo procedimento vi aveva rinviato, non era stato considerato in grado di violare il diritto dell'interessato al rispetto della sua vita privata.

255. Nella causa *Drakšas c. Lituania*, 2012 (§ 60), la divulgazione nell'ambito di un procedimento di destituzione di registrazioni di conversazioni telefoniche intercettate dai Servizi segreti, tra il ricorrente, un noto politico, e il Presidente, che era oggetto del procedimento di destituzione, in una pubblica udienza dinazi alla Corte costituzionale, trasmessa in diretta dai canali televisivi nazionali, non aveva costituito violazione dell'articolo 8. La Corte ha ritenuto che essendo una figura pubblica, il ricorrente si era esposto inevitabilmente e consapevolmente a un attento controllo, sia da parte dei giornalisti che della popolazione, di ogni sua parola pronunciata e ogni suo atto compiuto. Data la situazione, la divulgazione, prevista dalla legge, delle sue conversazioni telefoniche non private, di carattere politico o commerciale, durante il procedimento costituzionale era stata necessaria alla protezione dei diritti altrui.

256. Si veda altresì il paragrafo 242 *supra* concernente la divulgazione alla stampa, da parte di Servizi di Polizia, di fotografie di persone in stato di arresto o processate, senza il consenso delle stesse, e i paragrafi 80-82 *supra* relativi agli obblighi positivi dello Stato in cause concernenti la divulgazione di dati personali da parte di privati.

c. Divulgazione dei dati al fine della protezione della salute pubblica

257. Il diritto di una persona al rispetto della riservatezza dei suoi dati medici non è assoluto e deve essere considerato in relazione ad altri diritti e interessi legittimi, quale il diritto del suo datore di lavoro a un procedimento in contraddittorio (*Eternit c. Francia* (dec.), 2012, § 37). Tale diritto può essere superato dalla necessità di proteggere un fondamentale aspetto di interesse pubblico, quale la sicurezza del personale ospedaliero e la protezione della salute pubblica (*Y. c. Turchia* (dec.), 2015, § 74).

258. In casi di cure di pazienti in ospedale e nell'ambito del sistema sanitario, la trasmissione di informazioni relative alla condizione del paziente può, in alcune circostanze, essere pertinente e necessaria non soltanto ai fini di garantire al paziente appropriate cure mediche, bensì anche di assicurare la protezione dei diritti e degli interessi del personale sanitario coinvolto nelle sue cure e in quelle di altri pazienti, permettendo di adottare le necessarie misure di precauzione (*Y. c. Turchia* (dec.), 2015, § 74). Se il personale sanitario stesso corre il rischio di infezione a causa della sua esposizione nello svolgimento dei propri compiti, la sicurezza del personale ospedaliero e la protezione della salute pubblica possono giustificare la trasmissione di informazioni relative allo stato di salute di un paziente tra il personale sanitario coinvolto nella sua cura, al fine di prevenire il rischio di trasmissione della patologia all'interno dell'ospedale (ibid., § 78).

259. Le informazioni sensibili quali i dati relativi allo stato di salute di un paziente dovrebbero essere trasmesse in modo da impedire qualsiasi forma di stigmatizzazione della persona interessata e di fornire sufficienti garanzie per evitare qualsiasi rischio di abuso (*Y. c. Turchia* (dec.), 2015, § 79). Il destinatario delle informazioni dovrebbe essere tenuto a precise regole di riservatezza proprie dei professionisti sanitari o ad analoghi obblighi di riservatezza (ibid., § 74).

260. Nella causa *Y. c. Turchia* (dec.), 2015 (§§ 78-79), la Corte ha rigettato in quanto manifestamente infondato un ricorso concernente lo scambio di informazioni sulla sieropositività di un paziente all'HIV, tra i vari professionisti sanitari, in un ospedale nel quale egli era stato sottoposto a cure, in quanto la condivisione di tali informazioni era stata giustificata dalla sicurezza del personale ospedaliero e dalla protezione della salute pubblica, nonostante il fatto che l'interessato non avesse prestato il consenso. La Corte ha attribuito importanza al fatto che ai sensi del diritto interno tutto il personale sanitario era tenuto a rispettare la riservatezza dei dati che gli erano trasmessi nell'ambito della loro situazione o della loro professione, pena sanzioni disciplinari o penali.

d. Divulgazione dei dati al fine della protezione della sicurezza nazionale

261. In diverse cause relative allo smantellamento dei vecchi regimi comunisti, la Corte ha esaminato la questione della rivelazione al pubblico di dati relativi al remoto passato di un individuo, raccolti e memorizzati al fine di proteggere la sicurezza nazionale (*Sõro c. Estonia*, 2015, § 58; *Anchev c. Bulgaria* (dec.), 2017, § 100). È attribuita importanza alle misure personalizzate attuate per il processo di smantellamento, alla loro disciplina e alle garanzie previste.

262. Pertanto, nella causa *Sõro c. Estonia*, 2015 (§§ 56-64), la rivelazione di informazioni che indicavano che il ricorrente aveva lavorato come autista nei vecchi Servizi di sicurezza aveva costituito violazione dell'articolo 8. Benché il ricorrente fosse stato informato in anticipo del fatto che i dati dovevano essere pubblicati e avesse avuto la possibilità di contestarne la comunicazione, non esisteva alcuna procedura per valutare le specifiche mansioni svolte da persone assunte dai vecchi Servizi di sicurezza, al fine di differenziare il pericolo che essi avrebbero potuto eventualmente rappresentare in un regime democratico diversi anni dopo la fine della loro carriera in tali istituzioni (ibid., § 61). La Corte ha ritenuto che la minaccia, che il ricorrente avrebbe potuto inizialmente rappresentare per la democrazia creata recentemente, dovesse essere notevolmente diminuita con il decorso del tempo tra la restaurazione dell'indipendenza dell'Estonia e la pubblicazione dei suoi dati personali (ibid., § 62). Benché la Legge sulla divulgazione non avesse *per se* imposto alcuna limitazione al nuovo impiego del ricorrente, egli era stato costretto a dimettersi dall'impiego a causa dell'atteggiamento adottato dai suoi colleghi, il che era indicativo della gravità dell'ingerenza nel diritto del ricorrente al rispetto della sua vita privata (ibid., § 63).

263. Per contro, nella causa *Anchev c. Bulgaria* (dec.), 2017 (§§ 92-116), in cui la procedura di divulgazione era disciplinata rigorosamente ed era accompagnata da diverse garanzie contro le arbitrarietà e gli abusi, compreso il fatto che essa era stata affidata a una commissione indipendente speciale le cui decisioni erano soggette a riesame giudiziario in due gradi di giurisdizione, la pubblica divulgazione di dati relativi al remoto passato del ricorrente era stata ritenuta incompatibile con l'articolo 8. Poiché la divulgazione non aveva comportato alcuna sanzione o incapacità giuridica, l'ingerenza non aveva ecceduto il notevole margine di discrezionalità di cui godevano le autorità (ibid., §§ 106-113). La Corte ha dichiarato che le sue conclusioni avrebbero potuto essere diverse se gli Stati avessero attuato misure comportanti una più grave ingerenza nella sfera personale dell'interessato, quali il divieto di lavorare o la parziale privazione del diritto di voto (ibid., § 113).

e. Divulgazione dei dati al fine della protezione del benessere economico del Paese

264. Le misure considerate in grado di assicurare la protezione del benessere economico del Paese e che violano la riservatezza dei dati raccolti o memorizzati dalle autorità non sono necessariamente contrarie all'articolo 8 se sono accompagnate da garanzie effettive e soddisfacenti (*M.S. c. Svezia*, 1997, § 41). Nel bilanciare i vari interessi concorrenti, le questioni volte a stabilire se il diritto interno disciplini le misure che possono essere adottate dai responsabili del trattamento, se essi siano responsabili in caso di inosservanza dei requisiti legali, e se il destinatario dei dati sia obbligato a osservare regole e garanzie analoghe e in particolare l'obbligo di riservatezza, sono importanti aspetti di cui si deve tenere conto (ibid., § 43).

265. Nella causa *M.S. c. Svezia*, 1997 (§§ 31-44), la trasmissione delle cartelle cliniche di una persona da un organo pubblico (il reparto di ginecologia di un ospedale) a un altro (la Cassa della sicurezza sociale), responsabile di valutare se la ricorrente soddisfacesse le condizioni legali per ottenere una prestazione che aveva richiesto, non era stata in violazione dell'articolo 8. La Corte ha ritenuto che la comunicazione dei dati fosse stata potenzialmente determinante per lo stanziamento di fondi pubblici a richiedenti meritevoli e si potesse quindi ritenere che avesse perseguito il fine di proteggere il benessere economico del Paese (ibid., § 38). La divulgazione dei dati riservati della ricorrente era stata accompagnata da garanzie effettive e soddisfacenti contro gli abusi: ai sensi della pertinente legislazione interna la comunicazione dei dati in questione era subordinata alla condizione che le

informazioni dovessero essere importanti al fine dell'applicazione della Legge sull'assicurazione per l'invalidità lavorativa (ibid., §§ 18, 43); il personale del reparto di ginecologia avrebbe potuto essere responsabile civilmente e/o penalmente se non avesse osservato tali condizioni (ibid., §§ 22, 43); e il destinatario dei dati aveva un analogo obbligo di rispettare la loro riservatezza (ibid., §§ 20, 22, 43).

f. Divulgazione in massa di dati personali

266. L'esistenza di un interesse pubblico a fornire accesso a notevoli quantità di dati fiscali e a permettere che fossero raccolti non comportava necessariamente o automaticamente che esistesse anche un interesse pubblico a divulgare *en masse* tali dati grezzi in forma inalterata, senza alcun apporto analitico. Nella causa *Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia* [GC], 2017 (§ 175), la Corte ha sottolineato che dovrebbe essere operata una distinzione tra il trattamento di dati a fini giornalistici e la diffusione dei dati grezzi ai quali era stato dato ai giornalisti un accesso privilegiato. Il fatto di impedire la diffusione in massa di dati fiscali personali, in base a procedure incompatibili con la disciplina nazionale e le norme dell'Unione europea in materia di protezione dei dati, non costituisce di per sé una sanzione, benché le limitazioni imposte riguardo alla quantità di informazioni da pubblicare può, in pratica, avere reso meno redditizie le attività commerciali di alcune società ricorrenti (ibid., § 197).

B. Diritti delle persone interessate

267. La giurisprudenza della Corte concede agli interessati diversi specifici diritti al fine di garantire il loro godimento dei diritti previsti da tale articolo.

1. Diritto di accesso ai propri dati

268. Le persone i cui dati personali sono stati raccolti e memorizzati dalle autorità sono titolari di un interesse, tutelato dall'articolo 8, a ricevere le informazioni: che sono state raccolte su di esse dai vecchi Servizi segreti sotto regimi totalitari e che sono state memorizzate negli archivi statali (*Haralambie c. Romania*, 2009, § 79; *Jarnea c. Romania*, 2011, § 50; *Joanna Szulc c. Polonia*, 2012, § 87); che sono necessarie per la loro salute o i rischi per la salute cui sono state esposte (*Roche c. Regno Unito* [GC], 2005, § 155; *K.H. e altri c. Slovacchia*, 2009, § 44; *Yonchev c. Bulgaria*, 2017, § 46); per conoscere e comprendere la loro infanzia e il loro precoce sviluppo (*Gaskin c. Regno Unito,* 1989, § 41); o a scoprire le loro origini, e in particolare l'identità dei loro genitori (*Odièvre c. Francia* [GC], 2003, §§ 43-44; *Godelli c. Italia*, 2012, §§ 62-63; *M.G. c. Regno Unito*, 2002, § 27).

269. In tali differenti contesti le autorità hanno un obbligo inerente all'effettivo rispetto della vita privata, garantito ai sensi dell'articolo 8, di prevedere procedure effettive e accessibili che permettano al ricorrente di accedere a qualsiasi informazione pertinente e appropriata necessaria per fini specifici (*Roche c. Regno Unito* [GC], 2005, § 162; *Haralambie c. Romania*, 2009, § 86; *Joanna Szulc c. Polonia*, 2012, §§ 86, 94).

270. Per contro, se lo Stato teme legittimamente che l'accesso a informazioni comprendenti dati personali potrebbe compromettere l'efficacia di un sistema di sorveglianza segreta finalizzato a proteggere la sicurezza nazionale o a contrastare il terrorismo, esso può rifiutare l'accesso alle informazioni raccolte e memorizzate in un registro segreto senza violare l'obbligo positivo spettante alle autorità ai sensi dell'articolo 8 (*Leander c. Svezia*, 1987, § 66; *Segerstedt-Wiberg e altri c. Svezia*, 2006, § 102). Al fine di determinare se lo Stato abbia il diritto di ritenere che gli interessi della sicurezza nazionale e della lotta contro il terrorismo prevalgano sugli interessi di una persona a essere pienamente informata delle informazioni conservate su di lei nei Servizi di sicurezza, la Corte deve essere convinta che sussistano sufficienti garanzie contro le arbitrarietà. La qualità della legge (ibid., §§ 79-80) e le garanzie predisposte, e in particolare la possibilità di riesame della misura contestata e dei mezzi di ricorso disponibili a livello nazionale per la persona interessata (ibid., §§ 52-68), sono

importanti criteri di cui si deve tenere conto nel bilanciare gli interessi concorrenti (ibid., § 103). Analoghi principi sono applicabili nell'ambito dell'espulsione di stranieri. Nella causa *Hassine c. Romania*, 2021, §§ 55-69, il ricorrente, un cittadino tunisino residente legalmente in Romania, era stato espulso dal Paese per motivi di sicurezza nazionale e dichiarato persona indesiderabile in Romania per un periodo di cinque anni, sulla base di alcune informazioni provenienti dai Servizi segreti romeni, che erano classificate segrete, e che indicavano che egli era asseritamente dedito ad attività che potevano mettere in pericolo la sicurezza nazionale. Né il ricorrente né il suo difensore erano stati autorizzati a consultare tali documenti. La Corte ha ritenuto che il procedimento amministrativo finalizzato all'espulsione del ricorrente avesse difettato delle necessarie garanzie processuali e ha riscontrato la violazione dell'articolo 1 del Protocollo n. 7.

271. In una causa relativa alla registrazione a lungo termine dei dati personali di un ricorrente nel Sistema di informazione Schengen, la Corte ha stabilito che l'impossibilità per il ricorrente di ottenere un pieno accesso personale alle informazioni che aveva chiesto non potesse violare il diritto al rispetto della sua vita privasta, in considerazione della necessità prioritaria di proteggere la sicurezza nazionale (*Dalea c. Francia* (dec.), 2010). Benché il ricorrente non avesse potuto impugnare i motivi precisi del suo inserimento nella banca dati Schengen, gli era stato concesso l'accesso a tutti gli altri dati che lo riguardavano ed era stato informato del fatto che considerazioni relative alla sicurezza, alla difesa e alla pubblica sicurezza dello Stato avevano dato luogo al rapporto (ibid., che rinvia a *Leander c. Svezia*, 1987, § 66).

272. Se soltanto alcuni documenti contenuti in un fascicolo memorizzato dalle autorità su un individuo, che conteneva dati personali, erano stati secretati ai fini di un segreto di Stato, le autorità avrebbero potuto concedere al ricorrente un parziale accesso al fascicolo (*Yonchev c. Bulgaria*, 2017, §§ 55-59). Pertanto, in una causa concernente il rifiuto da parte delle autorità di consentire al ricorrente, un ex agente di Polizia, di consultare documenti selezionati del suo fascicolo personale, vale a dire le sue valutazioni psicologiche, la Corte ha constatato la violazione dell'articolo 8 in ragione di disposizioni nazionali eccessivamente formali che imponevano che se anche un solo documento contenuto in un fascicolo fosse secretato, anche il resto doveva essere considerato automaticamente secretato e quindi soggetto alle regole relative alla protezione delle informazioni secretate (ibid., § 60).

273. Se la legislazione nazionale prevedeva esplicitamente il diritto di accesso a un fascicolo personale registrato e memorizzato dai vecchi Servizi di sicurezza durante i regimi totalitari negli ex Stati comunisti, lo Stato doveva predisporre una procedura effettiva e accessibile che permettesse all'interessato di ottenere un accesso ragionevolmente rapido a tutte le informazioni pertinenti (*Haralambie c. Romania*, 2009, § 86; *Jarnea c. Romania*, 2011, § 50; *Antoneta Tudor c. Romania*, 2013, § 34; *Joanna Szulc c. Polonia*, 2012, §§ 86, 94). La Corte ha constatato la violazione dell'articolo 8 in una causa in cui il ricorrente aveva avuto accesso soltanto a parte del fascicolo conservato a suo nome, che era stato registrato e memorizzato dai vecchi Servizi segreti (*Jarnea c. Romania*, 2011, §§ 54-60), e in altre due cause in cui ai ricorrenti era stato concesso l'accesso ai loro documenti soltanto dieci anni dopo la loro iniziale richiesta (*Joanna Szulc c. Polonia*, 2012, §§ 93-95; *Antoneta Tudor c. Romania*, 2013, §§ 34-40). Vizi nel sistema di archiviazione o errori fattuali, come la registrazione di una data di nascita errata nel fascicolo personale di un ricorrente, non potevano giustificare un ritardo di sei anni nel concedergli l'accesso ai suoi dati personali (*Haralambie c. Romania,* 2009, § 95). L'avanzata età di una persona che aveva chiesto di accedere a tale tipo di informazioni conferiva perfino maggiore urgenza al suo interesse a scoprire la sua storia personale all'epoca del regime totalitario (ibid., § 93 *in fine*).

274. Per quanto riguarda le informazioni relative alla salute o ai rischi per la salute, il diritto di accesso ai dati personali si estende all'obbligo di mettere a disposizione dell'interessato copie dei fascicoli contenenti i suoi dati (*K.H. e altri c. Slovacchia*, 2009, § 47). Chi detiene il fascicolo deve determinare le modalità per copiare i fascicoli contenenti dati personali e se le relative spese debbano essere sostenute dall'interessato (ibid., § 48). Gli interessati non dovrebbero essere obbligati a giustificare

specificamente la domanda finalizzata a ottenere una copia dei fascicoli contenenti i loro dati personali. Spetta piuttosto alle autorità dimostrare l'esistenza di motivi imperativi per rifiutare tale possibilità (ibid., § 48). Nella causa *K.H. e altri c. Slovacchia*, 2009 (§§ 50-58), delle ex pazienti di un ospedale non avevano potuto fotocopiare le loro cartelle cliniche originali, che erano state collazionate e memorizzate in un ospedale pubblico, e che contenevano informazioni che esse ritenevano importanti per la loro integrità morale e fisica. La Corte ha ritenuto che la sola possibilità offerta dall'ospedale di compilare degli estratti scritti a mano delle cartelle originali non avesse fornito loro un accesso effettivo ai documenti pertinenti riguardanti la loro salute.

275. Se un Governo svolge attività pericolose che potrebbero avere conseguenze negative occulte per la salute delle persone coinvolte in tali attività, le autorità hanno l'obbligo positivo di fornire una "procedura effettiva e accessibile" che consenta al ricorrente di accedere a "qualsiasi informazione pertinente e appropriata" che gli permetta di valutare i rischi cui è stato esposto (*McGinley ed Egan c. Regno Unito*, 1998, § 101; *Roche c. Regno Unito* [GC], 2005, § 161-162). Un periodo di attesa irragionevole, per esempio quando i Servizi di informazione e ricerca sanitaria hanno avviato le pertinenti procedure di recupero e divulgazione dei documenti quasi dieci anni dopo l'inizio della ricerca dei documenti in questione da parte del ricorrente, costituisce un inadempimento da parte dello Stato, in violazione dell'articolo 8, del suo obbligo positivo inerente al rispetto della vita privata dell'interessato, nonostante le difficoltà legate all'età e al carattere dispersivo dei documenti (ibid., § 166).

276. Per quanto riguarda l'accesso ai dati personali di un individuo che era stato collocato da bambino in affidamento familiare, a seguito del decesso dei suoi genitori o della loro incapacità di prendersi cura di lui, un regime che subordinava l'accesso ai fascicoli al consenso delle "persone che hanno collaborato ai fascicoli", vale a dire delle persone che avevano prodotto la documentazione pertinente, può, in linea di principio, essere compatibile con l'articolo 8 ai sensi del margine di discrezionalità dello Stato. Tuttavia, tale regime deve proteggere gli interessi di chiunque chieda di consultare documenti relativi alla sua vita privata e familiare, ed è conforme al principio di proporzionalità soltanto se prevede che un'autorità indipendente decida in via definitiva se debba essere concesso l'accesso nei casi in cui un collaboratore non risponda o neghi il consenso (*Gaskin c. Regno Unito*, 1989, § 49). Nei casi in cui il regime nazionale non abbia previsto un appello a tale organo in caso di rifiuto da parte dei Servizi sociali di concedere l'accesso a tutta la documentazione contenuta in un dato fascicolo, compreso se un terzo interessato o che ha prodotto le informazioni neghi il consenso alla divulgazione, la Corte ha constatato la violazione dell'articolo 8 (ibid., § 49; *M.G. c. Regno Unito*, 2002, §§ 30-32).

277. La Corte ritiene che il figlio nato fuori del matrimonio che chiede la determinazione del suo legame giuridico con il padre biologico abbia un interesse cruciale tutelato dalla Convenzione a ottenere le informazioni di cui ha bisogno per apprendere la verità riguardo a un importante aspetto della sua identità personale (*Mikulić c. Croazia*, 2002, § 64; *Boljević c. Serbia*, 2020, § 50). Un regime che non dispone di mezzi per obbligare l'asserito padre a osservare un ordine di un tribunale che gli impone di sottoporsi all'esame del DNA, può essere considerato in via di principio compatibile con gli obblighi derivanti dall'articolo 8, tenuto conto del margine di discrezionalità dello Stato (*Mikulić c. Croazia*, 2002, § 64). Tuttavia, l'assenza di una misura procedurale per obbligare l'asserito padre a osservare l'ordine di un tribunale è conforme al principio di proporzionalità soltanto se prevede mezzi alternativi che permettano a un'autorità indipendente di determinare rapidamente la domanda di accertamento della paternità (ibid., § 64). La Corte ha riscontrato la violazione dell'articolo 8 in una causa in cui, se il padre putativo aveva rifiutato di partecipare alla procedura medica, il regime nazionale non prevedeva alcuna misura per costringerlo a sottoporsi all'esame del DNA o mezzi alternativi che permettessero a un'autorità indipendente di determinare velocemente la domanda di accertamento della paternità (ibid., § 64). L'interesse di una persona a scoprire l'identità dei suoi genitori non scompare con l'età, anzi è vero il contrario (*Jäggi c. Svizzera*, 2006, § 40, concernente il

rifiuto di autorizzare l'esame del DNA di una persona deceduta come richiesto dal suo asserito figlio, che desiderava accertare la sua origine legale; *Boljević c. Serbia*, 2020, § 54).

278. Nel caso di figli partoriti nell'anonimato, la questione dell'accesso alle proprie origini e alle informazioni relative all'identità dei propri genitori biologici è differente da quella dell'accesso a un registro relativo a un minore in affido o alle prove dell'asserita paternità (*Odièvre c. Francia* [GC], 2003, § 43; *Godelli c. Italia*, 2012, § 62). A causa dell'ampia gamma di differenti tradizioni e ordinamenti giuridici, gli Stati dovevano beneficiare di un livello di discrezionalità nel mantenere la riservatezza delle identità dei genitori biologici (*Odièvre c. Francia* [GC], 2003, § 46; *Godelli c. Italia*, 2012, § 65). Un regime nazionale che forniva a una ricorrente accesso a informazioni non concernenti l'identità di sua madre e della sua famiglia biologica, permettendole di accertare parte della sua storia personale, senza pregiudizio per gli interessi di terzi, accompagnato dalla possibilità ai sensi di una legislazione promulgata recentemente di chiedere le prestazioni di un organo indipendente incaricato di aiutare le persone a scoprire le loro origini biologiche al fine di ottenere la rivelazione dell'identità di sua madre, subordinatamente al consenso di quest'ultima, è stato considerato compatibile con l'articolo 8 (*Odièvre c. Francia* [GC], 2003, § 49). Per contro, un regime che concedeva una preferenza assoluta al desiderio di una madre di rimanere anonima e non prevedeva alcun mezzo mediante il quale una minore adottata, che non era stata riconosciuta alla nascita, potesse chiedere l'accesso a informazioni relative alle sue origini, che non permettevano l'identificazione o la rivelazione dell'identità di sua madre, è stato ritenuto incompatibile con i requisiti dell'articolo 8 (*Godelli c. Italia*, 2012, §§ 70-72).

2. Diritto di rettifica

279. La Corte ha esaminato diverse cause relative alla memorizzazione da parte delle autorità di dati falsi, o di dati dei quali il ricorrente aveva contestato l'accuratezza (*Rotaru c. Romania* [GC], 2000, §§ 42-44, 55-63, concernente l'incapacità del ricorrente di confutare dati relativi alla sua asserita partecipazione al movimento legionario romeno, in un fascicolo costituito dal Servizio di sicurezza; *Cemalettin Canlı c. Turchia*, 2008, §§ 34-37, concernente l'inserimento in un procedimento giudiziario di dati personali incompleti, raccolti dalla Polizia; *Khelili c. Svizzera*, 2011, § 56, concernente la conservazione nei registri della Polizia della menzione di "prostituta" quale occupazione di una persona che aveva sempre negato di essersi prostituita).

280. L'incapacità di una persona di ottenere la rettifica di un rapporto che la riguardava nella banca dati Schengen (*Dalea c. Francia* (dec.), 2010) e la registrazione dell'origine etnica di una persona nei registri ufficiali (*Ciubotaru c. Moldavia*, 2010, § 59) costituiscono un'ingerenza nel loro diritto al rispetto della vita privata. In alcune circostanze, in particolare se sono in gioco considerazioni in materia di sicurezza statale, difesa nazionale e sicurezza pubblica, tale ingerenza non è necessariamente incompatibile con l'articolo 8 (*Dalea c. Francia* (dec.), 2010). L'esistenza di garanzie contro le arbitrarietà e la possibilità di ottenere il riesame della misura in questione, da parte di un organo indipendente e imparziale competente a riesaminare qualsiasi questione giuridica e fattuale pertinente, al fine di determinare la legittimità della misura e di censurare un eventuale abuso da parte delle autorità, sono essenziali (ibid., che rinvia a *Leander c. Svezia*, 1987, § 66).

281. Informazioni personali false o incomplete raccolte e conservate dalle autorità possono rendere più difficile la vita quotidiana della persona interessata (*Khelili c. Svizzera*, 2011, § 64), dimostrarsi diffamatorie (*Rotaru c. Romania* [GC], 2000, § 44) o eliminare diverse garanzie procedurali sostanziali previste dalla legge per proteggere i diritti delle persone interessate (*Cemalettin Canlı c. Turchia*, 2008, §§ 35, 40-42). In una causa in cui un fascicolo di polizia intitolato "nota informativa su altri reati" era stato presentato dinanzi a un tribunale nazionale e menzionava due azioni penali instaurate nei confronti dell'imputato in passato per partecipazione a organizzazioni illegali, la Corte ha constatato la violazione dell'articolo 8. In tale causa non solo le informazioni esposte nel fascicolo erano false, ma il fascicolo non aveva neanche menzionato l'assoluzione del ricorrente durante la prima azione penale e l'archiviazione del procedimento durante la seconda (ibid., § 42). La mancata menzione dell'esito dei due procedimenti aveva violato gli obblighi esposti inequivocabilmente nelle disposizioni nazionali,

e aveva quindi eliminato diverse garanzie procedurali sostanziali previste dalla legge per tutelare i diritti del ricorrente (ibid., 2008, § 42).

282. Il fatto di imporre a una persona che chiede la rettifica dei suoi dati personali nei registri ufficiali dello Stato un obbligo che crea per la stessa barriere insormontabili può risultare incompatibile con l'obbligo dello Stato di garantire l'effettivo rispetto della sua vita privata (*Ciubotaru c. Moldavia*, 2010, §§ 51-59). In una causa concernente l'incapacità del ricorrente di ottenere la modifica della registrazione della sua origine etnica nei registri ufficiali, l'obbligo di dimostrare che i suoi genitori appartenessero a uno specifico gruppo etnico aveva creato barriere insormontabili per l'interessato nel registrare un'origine etnica differente da quella registrata dalle autorità riguardo ai suoi genitori (ibid., § 57).

283. Nel contesto di domande di rettifica dei registri dello stato civile per tenere conto dello status successivo all'operazione di una persona transessuale, la coerenza delle prassi amministrative e giuridiche nell'ambito del sistema nazionale deve essere considerato un fattore importante nella valutazione di tali domande, svolta ai sensi dell'articolo 8 (*Christine Goodwin c. Regno Unito* [GC], 2002, § 78). In una causa concernente il rifiuto da parte delle autorità di modificare il registro delle nascite, la Corte ha dichiarato che era colpita dal fatto che il cambiamento di sesso, che era stato effettuato legalmente, non fosse riconosciuto pienamente dalla legge, in quanto esso avrebbe potuto essere considerato la fase finale e culminante nel lungo e difficile processo di trasformazione cui si era sottoposto il transessuale (ibid., § 78, che ribalta la sua giurisprudenza per tenere conto degli sviluppi della scienza e della società successivamente a sentenze più remote quali *Rees c. Regno Unito*, 1986, §§ 42-44, *Cossey c. Regno Unito,* 1990, §§ 39-40, e *Sheffield e Horsham c. Regno Unito* [GC], 1998, §§ 60-61). Se uno Stato ha autorizzato le cure e l'intervento chirurgico che alleviano la condizione di un transessuale, finanziato o contribuito a finanziare le operazioni e permette effettivamente l'inseminazione artificiale di una donna che vive con un transessuale, che è passato dal sesso femminile a quello maschile, sembra illogico rifiutare di riconoscere le conseguenze giuridiche del risultato cui conducono le cure (*Christine Goodwin c. Regno Unito* [GC], 2002, § 78), specialmente perché le difficoltà poste dalla rettifica della menzione del genere iniziale nel registro delle nascite non sono affatto insormontabili (ibid., § 91).

284. Nella causa *S.V. c. Italia*, 2018 (§ 72), il rifiuto da parte delle autorità di autorizzare la modifica del prenome di un transessuale, durante la procedura di transizione del genere e prima del completamento dell'operazione di cambiamento di sesso, era stato basato su una rigida procedura giudiziaria che aveva collocato la ricorrente per un tempo irragionevole (due anni e mezzo) in una situazione anomala in cui ella provava sensazioni di vulnerabilità.

285. Nella causa *Hämäläinen c. Finlandia* [GC], 2014 (§§ 87-89), la Corte ha ritenuto che non fosse stato sproporzionato esigere, quale condizione preliminare per il riconoscimento giuridico di un genere acquisito, che il matrimonio della ricorrente fosse convertito in un'unione registrata, poiché si trattava di una autentica opzione che forniva una protezione giuridica alle coppie omosessuali quasi identica a quella del matrimonio (in Finlandia il matrimonio omosessuale è illegale). Conseguentemente, le lievi differenze tra queste due nozioni giuridiche non erano tali da rendere l'attuale regime finlandese carente dal punto di vista dell'obbligo positivo dello Stato. Si veda altresì *A.P., Garçon e Nicot c. Francia*, 2017, concernente le condizioni giuridiche per una modifica dello stato civile in relazione a persone transgender, quali il carattere irreversibile della modifica dell'aspetto (§§ 116-135), la realtà del disturbo di identità di genere (§§ 138-144) e l'obbligo di sottoporsi a una visita medica (§§ 149-154).

3. Diritto alla cancellazione dei dati ("diritto all'oblio")

286. La Corte ha trattato la questione del diritto alla cancellazione dei dati personali ("diritto all'oblio"), dopo un preciso periodo di tempo, per quanto riguarda:

- una scelta o una prassi dei media di lasciare nei loro siti internet archivi comprendenti dati personali relativi a degli individui quali cognomi, prenomi e fotografie, che erano stati pubblicati in passato (*M.L. e W.W. c. Germania*, 2018);
- la capacità delle persone accusate, o semplicemente sospettate, della commissione di un reato, di ottenere dopo un certo periodo di tempo, l'eliminazione dei loro dati personali (profilo del DNA, fotografie identificative e impronte digitali) raccolti dalle autorità in banche dati finalizzate a prevenire e contrastare i reati (*B.B. c. Francia*, 2009; *Gardel c. Francia*, 2009; *M.B. c. Francia*, 2009; *M. K. c. Francia*, 2013; *Brunet c. Francia*, 2014; *Ayçaguer c. Francia*, 2017; *Catt c. Regno Unito*, 2019; *Gaughran c. Regno Unito*, 2020);
- l'incapacità di un individuo di ottenere l'eliminazione delle sue precedenti condanne dal casellario giudiziale dopo uno specifico periodo di tempo (*M.M. c. Regno Unito*, 2012);
- la protratta conservazione negli archivi dei Servizi di sicurezza dei dati personali dei ricorrenti, che non soddisfacevano più il requisito della "necessità in una società democratica" in considerazione della loro natura e dell'età (*Segerstedt-Wiberg e altri c. Svezia*, 2006).

287. Nel contesto degli archivi internet dei media contenenti i dati personali di un individuo che era stato in passato oggetto di pubblicazione, il "diritto all'oblio" è finalizzato a proteggere l'interessato permettendogli di chiedere la parziale o totale eliminazione dei risultati della ricerca connessi al suo nome, che egli riteneva inappropriati dopo un certo periodo di tempo (*M.L. e W.W. c. Germania*, 2018, § 100). Tale diritto non è assoluto. Per quanto possa essere importante, esso deve essere bilanciato con il diritto del pubblico generale di essere informato dei fatti avvenuti in passato e in relazione alla storia contemporanea, in particolare per mezzo degli archivi digitali della stampa (ibid., § 101). Oltre alla principale funzione della stampa di fornire informazioni e idee di interesse generale, essa ha un ruolo secondario, ma purtuttavia prezioso nel mantenere archivi contenenti notizie precedentemente pubblicate e metterle a disposizione del pubblico (ibid., § 90). Gli archivi internet danno un importante contributo nel conservare e nel mettere a disposizione notizie e informazioni. Gli archivi digitali costituiscono una importante fonte per l'istruzione e la ricerca storica, particolarmente poiché sono facilmente accessibili al pubblico e sono generalmente gratuiti (ibid., § 90, e i rinvii ivi contenuti).

288. Nella causa *M.L. e W.W. c. Germania*, 2018, due persone che erano state condannate per omicidio ed erano state scarcerate quattordici anni dopo, avendo espiato la loro pena detentiva, avevano chiesto senza successo che gli archivi internet del giornale eliminassero le loro fotografie e le indicazioni delle loro identità integrali (cognomi e prenomi) per consentire loro di rifarsi una vita lontano dalla vista del pubblico. La Corte non ha riscontrato alcuna violazione dell'articolo 8 in quanto l'interesse pubblico ad accedere ad archivi accurati e obiettivi dovrebbe avere la precedenza (ibid., § 116).

289. La sentenza relativa alla causa *M.L. e W.W. c. Germania*, 2018, suggerisce diversi indicatori sulla portata del "diritto all'oblio" nell'ambito degli archivi internet dei media comprendenti i dati personali di persone.

- secondo la Corte, sarebbe troppo complicato per i media dovere introdurre sistematicamente procedure per accettare richieste di anonimato, o almeno per valutarle in conformità ai criteri basati sul precedente. Tale obbligo pone il rischio che la stampa si astenga dal conservare dei rapporti nei suoi archivi online, o ometta di individuare le informazioni contenute nei suoi rapporti che potrebbero diventare oggetto di tali richieste (ibid., § 103).
- L'obbligo per i giornalisti di rendere un servizio anonimo è meno nocivo per la libertà di espressione della cancellazione di un intero rapporto (ibid., § 105, e i rinvii ivi citati). Tuttavia, l'approccio al trattamento di una data materia è una questione concernente la libertà giornalistica, e l'articolo 10 della Convenzione lascia ai giornalisti la facoltà di decidere quali particolari debbano essere pubblicati, al fine di assicurare la credibilità di un articolo, purché

le scelte che essi compiono al riguardo siano basate sulla loro deontologia professionale e sui loro codici di condotta. L'inserimento in un servizio di informazioni personalizzate, come il nome completo della persona interessata, è un importante aspetto dell'attività della stampa, specialmente quando essa si occupa di procedimenti penali che hanno suscitato notevole interesse.

- Il comportamento di una persona condannata che eccede il mero uso dei mezzi di ricorso disponibili ai sensi del diritto penale nazionale per impugnare la sua condanna può limitare la sua legittima aspettativa di ottenere l'anonimato nei servizi giornalistici, o perfino il diritto all'oblio online, anche quando si avvicina la data della sua scarcerazione (ibid., § 109).
- Si può tenere conto delle modalità di pubblicazione di un servizio, o di una fotografia e di presentazione della persona interessata in essi, nonché della portata della divulgazione del servizio o della fotografia (ibid., § 110). Delle immagini che mostravano un individuo con l'aspetto che aveva trent'anni prima, avevano ridotto la probabilità che fosse riconosciuto da terzi sulla base delle fotografie (ibid., § 115).

290. Nella causa *M.M. c. Regno Unito*, 2012 (§§187-207), la registrazione vita natural durante di un ammonimento nel casellario giudiziale di una persona ha dato luogo alla constatazione di violazione dell'articolo 8. La Corte ha ritenuto che una condanna o un ammonimento emessi in passato nei confronti di un individuo fossero diventati, con il decorso del tempo, parte integrante della sua vita privata, che doveva essere rispettata. Benché i dati contenuti nel casellario giudiziale fossero, in un certo senso, delle informazioni pubbliche, la loro sistematica memorizzazione in archivi centrali significava che essi potevano essere divulgati molto tempo dopo l'evento, quando chiunque tranne la persona interessata avrebbe probabilmente dimenticato l'incidente. La Corte ha ritenuto preoccupante il fatto che i criteri di riesame per consentire la cancellazione dei dati fossero molto restrittivi, e che le domande di cancellazione dei dati fossero accolte soltanto in casi eccezionali (ibid., § 202).

291. La Corte ritiene che se uno Stato spinge il suo margine di discrezionalità all'estremo, massimizzando i suoi poteri nella sfera della conservazione dei dati, vale a dire, memorizzando i dati a tempo indeterminato, è decisivo che debbano esservi garanzie effettive che prevedano la cancellazione dei dati personali quando il proseguimento della loro conservazione è diventato sproporzionato (*Catt c. Regno Unito*, 2019, § 119; *Gaughran c. Regno Unito*, 2020, § 94). In una causa in cui i dati biometrici e le fotografie del ricorrente, condannato per guida in stato di ebbrezza, erano stati conservati dalla Polizia in base a una politica di memorizzazione illimitata dei dati personali di qualsiasi persona ritenuta colpevole di un reato, la Corte ha constatato la violazione dell'articolo 8 (ibid., § 98). Non vi era alcuna disposizione che consentisse al ricorrente di ottenere la cancellazione dei dati che lo riguardavano se la loro conservazione non sembrava più necessaria in considerazione della natura del reato, dell'età della persona interessata, della quantità del tempo trascorso e dell'attuale personalità della persona. La Polizia poteva eliminare i dati biometrici e le fotografie delle persone condannate soltanto in casi eccezionali. Le possibilità di riesame erano talmente esigue da essere quasi ipotetiche (ibid., § 94).

292. L'assenza di garanzie effettive riguardo alla cancellazione di dati personali che non sono più pertinenti per quanto riguarda la finalità della loro memorizzazione è particolarmente preoccupante in caso di particolari categorie di dati sensibili, che esigono un maggiore livello di protezione (*Catt c. Regno Unito*, 2019, § 112). In una causa concernente la conservazione in una banca dati della Polizia di dati sensibili relativi a un manifestante pacifico, che rivelavano le sue opinioni politiche, la Corte ha constatato la violazione dell'articolo 8 (ibid., § 128). In assenza di disposizioni relative al termine massimo di memorizzazione di tali dati, il ricorrente era stato lasciato a dipendere interamente dalla diligenza con la quale le autorità avrebbero applicato le garanzie previste dal codice di condotta applicabile, che era molto elastico, al fine di assicurare la proporzionalità del periodo di conservazione dei suoi dati. La Corte ha ritenuto che la garanzia di ottenere l'eliminazione dei dati avesse un effetto

limitato se le autorità rifiutavano, a seguito di una domanda della persona interessata, di cancellare i dati in questione o di comunicare i motivi della loro decisione di conservarli (ibid., §§ 118 e 122).

293. In diverse cause relative alla conservazione dei dati personali di individui condannati per violenza sessuale, la Corte non ha riscontrato alcuna violazione dell'articolo 8, dopo avere osservato che gli interessati avevano avuto la possibilità di presentare una domanda di cancellazione dei dati se la conservazione dei loro dati non sembrava più pertinente, in considerazione, *inter alia*, del tempo decorso successivamente alla loro condanna (*B.B. c. Francia*, 2009, §§ 66-68; *Gardel c. Francia*, 2009, §§ 67-69; *M.B. c. Francia*, 2009, §§ 58-60).

294. Nella causa *Peruzzo e Martens c. Germania* (dec.), 2013 (§ 46), concernente la memorizzazione di dati personali in un file a seguito di una condanna per gravi reati connessi al traffico di sostanze stupefacenti, la Corte era convinta che benché la legge non prevedesse termini massimi per la memorizzazione di profili del DNA, l'Ufficio penale federale dovesse controllare a intervalli regolari non superiori a dieci anni se la memorizzazione dei dati continuasse a essere necessaria, tenendo conto in ciascun caso del fine della conservazione dei dati, nonché della natura e della gravità della circostanze del caso.

295. Nella causa *Ayçaguer c. Francia*, 2017 (§ 44), la Corte ha riscontrato la violazione dell'articolo 8 in quanto, a causa della sua durata e dell'impossibilità di eliminazione, le attuali disposizioni in materia di memorizzazione dei profili del DNA nella banca dati nazionale, cui il ricorrente si era opposto rifiutando di fornire un campione, non fornivano all'interessato una sufficiente protezione (ibid., § 45). La Corte ha sottolineato che le persone condannate dovrebbero, come le persone sospettate della commissione di un reato, prosciolte o assolte, avere la concreta possibilità di presentare una domanda di cancellazione dei dati memorizzati, che assicuri che il periodo di conservazione dei dati sia proporzionato alla natura dei reati e ai fini delle restrizioni (ibid., § 45; *B.B. c. Francia*, 2009, § 68; *Brunet c. Francia*, 2014, §§ 41-43).

296. In relazione alla possibilità di ottenere la cancellazione dei dati personali, il diritto di presentare in qualsiasi momento una domanda di cancellazione può contrastare con gli interessi delle autorità inquirenti, che esigono l'accesso a una banca dati con il maggior numero di riferimenti possibile. Conseguentemente, poiché gli interessi in gioco sono contrastanti, anche soltanto parzialmente, la cancellazione fornisce una garanzia che è "teorica e illusoria" piuttosto che "pratica ed effettiva" (*M. K. c. Francia*, 2013, §§ 44-47).

297. Nella causa *Segerstedt-Wiberg e altri c. Svezia*, 2006 (§§ 73-92), la memorizzazione nei registri dei Servizi di sicurezza dello Stato di dati personali molto remoti relativi alla presenza dei ricorrenti a una riunione politica, il fatto che essi avessero opposto una violenta resistenza ai controlli della Polizia durante delle manifestazioni, e la loro appartenenza a un preciso partito politico, aveva costituito violazione dell'articolo 8. La Corte ha ritenuto che l'interesse dello Stato a proteggere la sicurezza nazionale e a contrastare il terrorismo, che giustificava la raccolta e la memorizzazione delle informazioni in questione, avrebbe dovuto essere valutato in rapporto alla gravità dell'ingerenza nell'esercizio da parte di ciascun ricorrente del suo diritto al rispetto della sua vita privata. In considerazione della natura e del periodo al quale risalivano le informazioni relative ai ricorrenti, i motivi alla base della loro memorizzazione, benché pertinenti, non potevano essere considerati sufficienti trent'anni dopo (ibid., § 90).

298. Nel contesto dell'articolo 10, la Corte ha trattato "il diritto all'oblio" nella causa *Mediengruppe Österreich GmbH c. Austria*, 2022, concernente un decreto di un tribunale che proibiva a un quotidiano di pubblicare particolari informazioni su una persona, legate indirettamente alla campagna di un candidato politico nel periodo precedente l'elezione presidenziale. Il quotidiano aveva pubblicato una fotografia del fratello del capoufficio del candidato in un "ambiente di destra" e aveva rivelato che egli era un "neonazista condannato". Erano trascorsi oltre vent'anni tra tale condanna e la pubblicazione dell'articolo in questione, e circa diciassette anni dalla sua scarcerazione: inoltre la condanna era già stata eliminata dal suo casellario giudiziale all'epoca della pubblicazione in questione. Il Tribunale

superiore nazionale aveva sottolineato l'assenza di nesso temporale e aveva proibito alla società ricorrente di pubblicare fotografie del fratello del capoufficio senza il consenso di quest'ultimo se avesse riferito nel medesimo articolo che egli era un neonazista condannato nel rapporto di accompagnamento. La Corte non ha riscontrato alcuna violazione dell'articolo 10, sottolineando, in particolare, il tempo decorso tra la condanna, la scarcerazione e la pubblicazione dell'articolo in questione; la perdita di notorietà dell'interessato; il fatto che egli non avesse riportato alcuna ulteriore condanna penale; l'importanza del reinserimento nella società delle persone che hanno espiato la loro pena; e il loro legittimo e molto significativo interesse a non doversi più confrontare con la loro condanna dopo un certo periodo di tempo.

4. Diritto di beneficiare di speciali garanzie procedurali e di un quadro procedurale effettivo per difendere i propri diritti

299. Benché l'articolo 8 non contenga alcun esplicito requisito procedurale, è importante al fine dell'effettivo godimento dei diritti garantiti da tale disposizione che il pertinente processo decisionale sia equo e tale da offrire il dovuto rispetto agli interessi tutelati da esso. Tale processo può esigere l'esistenza di un quadro procedurale effettivo mediante il quale un ricorrente può esercitare i suoi diritti di cui all'articolo 8 a condizioni eque, anche in materia di prove (*I. c. Finlandia*, 2008, § 44; *Ciubotaru c. Moldavia*, 2010, § 51). Il fatto di imporre un obbligo che crea una barriera insormontabile per una persona che chiede la rettifica dei dati relativi alla sua identità, contenuti nei registri ufficiali dello Stato, può essere incompatibile con l'obbligo positivo dello Stato di garantire l'effettiva osservanza del diritto al rispetto della vita privata (ibid., §§ 51-59). In una causa concernente la rivelazione della sieropositività della ricorrente all'HIV, la Corte, constatando la violazione dell'articolo 8, ha attribuito importanza al fatto che lo Stato avesse imposto alla ricorrente un onere della prova eccessivamente pesante nell'ambito di un procedimento civile nel quale ella aveva chiesto il risarcimento per la diffusione di informazioni sul suo stato di salute (*I. c. Finlandia*, 2008, § 44).

300. Le restrizioni imposte dalla legge ai poteri dei tribunali nazionali di risarcire il danno causato dalla divulgazione, a mezzo stampa, di informazioni riservate sulla salute di persone identificate e di astenersi dal ricorrere a tali abusi, potevano ostacolare l'efficacia di un appello, e non fornivano quindi ai ricorrenti la protezione della loro vita privata che essi avrebbero potuto legittimamente attendersi. Pertanto, nelle cause *Armonienė c. Lituania*, 2008 (§§ 47-48) e *Biriuk c. Lituania*, 2008 (§§ 46-47), la Corte ha riscontrato la violazione dell'articolo 8 perché la Legge sulla divulgazione di informazioni al pubblico vigente all'epoca dei fatti aveva fissato un tetto superiore ai risarcimenti concessi dai tribunali nazionali a seguito della divulgazione di informazioni sulla loro sieropositività all'HIV sul più importante quotidiano nazionale, senza il loro consenso e rivelando le loro identità.

301. La mancata previsione da parte dello Stato, a livello nazionale, di un riesame indipendente della giustificazione della conservazione di dati personali raccolti nell'ambito di un procedimento penale, o successivamente a un procedimento penale, nel quale l'imputato era stato assolto, prosciolto, o condannato, costituisce un aspetto importante del quale si deve tenere conto nel determinare se tale conservazione dei dati sia compatibile con l'articolo 8 (*S. e Marper c. Regno Unito* [GC], 2008, §§ 119, 125). In una causa concernente la conservazione a tempo indeterminato di campioni cellulari, profili del DNA, e impronte digitali di due persone, dopo che un procedimento nei loro confronti si era concluso rispettivamente con un'assoluzione e un'archiviazione, la Corte ha constatato la violazione dell'articolo 8, osservando che i ricorrenti avevano avuto poche possibilità di ottenere l'eliminazione dei dati dalla banca dati nazionale o la distruzione dei campioni.

302. Nella causa *Vicent Del Campo c. Spagna*, 2018 (§§ 39, 53), l'impossibilità per il ricorrente, terzo in un procedimento giudiziario, di chiedere ai tribunali nazionali di astenersi dal comunicare la sua identità o informazioni personali che lo concernevano, prima della pronuncia di una sentenza, lo aveva privato di un quadro procedurale effettivo per difendere i suoi diritti.

303. Il mancato svolgimento da parte delle autorità dell'analisi della proporzionalità degli interessi concorrenti in gioco e dell'esame dei diritti del ricorrente alla vita privata e le questioni relative alla protezione dei dati viola i requisiti dell'articolo 8 della Convenzione (*Liebscher c. Austria*, 2021, §§ 64-69).

304. Nella causa *M.D. e altri c. Spagna*, 2022 (§§ 65-72) concernente la trasmissione alla stampa dei dati personali del ricorrente, contenuti nella banca dati della Polizia cui soltanto le autorità avevano accesso, la Corte ha ritenuto, per quanto riguarda tale illecita divulgazione di dati privati conservati da organi pubblici, che l'obbligo positivo di cui all'articolo 8 comportasse "l'obbligo di svolgere indagini effettive" al fine di determinare le circostanze in cui i giornalisti avevano ottenuto l'accesso ai dati e, se necessario, di sanzionare le persone responsabili degli inconvenienti verificatisi. Il mancato svolgimento di tali indagini da parte delle autorità costituiva violazione dell'articolo 8. Analogamente, nella causa *Y.G. c. Russia*, 2022, (§§ 46-53), in cui il ricorrente aveva lamentato che una banca dati contenente i suoi dati personali, tra cui informazioni relative alle sue condizioni di salute, fosse stata messa in vendita al mercato, la Corte ha ritenuto che a fronte di tale grave violazione della privacy, poiché il ricorrente aveva agito in proprio, senza il vantaggio di un'assistenza da parte dello Stato sotto forma di un'indagine ufficiale, egli non avesse avuto alcun mezzo effettivo per accertare gli autori di tali atti e quindi la sua denuncia non era stata un mezzo di ricorso inappropriato date le circostanze. Non avendo svolto un'indagine, le autorità avevano violato il loro obbligo positivo di garantire un'adeguata protezione al suo diritto al rispetto della sua vita privata.

305. L'efficacia dei ricorsi disponibili a livello nazionale alle persone che desideravano accedere ai propri dati personali esige che i ricorsi presentati dalle stesse siano trattati entro un termine ragionevole. Nella causa *Roche c. Regno Unito* [GC], 2005 (§§ 166-167, 169), la Corte ha constatato la violazione dell'articolo 8 a causa di un irragionevole periodo di attesa del ricorrente per accedere a documenti contenenti dati personali, che gli avrebbero consentito di valutare i potenziali rischi per la sua salute causati dalla sua partecipazione a test militari sui gas.

306. L'eccessiva importanza attribuita dalle autorità nazionali al requisito della riservatezza nei confronti dei dati di traffico di utenti di internet può, in determinate circostanze dimostrarsi contraria all'articolo 8 se ostacola l'efficacia di un'indagine penale, finalizzata a individuare e punire l'autore di un reato (*K.U. c. Finlandia,* 2008, § 49). Nella causa *K.U. c. Finlandia*, 2008 (§§ 49-50), la Corte ha riscontrato la violazione dell'articolo 8, data l'assenza di un quadro procedurale che permettesse l'identificazione e il perseguimento di una persona che aveva pubblicato un annuncio pubblicitario su internet, rendendo un minore il bersaglio di proposte da parte di pedofili, in modo da consentire alla vittima di chiedere il risarcimento alla persona in questione. La garanzia goduta dagli utenti di servizi di telecomunicazioni e di internet riguardo al rispetto della loro privacy è a volte superata da altre legittime preoccupazioni, quali la difesa dell'ordine e la prevenzione dei reati o la protezione dei diritti e delle libertà altrui.

307. Nell'ambito della sicurezza nazionale, chiunque sia oggetto di una misura per i summenzionati motivi deve poter ottenere il riesame della misura contestata da parte di un organo indipendente e imparziale, autorizzato a esaminare tutte le pertinenti questioni fattuali e giuridiche e, se necessario, a perseguire qualsiasi abuso commesso dalle autorità. Dinanzi a tale organo di riesame gli interessati devono potere beneficiare di un procedimento in contraddittorio che consenta loro di presentare il proprio punto di vista e confutare i rilievi formulati dalle autorità. Pertanto, nella causa *Dalea c. Francia* (dec.), 2010, la Corte ha ritenuto che la protratta registrazione dei dati personali del ricorrente nella banca dati Schengen potesse essere considerata "necessaria in una società democratica" perché egli aveva beneficiato di un riesame della misura contestata. Benché non fosse stato in grado di contestare il motivo specifico della registrazione dei suoi dati, egli aveva avuto cognizione di tutti gli altri dati che lo riguardavano, contenuti nella banca dati Schengen.

308. L'organo indipendente e imparziale cui qualsiasi persona oggetto di una misura per motivi di sicurezza nazionale deve poter chiedere un riesame della misura contestata non deve essere di natura

giudiziaria. Nella causa *Leander c. Svezia*, 1987 (§ 59), concernente l'utilizzo di un registro segreto della Polizia per assumere un falegname, la Corte non ha constatato alcuna violazione dell'articolo 8 a causa dell'esistenza di garanzie, tra cui la possibilità per il Parlamemto e per le istituzioni indipendenti di svolgere un riesame delle operazioni che autorizzano le pertinenti autorità nazionali a raccogliere e memorizzare in registri segreti informazioni relative agli individui e a utilizzarle successivamente (ibid., § 65), benché il ricorrente non avesse diritto a un ricorso giudiziario (ibid., §§ 62, 67). Al fine di valutare l'efficacia di un ricorso dinanzi a un organo responsabile a livello nazionale di rivedere la misura basata su motivi di sicurezza nazionale, si doveva tenere conto dei poteri e delle garanzie procedurali attuati dall'organo in questione (ibid., §§ 77, 80, 83-84). Un ricorso gerarchico a un diretto supervisore dell'autorità i cui atti sono contestati non soddisfa i richiesti criteri di indipendenza necessari perché costituisca una sufficiente protezione contro l'abuso di potere (*Roman Zakharov c. Russia* [GC], 2015, § 292).

309. Nell'ambito di misure di sorveglianza segreta, il riesame e la supervisione delle misure di sorveglianza segreta possono entrare in gioco in tre fasi: quando la sorveglianza è disposta per la prima volta, durante il suo svolgimento o successivamente alla sua concusione. Per quanto riguarda le prime due fasi, la natura e la logica stesse della sorveglianza segreta impongono che non soltanto la sorveglianza bensì anche il riesame che l'accompagna debbano essere effettuati all'insaputa della persona. Conseguentemente, poiché alla persona dovrà essere necessariamente impedito di chiedere un ricorso effettivo di propria iniziativa, o di partecipare direttamente a un procedimento di riesame, è essenziale che le procedure istituite prevedano garanzie adeguate ed equivalenti, che tutelino i suoi diritti. In un campo in cui l'abuso è potenzialmente così facile in singoli casi e potrebbe avere conseguenze nocive per la società democratica nel suo insieme, è in linea di principio auspicabile affidare la supervisione a un giudice, poiché il controllo giudiziario offre le migliori garanzie di indipendenza, di imparzialità e di una procedura corretta (ibid., § 233; *Klass e altri c. Germania*, 1978, §§ 55-56).

310. Per quanto riguarda la terza fase, successivamente alla conclusione della sorveglianza, la questione della successiva notifica delle misure di sorveglianza è inscindibilmente legata all'efficacia dei ricorsi dinanzi ai tribunali e quindi all'esistenza di effettive garanzie contro l'abuso dei poteri di controllo (*Roman Zakharov c. Russia* [GC], 2015, § 234). Vi è in linea di principio uno scarso margine di ricorso ai tribunali da parte dell'interessato, tranne se quest'ultimo è informato delle misure adottate a sua insaputa e quindi in grado di impugnarne la legalità retroattivamente (*Klass e altri c. Germania*, 1978, §§ 57-59; *Weber e Saravia c. Germania* (dec.), 2006, §§ 135-137), o se una persona che sospetta che le sue comunicazioni siano o siano state intercettate può rivolgersi ai tribunali, cosicché la competenza dei tribunali non dipende dalla notifica alla persona intercettata del fatto che le sue comunicazioni sono state intercettate (*Kennedy c. Regno Unito*, 2010, §§ 167, 169; *Roman Zakharov c. Russia* [GC], 2015, § 234).

311. Nelle cause *Klass e altri c. Germania*, 1978 (§§ 57-59) e *Weber e Saravia c. Germania* (dec.), 2006 (§§ 135-137), la Corte ha ritenuto che i ricorsi disponibili a livello interno fossero adeguati. Le persone le cui comunicazioni eramo state controllate erano state informate appena possibile, senza compromettere il fine del controllo. I ricorsi erano anche stati accompagnati da garanzie effettive, come il fatto che un organo indipendente era autorizzato a decidere se una persona sottoposta a controllo avrebbe dovuto essere informata della misura. Invocando tale notifica, la persona aveva varie opzioni giudiziarie, per esempio instaurare un'azione civile risarcitoria, o un ricorso alla Corte costituzionale federale per una pronuncia circa l'eventuale violazione della Legge fondamentale (*Klass e altri c. Germania*, 1978, §§ 57, 24).

312. Per gli ordinamenti che non prevedono la notifica alla persona interessata delle misure adottate nei suoi confronti, il fatto che le persone interessate che ritengono che il loro diritto al rispetto della loro vita privata sia stato violato da una misura di controllo segreto possano adire un organo indipendente e imparziale, anche se non sono state informate anticipatamente dell'intercettazione delle loro comunicazioni, è stato considerato dalla Corte un'importante garanzia, in una causa in cui

essa non ha riscontrato alcuna violazione dell'articolo 8 (*Kennedy c. Regno Unito*, 2010, §§ 167, 169). Per contro, se i ricorsi disponibili ai sensi del diritto interno sono accessibili unicamente a persone che dispongono di un minimo di informazioni sulle misure contestate, la Corte ha ritenuto che gli interessati non disponessero di un ricorso effettivo contro le misure di sorveglianza segreta, in violazione dell'articolo 8 (*Roman Zakharov c. Russia* [GC], 2015, §§ 293-298, 305).

III. Interazione con altre disposizio ni della Convenzione e dei suoi Protocolli

313. Oltre al diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza garantito dall'articolo 8 della Convenzione, che è la principale fonte di protezione dei dati personali nel sistema della Convenzione, le questioni connesse a tale protezione possono entrare in gioco anche ai sensi di altre disposizioni della Convenzione e dei suoi Protocolli. In tali casi il compito principale della Corte è quello di valutare tale protezione e conciliarla con altri diritti e interessi legittimi. In alcuni casi, la questione della protezione dei dati personali ha consentito alla Corte di determinare la portata di un altro diritto garantito dalla Convenzione e dai suoi Protocolli aggiuntivi.

A. Protezione dei dati e diritti sostanziali[10]

Articolo 9 della Convenzione

"1. Ogni persona ha diritto alla libertà di pensiero, di coscienza e di religione; tale diritto include la libertà di cambiare religione o credo, così come la libertà di manifestare la propria religione o il proprio credo individualmente o collettivamente, in pubblico o in privato, mediante il culto, l'insegnamento, le pratiche e l'osservanza dei riti.

2. La libertà di manifestare la propria religione o il proprio credo non può essre oggetto di restrizioni diverse da quelle che sono stabilite dalla legge e che costituiscono misure necessarie, in una società democratica, alla pubblica sicurezza, alla protezione dell'ordine, della salute e della morale pubblica, o alla protezione dei diritti e delle libertà altrui."

Articolo 10 della Convenzione

"1. Ogni persona ha diritto alla libertà di espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera. Il presente articolo non impedisce agli Stati di sottoporre a un regime di autorizzazione le imprese di radiodiffusione, cinematografiche o televisive.

2. L'esercizio di queste libertà, poiché comporta doveri e responsabilità, può essere sottoposto alle formalità, condizioni, restrizioni o sanzioni che sono previste dalla legge e che costituiscono misure necessarie, in una società democratica, alla sicurezza nazionale, all'integrità territoriale o alla pubblica sicurezza, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, alla protezione della reputazione o dei diritti altrui, per impedire la divulgazione di informazioni riservate o per garantire l'autorità e l'imparzialità del potere giudiziario."

Articolo 14 della Convenzione

"Il godimento dei diritti e delle libertà riconosciuti nella presente Convenzione deve essere assicurato senza nessuna discriminazione, in particolare quelle fondate sul sesso, la razza, il colore, la lingua, la religione, le opinioni politiche o quelle di altro genere, l'origine nazionale o sociale, l'appartenenza a una minoranza nazionale, la ricchezza, la nascita od ogni altra condizione."

Articolo 1 del Protocollo n. 1

"Ogni persona fisica o giuridica ha diritto al rispetto dei suoi beni. Nessuno può essere privato della sua proprietà se non per causa di pubblica utilità e nelle condizioni previste dalla legge, e dai suoi principi generali del diritto internazionale.

Le disposizioni precedenti non portano pregiudizio al diritto degli Stati di porre in vigore le leggi da essi ritenute necessarie per disciplinare l'uso dei beni in modo conforme all'interesse generale o per assicurare il pagamento delle imposte o di altri contributi o delle ammende."

[10] Il presente capo dovrebbe essere letto alla luce e congiuntamente alla Guida all'articolo 9, alla Guida all' articolo 10, alla Guida all'articolo 14 e all'articolo 1 del Protocollo N. 12 e alla Guida all'articolo 1 del Protocollo N. 1.

Articolo 2 del Protocollo n. 4

"1. Chiunque si trovi regolarmente sul territorio di uno Stato ha il diritto di circolarvi liberamente e di fissarvi liberamente la sua residenza.

2. Ognuno è libero di lasciare qualsiasi Paese, compreso il proprio.

3. L'esercizio di tali diritti non può essere oggetto di restrizioni diverse da quelle che sono previste dalla legge e che costituiscono, in una società democratica, misure necessarie alla sicurezza nazionale, alla pubblica sicurezza, al mantenimento dell'ordine pubblico, alla prevenzione delle infrazioni penali, alla protezione della salute o della morale o alla protezione dei diritti e libertà altrui.

4. I diritti riconosciuti al paragrafo 1 possono anche, in alcune zone determinate, essere oggetto di restrizioni previste dalla legge e giustificate dall'interesse pubblico in una società democratica."

1. Protezione dei dati e libertà di pensiero, di coscienza e di religione (articolo 9 della Convenzione)

314. La Corte ha constatato la violazione dell'articolo 9 in alcune cause che sollevano anche la questione della protezione dei dati personali, mentre in altre cause non ha riscontrato alcuna violazione.

315. Nella causa *Sinan Işık c. Turchia*, 2010 (§§ 37-53), la Corte ha dovuto affrontare la questione della menzione – obbligatoria o facoltativa – della confessione religiosa del ricorrente sulla sua carta d'identità. Secondo la Corte, il fatto di dover chiedere per iscritto alle autorità di modificare la menzione relativa alla religione nei registri civili e sulla carta d'identità, e analogamente, il mero fatto di essere titolare di una carta d'identità sulla quale la casella relativa alla "religione" era lasciata in bianco, obbligava la persona a divulgare, contro la sua volontà, informazioni concernenti un aspetto della sua religione o delle sue convinzioni più personali. La Corte ha constatato la violazione dell'articolo 9, dopo avere ribadito che la libertà di manifestare la propria religione o le proprie convinzioni aveva anche un aspetto negativo, vale a dire il diritto di una persona di non essere obbligato a rivelare la propria religione o ad agire in modo tale da permettere di concludere che la persona avesse - o non avesse – tali convinzioni. Benché la casella della religione potesse essere lasciata in bianco, il mero fatto di farlo aveva di per sé una specifica connotazione, in quanto avrebbe consentito inevitabilmente di operare una distinzione tra i titolari di una carta d'identità contenente l'informazione in questione e quelli che avevano scelto di non indicarla (ibid., § 51).

316. Nella causa *Alexandridis c. Grecia*, 2008 (§ 41), l'obbligo per un avvocato di rivelare al tribunale di non essere cristiano ortodosso, e che desiderava compiere una dichiarazione solenne, piuttosto che un giuramento religioso, aveva costituito un'ingerenza nei suoi diritti di cui all'articolo 9. Le autorità statali non avevano il diritto di intervenire nella sfera della coscienza individuale e di accertare le convinzioni religiose delle persone, o di obbligarle a rivelare le proprie convinzioni in materia spirituale. Ciò era ancora più valido nei casi in cui una persona era obbligata a compiere una simile azione al fine di eseguire alcuni compiti, in particolare al momento di prestare un giuramento (ibid., § 38). Nella causa *Dimitras e altri c. Grecia*, 2010 (§ 88), anche l'obbligo per i ricorrenti di rivelare le proprie convinzioni religiose, al fine di non prestare un giuramento religioso in qualità di testimoni in un procedimento penale, è stato considerato in violazione dell'articolo 9. La Corte ha ritenuto che fosse difficile conciliare con la libertà di religione le disposizioni del codice di procedura penale che prevedevano che, al fine di verificare la loro identità, tutti i testimoni dovessero dichiarare, tra le altre informazioni, la loro religione prima di deporre (ibid., § 88).

317. Nella causa *Mockutė c. Lituania*, 2018 (§ 129), la Corte era pronta ad accettare che l'esigenza di cure psichiatriche avrebbe potuto rendere necessario che uno psichiatra discutesse di varie questioni con un paziente, compreso di religione. Tuttavia, tali discussioni non avrebbero dovuto avere la forma

di indagini da parte degi psichiatri circa le convinzioni dei pazienti, al fine di "correggerle", quando non vi era un chiaro e imminente rischio del fatto che tali convinzioni avrebbero potuto manifestarsi con azioni pericolose per il paziente e per altri. Uno Stato non poteva imporre ciò che una persona doveva credere, o adottare misure coercitive per farle modificare le proprie convinzioni, né la portata del margine di discrezionalità degli Stati poteva essere più ampia o più esigua a seconda della natura delle convinzioni religiose.

2. Protezione dei dati e libertà di espressione (articolo 10 della Convenzione)[11]

318. Come regola generale, nelle cause in cui la Corte ha dovuto ponderare e conciliare il diritto alla protezione dei dati personali garantito dall'articolo 8 con il diritto alla libertà di espressione di cui all'articolo 10, essa ha ritenuto che l'esito non avrebbe dovuto, in via di principio, variare a seconda del fatto che il ricorso fosse stato presentato ai sensi dell'articolo 8 o ai sensi dell'articolo 10. Secondo la Corte, i due diritti meritano uguale rispetto (*Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia* [GC], 2017, § 163; *Alpha Doryforiki Tileorasi Anonymi Etairia c. Grecia*, 2018, § 46).

319. Il rifiuto da parte delle autorità di fornire a organizzazioni non governative l'accesso a determinate informazioni contenenti dati personali detenuti dallo Stato è stato ritenuto in violazione dell'articolo 10 nelle seguenti cause:

- *Centro per la democrazia e lo stato di diritto c. Ucraina*, 2020 (§§ 120-121), concernente il rifiuto della Commissione elettorale centrale di fornire a una ONG copie dei *curriculum vitae* dei leaders di partiti politici che si erano candidati alle elezioni parlamentari, in quanto le informazioni richieste erano riservate e potevano essere rivelate nella loro integralità soltanto con il consenso delle persone interessate;
- *Magyar Helsinki Bizottság c. Ungheria* [GC], 2016 (§§ 195-197, 200), nella quale le autorità avevano rifiutato di fornire a ONG che svolgevano uno studio i nominativi di difensori nominati d'ufficio e il numero delle rispettive nomine;
- *Youth Initiative for Human Rights c. Serbia*, 2013 (§§ 24-26), concernente il rifiuto di un'agenzia di intelligence di fornire informazioni a una ONG, benché le fosse stato ordinato di farlo.

320. In relazione alla divulgazione di dati personali nella stampa scritta o nei mezzi di informazione audiovisivi, la Corte ha riscontrato la violazione dell'articolo 10 in diverse cause tra cui:

- *N. Š. c. Croazia*, 2020 (§§ 92-117), nella quale la ricorrente era stata condannata per avere divulgato in televisione informazioni presumibilmente riservate che aveva ottenuto nel corso di un procedimento amministrativo relativo all'affidamento di un minore. La Corte ha ritenuto che, a causa della vulnerabilità dei minori, la protezione dei loro dati personali fosse essenziale (ibid., § 99). Tuttavia, l'approccio indebitamente formalistico adottato dai tribunali nazionali, che non avevano tenuto conto del contesto della divulgazione, e in particolare del fatto che le informazioni fossero già di dominio pubblico, era incompatibile con l'articolo 10 (ibid., §§ 115-116);
- *Gîrleanu c. Romania*, 2018 (§§ 68-100), relativo a un ordine al ricorrente di pagare una sanzione amministrativa per avere divulgato informazioni militari riservate nell'ambito di un'inchiesta giornalistica;

[11] Il presente capo dovrebbe essere letto alla luce e congiuntamente alla Guida all'articolo 10 (si vedano, in particolare, le pp. 26-47; 58-60 e 62-65).

- *Couderc et Hachette Filipacchi Associés c. Francia* [GC], 2015 (§§ 94-153), relativa alla condanna del direttore editoriale e dell'editore di una rivista settimanale per la pubblicazione di un articolo che rivelava l'esistenza del figlio segreto di un monarca;
- *Axel Springer AG c. Germania* [GC], 2012 (§§ 75-111), relativa al divieto di informare dell'arresto e della condanna di un noto attore;
- *Dupuis e altri c. Francia*, 2007 (§§ 30-32, 39-49), relativa alla condanna di giornalisti per avere utilizzato e riprodotto nel loro libro informazioni provenienti da un fascicolo relativo a un'indagine giudiziaria in corso, compresi i dati personali dell'imputato.

321. Per contro, la Corte non ha riscontrato alcuna violazione dell'articolo 10 in diverse cause tra le quali:

- *Biancardi c. Italia*, 2021 (§§ 67-71) relativa alla compatibilità con l'articolo 10 di una sentenza civile nei confronti di un giornalista per non avere deindicizzato informazioni sensibili pubblicate su internet concernenti il procedimento penale nei confronti di un privato e la decisione del giornalista di mantenere le informazioni facilmente accessibili nonostante l'opposizione della persona;
- *Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia* [GC], 2017 (§§ 139-199), relativa a una decisione giudiziaria che proibiva la pubblicazione in massa di dati fiscali personali;
- *Bédat c. Svizzera* [GC], 2016 (§§ 44-82), sulla condanna di un giornalista per avere pubblicato informazioni coperte dal segreto istruttorio;
- *Mediengruppe Österreich GmbH c. Austria*, 2022 (§§ 44-73), relativa all'ordine di un tribunale che imponeva a un quotidiano di non pubblicare una fotografia accompagnata dalla didascalia "neonazista condannato" in relazione a una persona legata indirettamente alla campagna di un candidato all'elezione presidenziale, poiché la pubblicazione pertinente aveva avuto luogo oltre vent'anni dopo la condanna;
- *Gafiuc c. Romania*, 2020 (§§ 85-90), relativa alla revoca dell'accreditamento concesso a un giornalista per compiere ricerche negli archivi della Sicurezza, a seguito della divulgazione in diversi articoli scritti dallo stesso, di dati personali in forma "grezza" relativi a varie note figure dello sport, senza che la pertinenza dei dati fosse stata valutata alla luce del fine dichiarato della ricerca, vale a dire lo sport in Romania durante il regime comunista;
- *Giesbert e altri c. Francia*, 2017 (§§ 77-103), relativa alla condanna di un giornale da parte dei tribunali per avere pubblicato dei documenti concernenti un procedimento penale prima che fossero letti in una pubblica udienza;
- *Verlagsgruppe Droemer Knaur GmbH & Co. KG c. Germania*, 2017 (§§ 36-62), relativa all'ordine impartito a una società editrice di pagare un risarcimento per non avere svolto una ricerca minuziosa e per la grave ingerenza nei diritti della personalità di un individuo;
- *Kurier Zeitungsverlag und Druckerei GmbH c. Austria*, 2012 (§§ 47-56), relativa all'obbligo di pagare un risarcimento a una minore vittima di abusi sessuali e la cui identità era stata divulgata in un articolo della stampa. In considerazione della vulnerabilità delle vittime di reato, la loro identità meritava particolare protezione;
- *MGN Limited c. Regno Unito*, 2011 (§ 152), nella quale la Corte era persuasa, tra le altre considerazioni, del fatto che la divulgazione a mezzo stampa di particolari relativi alla terapia seguita da una celebrità per la tossicodipendenza fosse pericolosa e rischiasse di essere molto nociva alla sua guarigione;
- *Editions Plon c. Francia*, 2004 (§§ 22-55), relativa alla sospensione definitiva della diffusione di un libro contenente informazioni concernenti un capo di stato defunto e coperte dal segreto medico.

322. In relazione alla diffusione di immagini personali nella stampa scritta o mediante i mezzi d'informazione audiovisivi, e alle disposizioni dei tribunali che vietavano la diffusione di tali dati

personali, la Corte ha riscontrato la violazione dell'articolo 10 in diverse cause tra cui: *Pinto Coelho c. Portogallo (n. 2)*, 2016 (§§ 31-56), relativa alla condanna di una giornalista per avere diffuso senza autorizzazione la registrazione di un'udienza; *Haldimann e altri c. Svizzera*, 2015 (§§ 63-68), nella quale quattro giornalisti, che perseguivano un fine d'interesse pubblico, erano stati condannati per avere registrato e diffuso un'intervista con un broker assicurativo privato, utilizzando una telecamera nascosta; *Krone Verlag GmbH & Co. KG c. Austria*, 2002, (§§ 21-39), relativa al divieto di pubblicare la fotografia di un uomo politico; e *News Verlags GmbH & Co. KG c. Austria*, 2000 (§§ 37-60), relativa al divieto per un quotidiano di pubblicare la fotografia di un indagato nell'ambito di un procedimento penale.

323. Tuttavia, la diffusione di tali immagini o gli ordini di non diffonderle, non sono stati considerati violazione dell'articolo 10 nelle seguenti cause: *Société de Conception de Presse et d'Édition c. Francia*, 2016 (§§ 32-54), relativa all'ordine da parte di un tribunale di cancellare in una rivista già in vendita la fotografia di una persona che era stata tenuta prigioniera e torturata; *Axel Springer SE and RTL Television GmbH c. Germania*, 2017 (§§ 43-59), relativa alla decisione di vietare la pubblicazione di immagini che avrebbero permesso l'identificazione di una persona processata per omicidio; *Egeland e Hanseid c. Norvegia*, 2009 (§§ 56-65), relativa alla condanna dei caporedattori di due quotidiani per avere pubblicato le fotografie di una persona che stava per essere condotta in carcere, per iniziare a espiare una lunga pena. Si vedano altresì i paragrafi 17 e 65 *supra* relativi alla causa *Vučina c. Croazia* (dec.) 2019.

324. Nella causa *Alpha Doryforiki Tileorasi Anonymi Etairia c. Grecia*, 2018 (§§ 59-69, 77-78), la diffusione, a fini giornalistici, di diversi video filmati mediante una telecamera nascosta, nell'ambito della sorveglianza segreta di una figura pubblica, ha dato luogo alla constatazione di violazione e a un'altra constatazione di non violazione dell'articolo 10, a seconda del fatto che la registrazione fosse stata effettuata in uno spazio pubblico o privato.

325. In relazione alla pubblicazione su internet da parte di privati delle immagini di altri individui filmati segretamente, senza il consenso degli interessati, nella causa *Khadija Ismayilova c. Azerbaigian*, 2019 (§§ 158-166), la Corte ha constatato che lo Stato convenuto non aveva protetto la ricorrente, una giornalista che era stata filmata da persone ignote che avevano utilizzato telecamere nascoste installate nel suo appartamento. L'ingiustificata diffusione pubblica da parte delle autorità, in un comunicato-stampa che pretendeva di fornire un aggiornamento sull'indagine penale, di dati personali quali il nome della ricorrente e gli indirizzi di amici e colleghi della stessa aveva ulteriormente aggravato la situazione, in contrasto con lo spirito di un ambiente protettivo nei confronti del giornalismo (ibid., § 165).

326. In una causa relativa alla protezione della libertà di espressione di un segnalatore e la diffusione di informazioni riservate concernenti la sicurezza dello Stato, la Corte ha riscontrato la violazione dell'articolo 10 a causa della condanna del ricorrente per avere reso pubbliche diverse irregolarità nella raccolta di dati personali da parte dei Servizi segreti, che egli aveva individuato nel corso della sua attività professionale (*Bucur e Toma c. Romania*, 2013, §§ 95-120). In un'altra causa relativa a un segnalatore, il vice-primario di un ospedale pubblico era stato licenziato dopo avere riferito i suoi sospetti, che erano stati successivamente ritenuti infondati, di eutanasia attiva da parte del suo superiore. La Corte non ha riscontrato alcuna violazione dell'articolo 10: il ricorrente aveva basato i suoi sospetti sulle informazioni disponibili nelle cartelle cliniche elettroniche (che, come egli sapeva, non contenevano tutte le informazioni relative alla salute dei pazienti) e non sulle cartelle cartacee (che contenevano tutte le informazioni). Pertanto, benché avesse agito in buona fede, non aveva verificato attentamente che le informazioni diffuse fossero accurate e attendibili (*Gawlik c. Liechtensten*, 2021, §§ 74-78).

327. La questione della protezione dei dati personali dei giornalisti, o dei dati di cui essi erano in possesso, che potevano comportare la scoperta delle loro fonti, è stata esaminata dalla Corte in diverse cause tra cui:

- *Sedletska c. Ucraina*, 2021 (§§ 59-60 e 64-73), nella quale l'autorizzazione giudiziaria concessa alle autorità inquirenti per accedere e raccogliere i dati delle comunicazioni di una giornalista – date, ore e posizione del suo telefono cellulare in prossimità delle strade e dei luoghi specificati per un periodo di sedici mesi – memorizzati dal suo operatore di telefonia mobile, è stata ritenuta in violazione dell'articolo 10 in quanto non era giustificata da una "imperativa esigenza di interesse pubblico" e difettava di garanzie procedurali;
- *Jecker c. Svizzera*, 2020 (§§ 37-43), nella quale l'ordine impartito a una giornalista di rivelare l'identità delle sue fonti, al fine di aiutare le autorità inquirenti a identificare uno spacciatore di sostanze stupefacenti, è stato ritenuto dalla Corte contrario all'articolo 10, in assenza di bilanciamento degli interessi specifici in gioco;
- *Telegraaf Media Nederland Landelijke Media B.V. e altri c. Paesi Bassi*, 2012 (§ 102), nella quale la sorveglianza disposta nei confronti di giornalisti, senza un precedente riesame da parte di un organo indipendente, e l'ordine di consegnare dei documenti in grado di condurre all'identificazione delle loro fonti, sono stati considerati in violazione degli articoli 8 e 10 in combinato disposto. Un riesame *post factum* non sarebbe stato sufficiente poiché la riservatezza delle fonti giornalistiche non poteva essere rispristinata una volta che era stata distrutta (ibid., §§ 100-101);
- *Financial Times Ltd e altri c. Regno Unito*, 2009 (§ 63), nella quale la Corte ha precisato che la condotta della fonte non avrebbe mai potuto essere decisiva nel determinare se dovesse essere ordinata la rivelazione, ma avrebbe rappresentato meramente un fattore, benché importante, di cui tenere conto nello svolgimento della necessaria ponderazione;
- *Weber e Saravia c. Germania* (dec.), 2006 (§§ 143-153), nella quale la Corte ha dichiarato manifestamente infondata una doglianza relativa alla violazione della libertà di espressione derivante dalle disposizioni di una legge, che autorizzava il controllo strategico delle telecomunicazioni e impediva ai giornalisti di garantire che le informazioni che essi ricevevano nel corso della loro attività rimanessero riservate;
- *Ernst e altri c. Belgio*, 2003 (§§ 94-105), nella quale le perquisizioni e i sequestri su larga scala nell'ufficio di giornalisti, finalizzati a individuare le loro fonti, sono stati ritenuti in violazione dell'articolo 10. (Si vedano altresì le cause *Roemen e Schmit c. Lussemburgo*, 2003, §§ 47-60, relativa alle perquisizioni svolte nell'abitazione di una giornalista finalizzate a individuare le sue fonti; *Tillack c. Belgio*, 2007, §§ 56-68, relativa a operazioni di perquisizione e sequestro svolte nell'ufficio di un giornalista sospettato della corruzione di un funzionario europeo per ottenere informazioni riservate su indagini in corso in seno alle istituzioni europee, al fine di identificare la fonte delle divulgazioni; *Sanoma Uitgevers B.V. c. Paesi Bassi* [GC], 2010, §§ 64-100, relativa al sequestro da parte della polizia di documenti che avrebbero permesso di identificare le fonti giornalistiche; *Nagla c. Lettonia*, 2013, §§ 78-102, relativa a perquisizioni urgenti nell'abitazione di una giornalista, che avevano comportato il sequestro di dispositivi per memorizzare i dati contenenti le sue fonti informative; *Sérvulo & Associados-Sociedade de Advogados, RL e altri c. Portogallo*, 2015, §§ 101-120, relativa al sequestro su larga scala dei files e delle e-mails di un computer in uno studio legale; e *Görmüş e altri c. Turchia*, 2016, §§ 32-77, relativa alla protezione delle fonti di un giornalista, che erano dei funzionari statali, i quali avevano segnalato delle prassi scorrette nel loro posto di lavoro, nel contesto della riservatezza delle questioni militari); e
- *Big Brother Watch e altri c. Regno Unito* [GC], 2021, §§ 442-458, relativa all'intercettazione in massa delle comunicazioni, che aveva permesso ai Servizi segreti di accedere inavvertitamente a un elevato volume di materiale giornalistico riservato quale "cattura accidentale" dell'operazione di massa. La Corte ha constatato la violazione dell'articolo 10 della Convenzione.

3. Protezione dei dati e divieto di discriminazione (articolo 14 della Convenzione)

328. Nella causa *Sheffield e Horsham c. Regno Unito* [GC], 1998 (§§ 51-61, 76-77), concernente la questione di sapere se lo Stato convenuto fosse obbligato a riconoscere giuridicamente la nuova identità di genere delle due ricorrenti, che si erano sottoposte a un intervento chirurgico per passare dal sesso maschile a quello femminile, la Corte ha ritenuto che non vi fosse stata alcuna violazione dell'articolo 8 considerato singolarmente o in combinato disposto con l'articolo 14. Secondo la Corte, le situazioni in cui le ricorrenti avrebbero potuto dovere rivelare i loro dati personali non avvenivano con una frequenza tale da poter affermare che si ripercuotessero in misura sproporzionata sul loro diritto al rispetto della loro vita privata. La Corte ha inoltre osservato che lo Stato convenuto si era sforzato in una certa misura di minimizzare domande invasive riguardo al genere delle persone transessuali, permettendo che fossero rilasciati alle stesse patenti di guida, passaporti e altri tipi di documenti ufficiali con il loro nuovo nome e genere, e che l'utilizzo di certificati di nascita quale mezzo di identificazione era ufficialmente scoraggiato (ibid., § 59; *Cossey c. Regno Unito*, 1990, §§ 36-42).

329. In alcune cause in cui ha esaminato questioni strettamente connesse alla protezione dei dati personali ai sensi dell'articolo 8 o dell'articolo 9, la Corte non ha riscontrato alcuna questione distinta ai sensi dell'articolo 14 (*Sinan Işık c. Turchia,* 2010, § 57, relativa alla menzione – obbligatoria o facoltativa – della religione del ricorrente sulla sua carta d'identità; *Avilkina e altri c. Russia*, 2013, § 61, relativa alla divulgazione delle cartelle cliniche di diversi Testimoni di Geova che avevano rifiutato di sottoporsi a trasfusioni ematiche; *Christine Goodwin c. Regno Unito* [GC], 2002, §§ 92-93 e 108, e *I. c. Regno Unito* [GC], 2006, §§ 72-73, 88, relativa al riconoscimento giuridico del cambiamento di genere di un individuo).

4. Protezione dei dati e diritto al rispetto dei beni (articolo 1 del Protocollo n. 1)

330. La Corte ha trattato la protezione dei dati personali e il diritto al pacifico godimento dei beni nell'ambito delle perquisizioni e dei sequestri.

331. Nella causa *Smirnov c. Russia*, 2007 (§§ 53-59), la Corte ha ritenuto che le autorità nazionali non fossero pervenute a un "giusto equilibrio" tra le esigenze dell'interesse generale della comunità e le esigenze di protezione del diritto del ricorrente al pacifico godimento dei suoi beni. Vi era pertanto stata violazione dell'articolo 1 del Protocollo n. 1, in ragione della perquisizione svolta nell'abitazione del ricorrente, che era un avvocato, seguita dal sequestro, tra altri articoli, dell'unità centrale del suo computer, contenente gli hard disk con i suoi dati personali. Benché la conservazione delle prove materiali potrebbe essere necessaria negli interessi della buona amministrazione della giustizia, il computer stesso non era un oggetto, uno strumento o un prodotto del reato. Poiché le informazioni memorizzate sull'hard disk, che erano potenzialmente preziose e strumentali per l'indagine, erano state esaminate dall'investigatore, stampate e versate nel fascicolo, non sussisteva alcun motivo per proseguire il trattenimento dell'unità centrale. Inoltre, il computer era lo strumento di lavoro del ricorrente ed era utilizzato anche per memorizzare i dati dei suoi assistiti.

332. Nella causa *Kruglov e altri c. Russia*, 2020 (§§ 145-146), le perquisizioni svolte dalla Polizia nelle abitazioni e negli uffici dei ricorrenti, che esercitavano la professione di avvocato, e dei loro assistiti, e il sequestro di computer e hard disk contenenti informazioni personali e documenti protetti dal segreto professionale – che non erano di per sé un oggetto, uno strumento o un prodotto di un reato – sono state ritenute in violazione dell'articolo 1 del Protocollo n. 1.

333. Nella causa *Pendov c. Bulgaria*, 2020 (§§ 43-51), la Corte ha ritenuto che la conservazione inutilmente protratta del server del computer del ricorrente, nell'ambito di un procedimento penale nei confronti di terzi, costituisse violazione dell'articolo 1 del Protocollo n. 1. Il fatto che il server non fosse mai stato esaminato ai fini dell'indagine penale che riguardava unicamente terzi; la possibilità di

copiare le informazioni necessarie; l'importanza del server per l'attività professionale del ricorrente; e la parziale inerzia della Procura, significavano tutti che il trattenimento del server per sette mesi e mezzo era stata sproporzionata (ibid., § 51).

5. Protezione dei dati e libertà di circolazione (articolo 2 del Protocollo n. 4)

334. La Corte ha trattato diverse cause in cui la libertà di circolazione di un individuo era stata limitata a causa dei dati personali memorizzati dalle autorità. La Corte ha esaminato le cause ai sensi dell'articolo 8.

335. Pertanto, nella causa *Dalea c. Francia* (dec.), 2010, la memorizzazione da parte della Polizia, nel Sistema informativo Schengen, di dati dei quali il ricorrente aveva contestato l'accuratezza gli impediva di spostarsi liberamente nello spazio Schengen. Il ricorrente non aveva potuto accedere ai dati personali contenuti nella banca dati e ottenerne la rettifica. La Corte ha ribadito che l'articolo 8 non garantiva di per sé il diritto di uno straniero di entrare o di risiedere in un particolare Paese. Nel caso di specie, l'ingerenza nella vita privata del ricorrente a causa del suo inserimento da parte delle autorità francesi nella banca dati Schengen era prevista dalla legge e perseguiva il fine legittimo di proteggere la sicurezza nazionale. Era proporzionata al fine perseguito ed era necessaria in una società democratica. Il ricorrente non aveva invocato l'articolo 2 del Protocollo n. 4.

336. Nella causa *Shimovolos c. Russia*, 2011 (§§ 64-71), le informazioni relative ai viaggi del ricorrente in treno e in aereo erano state registrate nella "banca dati della sorveglianza" a causa della sua appartenenza a un'organizzazione per la difesa dei diritti umani. Ogniqualvolta una persona il cui nome figurava in tale elenco acquistava un biglietto ferroviario o aereo, il Dipartimento interno dei Trasporti riceveva una notifica automatica. Conseguentemente, quando il ricorrente era salito su un treno per recarsi a Samara in relazione a un summit UE-Russia e per partecipare a un rally di protesta in tale città, tre agenti di polizia avevano controllato i suoi documenti d'identità e gli avevano chiesto il motivo del suo viaggio. La Corte ha ritenuto che, raccogliendo e memorizzando i dati relativi agli spostamenti del ricorrente, ai sensi di un decreto ministeriale che non era stato pubblicato e che non era accessibile al pubblico, le autorità avessero interferito nella sua vita privata in modo incompatibile con i diritti garantiti dall'articolo 8. La Corte ha inoltre ritenuto che non sorgesse alcuna questione distinta ai sensi dell'articolo 2 del Protocollo n. 4 (ibid., § 73).

337. Nella causa *Beghal c. Regno Unito*, 2019 (§§ 89-109), che sollevava la questione dell'importanza del controllo degli spostamenti internazionali dei terroristi, la Corte ha ritenuto, prima di constatare la violazione dell'articolo 8, che i poteri conferiti agli agenti della polizia, ai funzionari dell'immigrazione e a designati funzionari doganali ai sensi di una legislazione anti-terrorismo, che permettevano di fermare, perquisire e interrogare i passeggeri nei porti, negli aeroporti e nelle stazioni di testa internazionali, non fossero sufficientemente circoscritti, né erano previste adeguate garanzie giuridiche contro gli abusi. In particolare, la legislazione non esigeva una preliminare autorizzazione e la facoltà di fermare e interrogare poteva essere esercitata anche se non sussisteva alcun sospetto di coinvolgimento nel terrorismo.

338. Nella causa *Willems c. Paesi Bassi* (dec.), 2021, relativo all'obbligo ai sensi della Legge sui passaporti di fare rilevare le impronte digitali al momento della richiesta di rilascio di un passaporto, nonché la memorizzazione di tali impronte su un supporto elettronico, a seguito del recepimento nel diritto interno (senza lasciare alcun margine di discrezionalità alle autorità nazionali) del Regolamento dell'Unione europea relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri, le doglianze sono state rigettate in quanto manifestamente infondate in ragione della "presunzione di protezione equivalente" nel diritto dell'Unione europea (ibid., §§ 26-36).

B. Protezione dei dati e diritti processuali

Articolo 6 della Convenzione

"1. Ogni persona ha diritto a che la sua causa sia esaminata equamente, pubblicamente ed entro un termine ragionevole da un tribunale indipendente e imparziale, costituito per legge, il quale sia chiamato a pronunciarsi sulle controversie sui suoi diritti e doveri di carattere civile o sulla fondatezza di ogni accusa penale formulata nei suoi confronti. La sentenza deve essere resa pubblicamente, ma l'accesso alla sala d'udienza può essere vietato alla stampa e al pubblico durante tutto o parte del processo nell'interesse della morale, dell'ordine pubblico o della sicurezza nazionale in una società democratica, quando lo esigono gli interessi dei minori o la protezione della vita privata delle parti in causa, o, nella misura giudicata strettamente necessaria dal tribunale, quando in circostanze speciali la pubblicità possa portare pregiudizio agli interessi della giustizia.

2. Ogni persona accusata di un reato è presunta innocente fino a quando la sua colpevolezza non sia stata legalmente accertata.

3. In particolare, ogni accusato ha diritto di:

(a) essere informato, nel più breve tempo possibile, in una lingua a lui comprensibile e in modo dettagliato, della natura e dei motivi dell'accusa formulata a suo carico;

(b) disporre del tempo e delle facilitazioni necessarie a preparare la sua difesa;

(c) difendersi personalmente o avere l'assistenza di un difensore di sua scelta e, se non ha i mezzi per retribuire un difensore, poter essere assistito gratuitamente da un avvocato d'ufficio, quando lo esigono gli interessi della giustizia;

(d) esaminare o far esaminare i testimoni a carico ed ottenere la convocazione e l'esame dei testimoni a discarico nelle stesse condizioni dei testimoni a carico;

(e) farsi assistere gratuitamente da un interprete se non comprende o non parla la lingua usata in udienza."

Articolo 13 della Convenzione

"Ogni persona i cui diritti e le cui libertà riconosciuti nella presente Convenzione siano stati violati, ha diritto ad un ricorso effettivo davanti a un'istanza nazionale, anche quando la violazione sia stata commessa da persone che agiscono nell'esercizio delle loro funzioni ufficiali."

1. Diritto a un equo processo (articolo 6 della Convenzione)[12]

339. Ogni persona i cui dati personali sono sottoposti a trattamento automatizzato nell'ambito di un procedimento giudiziario deve godere delle garanzie dell'articolo 6, a prescindere dalla sua qualità nel procedimento (attore, convenuto, testimone, imputato o terzo).

a. Garanzie generali (articolo 6 § 1 della Convenzione)

340. In diverse cause la Corte ha valutato dal punto di vista dell'articolo 6 § 1 la necessità di proteggere i dati personali delle parti o di terzi, nell'ambito di varie garanzie generali finalizzate ad assicurare l'equità dei procedimenti giudiziari. Esse comprendono, in particolare, la parità delle armi e il diritto a un procedimento in contraddittorio, il diritto a una pubblica udienza e alla pubblica

[12] Il presente capo dovrebbe essere letto alla luce e congiuntamente alla Guida all'articolo 6 nel suo aspetto civile (pp. 60-91) e nel suo aspetto penale (pp. 32-100).

pronuncia della sentenza, l'acquisizione delle prove, la ragionevole durata del procedimento e l'obbligo di motivare le decisioni giudiziarie.

i. Parità delle armi e rispetto del principio del contraddittorio nei procedimenti riguardanti informazioni sensibili o riservate

341. Nella causa *Eternit c. Francia* (dec.), 2012 (§§ 35-42), un datore di lavoro aveva instaurato un procedimento contestando la decisione della Cassa assicurazioni malattia di riconoscere la natura lavorativa della malattia di un suo dipendente. La Corte non ha ritenuto che il procedimento avesse violato l'articolo 6 § 1, nonostante il fatto che non fosse stata fornita al datore di lavoro una copia delle osservazioni formulate dal consulente medico della Cassa assicurativa. La mancata fornitura delle cartelle cliniche del dipendente al datore di lavoro era stata giustificata dalla necessità di proteggere la riservatezza dei suoi dati medici, ai quali i tribunali dovevano attribuire il medesimo livello del diritto della società ricorrente a un procedimento in contraddittorio, in modo da assicurare che l'essenza stessa del diritto non fosse pregiudicata in entrambi i casi. Il necessario equilibrio era conseguito se il datore di lavoro poteva chiedere al tribunale di nominare un consulente medico indipendente che riesaminasse le cartelle cliniche del dipendente e redigesse una perizia – rispettando la riservatezza delle cartelle cliniche – per guidare il tribunale e le parti (ibid., § 37). Il fatto che una perizia non fosse commissionata ogni volta che un datore di lavoro lo richiedeva, ma soltanto quando il tribunale riteneva di essere in possesso di informazioni insufficienti, non violava i requisiti di un equo processo ai sensi dell'articolo 6 § 1 della Convenzione (ibid., §§ 35-39).

342. Nella causa *Kennedy c. Regno Unito*, 2010 (§§ 184-191), le limitazioni del principio della parità delle armi e del contraddittorio nei procedimenti dinanzi al Tribunale per i poteri d'indagine, organo indipendente istituito al fine di esaminare le doglianze formulate da persone che sospettavano che le loro comunicazioni fossero state illecitamente intercettate dalle autorità, non sono state considerate incompatibili con l'articolo 6 § 1. Gli interessi della sicurezza nazionale e di tenere segreti alcuni metodi di indagine penale dovevano essere ponderati con il diritto al procedimento in contraddittorio. Secondo la Corte, vi era stata la necessità di mantenere segreto del materiale sensibile e riservato, la cui divulgazione avrebbe impedito di conseguire l'obiettivo perseguito (ibid., §§ 186-187).

343. Più in generale, la Corte ha sottolineato che il diritto a un processo in contraddittorio significa, in una causa penale, che deve essere fornita sia all'accusa che alla difesa la possibilità di conoscere e commentare le osservazioni depositate e le prove addotte dall'altra parte, compresa, per esempio, la video-registrazione di un'imputata utilizzata quale prova a suo carico (*Murtazaliyeva c. Russia*, [GC], 2018, §§ 90-95).

ii. Motivazione delle decisioni giudiziarie e protezione dei dati

344. Nella causa *Surikov c. Ucraina*, 2017 (§§ 102-103), la Corte ha riscontrato la violazione dell'articolo 6 § 1 in quanto i tribunali nazionali non avevano trattato diversi pertinenti e importanti rilievi sollevati. Il ricorrente ha sostenuto che il suo datore di lavoro aveva raccolto e memorizzato arbitrariamente informazioni sensibili e superate relative alla sua salute mentale, aveva utilizzato le informazioni nell'esame della sua domanda di promozione, e le aveva rivelate illegalmente ai suoi colleghi e al tribunale. La Corte ha ribadito che l'articolo 6 obbligava i tribunali a motivare le loro sentenze. Benché non si potesse intendere che tale obbligo imponesse una replica dettagliata a ciascun rilievo, il principio di equità sarebbe stato turbato se i tribunali nazionali avessero ignorato un preciso, pertinente e importante rilievo formulato dal ricorrente (ibid., § 101 e la giurisprudenza ivi citata).

345. Nella causa *Samoylova c. Russia*, 2021 (§§ 50-52), concernente la diffusione di un servizio televisivo nel quale era indicato l'esatto indirizzo della ricorrente, il suo codice fiscale e delle immagini dell'interno della sua casa di campagna, la Corte ha ritenuto che i tribunali nazionali non avessero fornito una specifica ed esplicita risposta ai rilievi che sarebbero stati determinanti per l'esito

del procedimento instaurato dalla ricorrente, in violazione del diritto a un equo processo garantito dall'articolo 6 § 1 della Convenzione.

346. Nella causa *Kennedy c. Regno Unito*, 2010 (§§ 185-191), la politica delle autorità di "non confermare né negare" che fosse stata svolta un'operazione di intercettazione di comunicazioni non è stata ritenuta incompatibile con l'articolo 6 § 1. Pertanto, era stato sufficiente per il Tribunale per i poteri investigativi, istituito per esaminare le doglianze presentate da persone che sospettavano che le loro comunicazioni fossero state intercettate illegalmente dalle autorità, informare semplicemente i ricorrenti che non era stata adottata alcuna determinazione a loro favore, in quanto la politica del Governo di "non confermare né negare" avrebbe potuto essere aggirata se un ricorso a tale tribunale avesse potuto comportare che un ricorrente fosse informato dello svolgimento di intercettazioni (ibid., § 189).

iii. Utilizzo come prove di dati personali raccolti illegalmente o in violazione dell'articolo 8

347. La questione dell'utilizzo come prove materiali in un procedimento giudiziario di dati personali raccolti in modo contrario ai requisiti del diritto interno o dell'articolo 8 è stata affrontata dalla Corte in diverse cause, nell'ambito di procedimenti amministrativi (*Vukota-Bojic c. Svizzera*, 2016, § 77, relativa all'utilizzo in una controversia con una persona assicurata di informazioni raccolte segretamente da una compagnia assicurativa nell'ambito dei suoi poteri ai sensi del regime di assicurazione pubblico); di procedimenti civili (*Bărbulescu c. Romania* [GC], 2017, §§ 140-141, relativa all'utilizzo dei dati raccolti da un datore di lavoro circa l'uso di internet da parte di un dipendente nel luogo di lavoro, per giustificarne il licenziamento; *Florindo de Almeida Vasconcelos Gramaxo c. Portogallo*, 2022, §§ 130-140, relativa all'utilizzo dei dati chilometrici registrati dal sistema GPS dell'automobile di servizio di un rappresentante medico per motivarne il licenziamento); e di procedimenti penali (*Bykov c. Russia* [GC], 2009, §§ 80-83, sull'intercettazione di una conversazione nell'ambito di un'operazione di polizia segreta e l'uso delle prove ottenute in tal modo quale base per una condanna).

348. La Corte ha ritenuto che l'ammissione e l'utilizzo in un procedimento giudiziario di prove di tale natura non conducesse automaticamente alla constatazione di iniquità del procedimento se esso fosse stato svolto complessivamente in modo equo (*Bykov c. Russia* [GC], 2009, §§ 89-91; *Vukota-Bojic c. Svizzera*, 2016, §§ 91-100).

349. La Corte ha riscontrato la violazione dell'articolo 6 § 1 in una causa concernente informazioni ottenute mediante un informatore della Polizia, utilizzando un dispositivo segreto per registrare le conversazioni nella cella del ricorrente, misura non "prevista dalla legge" (*Allan c. Regno Unito*, 2002, §§ 45-53). Le ammissioni compiute dal ricorrente non erano state spontanee, bensì indotte dal persistente interrogatorio da parte dell'informatore il quale, su istigazione della Polizia, aveva orientato le conversazioni in circostanze che potevano essere considerate l'equivalente funzionale di un interrogatorio, senza alcuna garanzia che sarebbe stata prevista in un formale interrogatorio di polizia. Benché non vi fosse alcun particolare rapporto tra il ricorrente e l'informatore e non sia stata individuata alcuna diretta coercizione, il ricorrente sarebbe stato sottoposto a pressioni psicologiche, che avevano compromesso la natura volontaria delle sue ammissioni. Date le circostanze, si poteva ritenere che le informazioni acquisite fossero state ottenute senza tenere conto della volontà del ricorrente, e che il loro utilizzo al processo avesse compromesso il suo diritto di non rispondere e di non rendere dichiarazioni incriminanti.

iv. Pubblica udienza e pubblica pronuncia della sentenza e riservatezza dei dati[13]

350. Nella causa *P. e B. c. Regno Unito*, 2001 (§§ 38-41, 46-49), l'assenza di una pubblica udienza e la pronuncia di una sentenza a porte chiuse in una causa concernente l'affidamento di minori non sono state ritenute in violazione dell'articolo 6 § 1. Secondo la Corte, i procedimenti in materia di affidamento di minori rappresentavano esempi fondamentali di cause in cui l'esclusione della stampa e del pubblico potevano essere giustificati al fine di proteggere i dati personali del minore interessato e delle parti e per evitare di compromettere gli interessi della giustizia (ibid., § 38). Il fatto che chiunque potesse giustificare un interesse avrebbe potuto consultare o ottenere una copia del testo integrale dei provvedimenti e delle sentenze, e che le sentenze dei tribunali erano automaticamente pubblicate senza menzionare i nomi delle persone interessate, era sufficiente a compensare l'assenza di una pubblica pronuncia (ibid., § 47).

351. Nella causa *Kennedy c. Regno Unito*, 2010 (§ 188), la Corte ha ribadito che, ai sensi dell'articolo 6 § 1, la sicurezza nazionale avrebbe potuto giustificare l'esclusione del pubblico dal procedimento. Ha ritenuto che la natura delle questioni sollevate dinanzi al Tribunale per i poteri investigativi, riguardanti l'illecita intercettazione di comunicazioni, giustificasse l'assenza di una pubblica udienza.

352. La Corte ha constatato una duplice violazione dell'articolo 6 nella causa *Vasil Vasilev c. Bulgaria*, 2021, concernente la totale assenza di pubblico accesso (esclusione del pubblico da tutte le udienze e assenza di pubblica pronuncia della sentenza) in un procedimento instaurato dal ricorrente per ottenere un risarcimento a seguito dell'intercettazione, della registrazione e della trascrizione di una conversazione telefonica che egli aveva avuto con un assistito, sottoposto a sorveglianza segreta nell'ambito di un procedimento penale. L'esclusione del pubblico da tutte le udienze e dalla pronuncia della sentenza era stata basata unicamente sulla presenza nel fascicolo di informazioni secretate (prove derivanti dall'intercettazione segreta della conversazione telefonica del ricorrente). Secondo la Corte, la totale assenza di accesso del pubblico non poteva essere giustificata dalla necessità di proteggere le informazioni secretate che erano oggetto della causa. La natura delle questioni sollevate durante il procedimento, concernenti la responsabilità delle autorità statali per un'asserita violazione dei diritti di cui all'articolo 8, non era di natura altamente tecnica e il ricorrente non aveva rinunciato al suo diritto a una pubblica udienza (ibid., §§ 107-111). Quando una causa concerne l'asserita violazione di un diritto fondamentale da parte delle autorità statali, il pubblico esame del procedimento è essenziale per il mantenimento della fiducia nello stato di diritto. La presenza nel fascicolo di informazioni secretate non può di per sé costituire un motivo per negare al pubblico l'intera sentenza. Se una causa concerne informazioni secretate, esistono tecniche che permettono una certa misura di pubblico accesso alle decisioni pronunciate in essa, mantenendo al medesimo tempo la riservatezza di informazioni sensibili (ibid., §§ 116-118).

V. Durata dei procedimenti giudiziari in materia di protezione dei dati

353. Nella causa *Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia* [GC], 2017 (§ 215), la Corte ha ritenuto che la durata complessiva – sei anni e sei mesi in due gradi di giudizio – di un procedimento concernente la compatibilità, ai sensi del diritto interno e del diritto dell'Unione europea, della pubblicazione in massa di dati fiscali personali da parte delle società ricorrenti non soddisfacesse il requisito del termine ragionevole di cui all'articolo 6 § 1. Non si poteva tenere conto del procedimento dinanzi alla Corte di Giustizia dell'Unione europea concernente una domanda di pronuncia pregiudiziale nel valutare la durata imputabile alle autorità nazionali (ibid., § 208).

[13] Si veda altresì, *supra*, la sezione della presente Guida relativa alla divulgazione dei dati nell'ambito di procedimenti giudiziari dal punto di vista dell'articolo 8 della Convenzione.

354. Per contro, nella causa *Surikov c. Ucraina*, 2017 (§§ 104-106), la Corte ha dichiarato manifestamente infondata una doglianza relativa alla durata del procedimento concernente la memorizzazione da parte di un datore di lavoro di informazioni sensibili e superate relative alla salute mentale di un dipendente e il loro utilizzo nell'esame della sua domanda di promozione. La Corte ha ritenuto che un periodo inferiore a sei anni per tre gradi di giudizio non sollevasse una questione riguardo al requisito del termine ragionevole di cui all'articolo 6 § 1 (ibid., § 101).

b. Specifiche garanzie (articolo 6 §§ 2 e 3 della Convenzione)

355. In materia penale, chiunque sia accusato sulla base dei suoi dati personali deve beneficiare di alcune specifiche garanzie.

i. Protezione dei dati e diritto alla presunzione di innocenza (articolo 6 § 2 della Convenzione)

356. Nella causa *Batiashvili c. Georgia*, 2019 (§§ 87-97), la Corte ha ritenuto che l'articolo 6 § 2 fosse applicabile in una situazione in cui le autorità avevano manipolato una registrazione delle conversazioni telefoniche di una persona precedentemente al suo arresto e l'avevano fatta trasmettere per televisione. Secondo la Corte, il coinvolgimento delle autorità aveva contribuito al fatto che il ricorrente fosse considerato colpevole prima che la sua colpevolezza fosse stata dimostrata in tribunale, e costituiva pertanto violazione dell'articolo 6 § 2. La sequenza degli eventi, considerata complessivamente, indicava che la situazione del ricorrente fosse stata notevolmente compromessa dal comportamento delle autorità inquirenti (ibid., § 94). Benché l'accusa di omessa denuncia di un reato fosse stata archiviata durante il procedimento di primo grado, la richiesta di rinvio a giudizio quasi quattro mesi dopo la registrazione era stata resa accessibile al pubblico e menzionava ancora l'accusa in questione, benché gli inquirenti dovessero essere consapevoli della falsità delle prove sulle quali era basata l'accusa (ibid., § 95).

357. Nella causa *Y.B. e altri c. Turchia*, 2004 (§§ 43-51), le dichiarazioni rilasciate dalla Polizia alla stampa relative a indagati fotografati dai giornalisti, durante una conferenza stampa svolta in un ufficio di Polizia, sono state ritenute in violazione dell'articolo 6 § 2. La pubblicazione delle fotografie degli indagati nel corso del procedimento penale non costituiva di per sé violazione del loro diritto alla presunzione di innocenza. Le autorità nazionali potevano informare il pubblico di indagini penali in corso, purché ciò avvenisse con tutta la discrezione e la prudenza necessarie. Ciononostante, se rendevano pubbliche informazioni obiettive relative a procedimenti penali, tali informazioni non dovevano contenere valutazioni o giudizi prematuri circa la colpevolezza (ibid., §§ 47-48). Nel caso di specie l'atteggiamento delle autorità di Polizia, nella misura in cui aveva comportato una preliminare valutazione delle accuse che avrebbero potuto essere formulate nei confronti del ricorrente e forniva alla stampa un facile mezzo materiale per individuarle, era incompatibile con la presunzione di innocenza (ibid., § 50).

358. Nella causa *Panteleyenko c. Ucraina,* 2006 (§ 68-71), le decisioni del tribunale di archiviare il procedimento penale nei confronti del ricorrente erano espresse in termini che non lasciavano alcun dubbio circa l'opinione dei giudici che il ricorrente avesse commesso il reato del quale era accusato; la Corte ha pertanto riscontrato la violazione dell'articolo 6 § 2. La decisione di archiviare il procedimento per "motivi non esimenti" era stata adottata sulla base di prove contenenti dati personali riguardanti il ricorrente, che esercitava la professione di notaio, e acquisite a seguito di una perquisizione del suo studio, svolta in violazione dell'obbligo previsto dalla legge di notificare preliminarmente il mandato di perquisizione alla persona che occupava i locali pertinenti e del divieto

di sequestrare qualsiasi documento o oggetto non connesso direttamente al caso oggetto di indagini (ibid., § 70)[14].

ii. Protezione dei dati e diritti di difesa (articolo 6 § 3, lettera b) della Convenzione)

359. Nella causa *Rook c. Germania*, 2019 (§ 69), la Corte ha stabilito che un periodo di tre mesi e mezzo per studiare una grande quantità di dati e file elettronici relativi al ricorrente, acquisiti mediante la sorveglianza delle telecomunicazioni, fosse sufficiente sotto il profilo dell'articolo 6 § 3, lettera b) a permettere al suo avvocato di preparare la sua difesa. In considerazione della complessità del procedimemto penale, non vi era stata la necessità di dare all'avvocato del ricorrente la possibilità di leggere e ascoltare ogni elemento dei dati di sorveglianza, comprendenti 45.000 telefonate e 34.000 altri insiemi di dati raccolti nel corso dell'indagine, e 14 milioni di file elettronici confiscati dalla Polizia nell'appartamento del ricorrente e in altri luoghi (ibid., §§ 7-8, 67-71).

360. Più in generale, la Corte ha sottolineato che i moderni metodi di indagine possono effettivamente produrre enormi quantità di dati, il cui inserimento nel procedimento penale non dovrebbe causare eccessivi ritardi a tale procedimento. Il diritto del ricorrente alla divulgazione non doveva essere confuso con il suo diritto di accesso a tutto il materiale già ritenuto pertinente dalle autorità, che esigeva generalmente che la persona interessata avrebbe dovuto essere in grado di comprendere il materiale nella sua interezza (ibid., § 67). Il mero fatto che il procedimento giudiziario fosse già iniziato quando l'avvocato aveva ottenuto una copia integrale del fascicolo, non significava che egli non avesse avuto sufficiente tempo per prepararsi. L'articolo 6 § 3, lettera b) non esige che la preparazione di un processo che dura un certo periodo di tempo sia completata prima della prima udienza (ibid., § 72)[15].

361. Nella causa *Sigurður Einarsson e altri c. Islanda*, 2019 (§§ 88-93), la Corte ha ritenuto che non vi fosse stata violazione dell'articolo 6 §§ 1 e 3, lettera b) in relazione al mancato accesso della difesa all'enorme quantità di dati raccolti dall'accusa e non inseriti nel fascicolo delle indagini, e al fatto che la difesa non avesse avuto voce in capitolo in merito alla setacciatura elettronica di tali dati da parte dell'accusa al fine di individuare le informazioni pertinenti all'indagine. In relazione alla "raccolta integrale dei dati", l'accusa non conosceva il contenuto della massa dei dati, e a tale proposito essa non aveva beneficiato di alcun vantaggio rispetto alla difesa. Quanto ai dati "taggati", in linea di principio sarebbe stato opportuno concedere alla difesa la possibilità di svolgere una ricerca delle prove potenzialmente a discarico. Tuttavia i ricorrenti non avevano chiesto formalmente in alcuna fase un provvedimento del tribunale in tal senso e non avevano precisato il tipo di prova che cercavano.

iii. Diritto a un ricorso effettivo (articolo 13 della Convenzione)[16]

362. Nella causa *Anne-Marie Anderson c. Svezia*, 1997 (§§ 41-42), concernente la divulgazione di cartelle cliniche, la Corte non ha riscontrato alcuna violazione dell'articolo 13 in combinato disposto con l'articolo 8 in relazione all'impossibilità per una paziente, prima della comunicazione di dati personali e riservati da parte dell'autorità medica a un'autorità per i servizi sociali, di impugnare la misura. Tra l'altro, la misura era stata notificata alla ricorrente ed era di natura limitata, in quanto le

[14] Si veda altresì la Guida all'articolo 6 della Convenzione (Diritto a un equo processo (aspetto penale)) in relazione alla motivazione delle decisioni giudiziarie (paragrafi 168-176)

[15] Si veda altresì la Guida all'articolo 6 della Convenzione (Diritto a un equo processo (aspetto penale)) in relazione ai mezzi necessari agli imputati per la preparazione della loro difesa.

[16] Il presente capo dovrebbe essere letto alla luce e congiuntamente alla Guida all'articolo 13 della Convenzione (Diritto a un ricorso effettivo, si vedano, in particolare, le pagine 49-51).

informazioni in questione non erano state rese pubbliche, bensì erano state protette dal medesimo livello di riservatezza applicabile alle cartelle cliniche psichiatriche.

363. Nella causa *Mik e Jovanović c. Serbia* (dec.) i ricorrenti hanno lamentato ai sensi dell'articolo 8, considerato singolarmente e in combinato disposto con l'articolo 13, la continua mancata fornitura di informazioni credibili a essi da parte dello Stato circa il destino dei loro figli neonati, che erano asseritamente morti poco dopo la nascita e i cui corpi non erano mai stati mostrati ai ricorrenti, la Corte ha osservato che una legge adottata recentemente aveva istituito un meccanismo (comprendente una banca dati del DNA) in relazione alla situazione affrontata dai ricorrenti e da altri. In particolare, il nuovo quadro giuridico prevedeva sia procedure giudiziarie che stragiudiziali, finalizzate a individuare il vero status di neonati dei quali si sospettava che fossero scomparsi in reparti maternità statali, e a risarcire i genitori. Inoltre, erano state adottate alcune importanti misure per attuare tale quadro, tra cui la formazione approfondita dei giudici, nonché la nomina, nell'ambito della procedura stragiudiziale, di membri (che erano per la maggioranza rappresentanti di associazioni riconosciute dei genitori) di una commissione dotata di ampi poteri investigativi, di raccolta dei dati e di riferire. Osservando che i ricorrenti stessi avevano scelto di avvalersi del nuovo meccanismo, la Corte ha concluso che non fosse più giustificato proseguire l'esame del ricorso ai sensi dell'articolo 37 § 1, lettera c) della Convenzione.

364. Nella causa *Panteleyenko c. Ucraina*, 2006 (§§ 82-84), la Corte ha constatato la violazione dell'articolo 13, in combinato disposto con l'articolo 8, in considerazione dell'assenza di un ricorso effettivo che permettesse al ricorrente di lamentare la divulgazione di informazioni riservate relative alla sua salute mentale nel corso di una pubblica udienza. Secondo la Corte, i ricorsi legali esistenti si erano dimostrati inefficaci poiché non avevano comportato la cessazione della divulgazione dei dati psichiatrici nel fascicolo processuale, o la concessione di un risarcimento al ricorrente per il danno subito in conseguenza dell'ingerenza nella sua vita privata. Benché la celebrazione di un'udienza a porte chiuse avrebbe impedito che le informazioni fossero divulgate al pubblico, essa non avrebbe impedito che le parti le conoscessero, o il loro inserimento nel fascicolo processuale.

365. In relazione alla pubblicazione su internet di una decisione giudiziaria che rivelava informazioni concernenti l'adozione dei figli dei ricorrenti, la Corte ha ritenuto, nella causa *X e altri c. Russia*, 2020 (§§ 73-79), che vi fosse stata violazione dell'articolo 13, in combinato disposto con l'articolo 8, in ragione dell'assenza di un ricorso giurisdizionale che fornisse un risarcimento del danno non patrimoniale causato dal malfunzionamento del sistema giudiziario.

366. In una causa relativa alla registrazione di un individuo come "delinquente" nei registri della polizia successivamente al suo interrogatorio in relazione a una violenza sessuale, e alla conservazione della registrazione nonostante il fatto che non fosse stata successivamente disposta alcuna richiesta di rinvio a giudizio, la Corte ha riscontrato la violazione dell'articolo 13, in combinato disposto con l'articolo 8, dopo aver osservato che all'epoca dei fatti il ricorrente non disponeva di alcun ricorso mediante il quale impugnare la misura (*Dimitrov-Kazakov c. Bulgaria*, 2011, §§ 37-39).

367. L'assenza di un ricorso effettivo che permettesse al ricorrente di chiedere l'eliminazione del suo nome dalla lista annessa all'Ordinanza sui talebani costituiva violazione dell'articolo 13, in combinato disposto con l'articolo 8, nella causa *Nada c. Svizzera* [GC], 2012 (§§ 209-214). Il ricorrente aveva potuto adire i tribunali nazionali, ma essi non avevano esaminato il merito delle sue doglianze.

368. In relazione all'utilizzo di dati personali in un contesto professionale, la Corte ha riscontrato la violazione dell'articolo 13, in combinato disposto con l'articolo 8, nella causa *Smith e Grady c. Regno Unito*, 1999 (§§ 136-139), in ragione dell'assenza di un ricorso effettivo in relazione alla violazione della privacy dei ricorrenti in conseguenza delle indagini invasive relative alla vita privata di omosessuali, che avevano dato luogo al loro licenziamento dalle Forze armate.

369. Nella causa *Karabeyoğlu c. Turchia*, 2016 (§§ 128-132), l'indisponibilità di un ricorso interno mediante il quale assicurare un riesame dell'utilizzo, in un procedimento disciplinare, di dati ottenuti

mediante le intercettazioni telefoniche in un'indagine penale, ha condotto la Corte a riscontrare la violazione dell'articolo 13, interpretato alla luce dell'articolo 8.

370. Nella causa *Peck c. Regno Unito*, 2003 (§§ 101-114), la Corte ha stabilito che il ricorrente non disponesse di un ricorso effettivo mediante il quale lamentare la divulgazione ai media della sequenza di una telecamera a circuito chiuso (CCTV) che lo mostrava mentre tentava di suicidarsi in un luogo pubblico. In relazione alla possibilità di riesame giudiziario, poiché l'unica questione dinanzi ai tribunali nazionali era stata quella di determinare se la politica relativa alle immagini catturate in luoghi pubblici da telecamere a circuito chiuso potesse essere definita "irrazionale", qualsiasi considerazione della questione di sapere se l'ingerenza nel diritto del ricorrente rispondesse a una imperativa esigenza sociale o fosse proporzionata era stata effettivamente esclusa (ibid., §§ 106-107). Quanto alle commissioni per i media, la loro impossibilità di concedere un risarcimento significava che esse non potessero fornire neanche un ricorso effettivo (ibid., §§ 108-109). Quanto a un'azione in violazione della riservatezza, era improbabile che all'epoca dei fatti i tribunali avrebbero accettato che le immagini avessero la "necessaria qualità di riservatezza", o che le informazioni fossero state "impartite in circostanze che comportavano un obbligo di riservatezza" (ibid., § 111).

371. Quanto alla sorveglianza segreta, la segretezza delle misure rende difficile, se non impossibile, l'esercizio di un ricorso da parte della persona interessata, in particolare mentre è in corso la sorveglianza. Un "ricorso effettivo" ai fini dell'articolo 13 deve significare un ricorso che è effettivo quanto lo può essere, tenuto conto della ristretta portata di un ricorso inerente a qualsiasi sistema di sorveglianza (*Klass e altri c. Germania*, 1978, §§ 68-69). Un obiettivo meccanismo di controllo può essere sufficiente finché le misure rimangono segrete. Soltanto una volta che le misure sono state divulgate i ricorsi giuridici devono essere resi disponibili alla persona interessata, entro un termine ragionevole (*Rotaru c. Romania* [GC], 2000, § 69).

372. Quanto alle misure di sorveglianza mirate, in cui gli abusi erano potenzialmente molto facili in singoli casi, e potevano avere conseguenze molto dannose per la società democratica nel suo insieme, è in linea di principio auspicabile affidare il controllo della vigilanza a un giudice, poiché il controllo giudiziario offre le migliori garanzie di indipendenza, di imparzialità e di una procedura corretta. Successivamente alla revoca della misura di sorveglianza, le persone interessate dovrebbero essere informate, appena la notifica può essere svolta senza mettere a repentaglio il fine della restrizione. Per consentire alla persona interessata di ottenere un riesame del procedimento concernente l'ingerenza nell'esercizio del suo diritto alla vita privata, è in linea di principio necessario fornire alla persona una minima quantità di informazioni relative alla decisione che potrebbe essere impugnata, quali la data in cui è stata adottata e il tribunale che l'ha pronunciata (*Roman Zakharov c. Russia* [GC], 2015, §§ 233, 287, 294; *İrfan Güzel c. Turchia*, 2017, §§ 96, 98-99).

373. Nella causa *Klass e altri c. Germania*, 1978 (§§ 65-72), la Legge "G10" consentiva alle autorità di aprire e ispezionare la corrispondenza e la posta, leggere i messaggi telegrafici e ascoltare e registrare le conversazioni telefoniche, al fine di difendere il Paese da "imminenti pericoli". La Corte ha ritenuto che l'insieme dei ricorsi previsti dalla legislazione tedesca soddisfacesse, date le particolari circostanze di tale causa, i requisiti dell'articolo 13, alla luce dell'articolo 8, in relazione al rispetto della vita privata e della corrispondenza. Benché, secondo la Legge, il fatto che fossero state disposte e attuate misure restrittive non potesse essere impugnato nei tribunali, le persone che ritenevano di essere sottoposte a sorveglianza avevano a disposizione vari altri ricorsi . Secondo la sentenza del 1970 della Corte costituzionale federale, la competente autorità doveva informare la persona interessata appena le misure di sorveglianza cessavano e la notifica poteva essere effettuata senza mettere a repentaglio il fine della restrizione. A decorrere dal momento della suddetta notifica, diventavano disponibili per le persone vari ricorsi giurisdizionali dinanzi ai tribunali. Esse potevano: instaurare un'azione di accertamento al fine di ottenere un riesame da parte dei tribunali amministrativi finalizzato a stabilire se la G10 fosse stata applicate legittimamente nella loro causa e se le misure di sorveglianza disposte fossero conformi alla legge; instaurare un'azione risarcitoria in un tribunale civile se erano state danneggiate; o instaurare un'azione finalizzata alla distruzione o, se del caso, alla restituzione dei

documenti. Infine, se nessuno di tali ricorsi aveva successo, esse potevano adire la Corte costituzionale federale affinché essa stabilisse se vi era stata violazione della Legge fondamentale. Si vedano altresì, per un effetto analogo, le cause *Leander c. Svezia*, 1987 (§§ 78-84), concernente un sistema di controlli segreti relativi a candidati all'impiego in posti importanti dal punto di vista della sicurezza nazionale, e *Amann c. Svizzera* [GC], 2000 (§§ 89-90), relativa all'intercettazione di una telefonata e alla memorizzazione di dati personali da parte dei Servizi segreti.

374. In considerazione della mancata risposta ai dubbi di un imputato circa la legittimità dell'intercettazione delle sue telefonate, la Corte ha riscontrato la violazione dell'articolo 13, in combinato disposto con l'articolo 8, nella causa *İrfan Güzel c. Turchia*, 2017 (§§ 100-109).

375. Nella causa *Allan c. Regno Unito*, 2002 (§ 55), la Corte ha riscontrato la violazione dell'articolo 13, in combinato disposto con l'articolo 8, in quanto all'epoca dei fatti la legge non prevedeva alcun sistema che disciplinasse l'uso di dispositivi segreti per registrare le conversazioni nella cella del ricorrente e il loro utilizzo da parte della Polizia.

376. In una causa in cui il controllo globale di un sistema di sorveglianza segreta era stato affidato solamente al Ministero degli Affari interni (che era direttamente coinvolto nelle domande di utilizzo di speciali mezzi di sorveglianza per proteggere la sicurezza nazionale), piuttosto che a organi indipendenti, la Corte ha riscontrato la violazione dell'articolo 13, alla luce dell'articolo 8, a causa dell'assenza di un ricorso effettivo (*Association for European Integration and Human Rights and Ekimdzhiev c. Bulgaria,* 2007, §§ 98-103).

377. In considerazione dell'assenza di un ricorso mediante il quale impugnare la memorizzazione, da parte di agenti statali, di dati relativi alla vita privata di una persona, o la veridicità di tali informazioni, la Corte ha riscontrato la violazione dell'articolo 13, interpretato congiuntamente all'articolo 8, nella causa *Rotaru c. Romania* [GC], 2000 (§§ 68-73). È pervenuta a una conclusione simile nella causa *Segerstedt-Wiberg e altri c. Svezia*, 2006 (§§ 116-122), in assenza di un ricorso che consentisse ai ricorrenti di esaminare nella loro interezza le informazioni che li riguardavano contenute negli archivi dei Servizi di sicurezza e di ottenere la distruzione dei fascicoli conservati che li riguardavano da parte dei Servizi di sicurezza e la cancellazione o la rettifica delle informazioni personali in tali fascicoli.

3. Diritto alla libertà e alla sicurezza (articolo 5 della Convenzione)

378. Nella causa *Akgün c. Turchia*, 2021 (§§ 178-181), in cui all'epoca dell'iniziale custodia cautelare del ricorrente la constatazione del fatto che egli aveva utilizzato il sistema di messaggistica crittografato ByLock era l'unica prova fornita per giustificare il sospetto, ai fini dell'articolo 5 § 1, lettera c), che egli avesse commesso il reato di appartenenza a un'organizzazione terroristica, la Corte ha riscontrato la violazione di tale disposizione della Convenzione. L'asserita attività criminale del ricorrente riguardava la criminalità organizzata. L'uso di prove elettroniche che indicavano che una persona si era avvalsa di un servizio di messaggistica crittografato, che era stato destinato appositamente all'utilizzo esclusivo per, e da parte di, un'organizzazione criminale ai fini della comunicazione interna di tale organizzazione, poteva costituire uno strumento significativo nella lotta contro la criminalità organizzata. Conseguentemente, una persona sospettata poteva essere validamente ristretta fin dall'inizio del procedimento sulla base di tale prova, in quanto essa poteva fornire un forte indizio dell'appartenenza di tale persona a una simile organizzazione. Se tale prova costituiva l'unica o l'esclusiva base dei sospetti nei confronti di una persona, il tribunale nazionale doveva disporre di informazioni sufficienti circa il materiale in questione prima di esaminare, con prudenza, il suo eventuale valore probatorio ai sensi del diritto interno. Nel caso di specie il Governo non era stato in grado di dimostrare che alla data in cui il ricorrente era stato collocato in custodia cautelare le prove di cui la Pretura disponeva soddisfacessero il criterio del "plausibile sospetto" richiesto dall'articolo 5 § 1, lettera c) della Convenzione, tale da convincere un osservatore obiettivo che egli avrebbe potuto avere commesso i reati per i quali era stato ristretto. Secondo la Corte, il documento che concludeva che il ricorrente avesse utilizzato ByLock non precisava, né indicava, di per

sé, alcuna attività illegale da parte del ricorrente, in quanto non individuava le date della sua presunta attività, né la sua frequenza, e non conteneva alcun particolare aggiuntivo connesso. Inoltre, né tale documento né il decreto di custodia cautelare avevano dimostrato in quale modo tale presunta attività da parte del ricorrente indicasse la sua appartenenza a un'organizzazione terroristica.

IV. Sfide del giorno d'oggi in materia di protezione dei dati

A. Progressi tecnologici, algoritmi e intelligenza artificiale[17]

379. In cause concernenti l'acquisizione e la memorizzazione da parte delle autorità, ai fini della prevenzione dei reati, di impronte digitali, campioni biologici e profili del DNA, di persone sospettate o condannate per dei reati, la Corte ha dichiarato chiaramente che l'uso di moderne tecniche scientifiche non può essere autorizzato a qualsiasi costo e senza bilanciare attentamente i potenziali vantaggi dell'ampio uso di tali tecniche con importanti interessi relativi alla vita privata (*S. e Marper c. Regno Unito* [GC], 2008, § 112). Uno Stato che rivendica un ruolo pioneristico nello sviluppo di nuove tecnologie si assume la particolare responsabilità di conseguire un giusto equilibrio a tale riguardo (ibid., § 112). Tenendo presente il rapido ritmo degli sviluppi nel campo della genetica e dell'informatica, la possibilità che in futuro gli interessi relativi alla vita privata legati alle informazioni genetiche possano essere lesi in nuovi modi, o in un modo che non può essere anticipato oggi con precisione, non può essere ignorata (ibid., § 71).

380. Secondo la Corte, il rapido sviluppo di tecniche sempre più sofisticate che permettono, tra l'altro, che le tecniche di ricoscimento facciale e di cartografia facciale siano applicate alle fotografie delle persone, rende problematiche l'acquisizione delle loro fotografie e la conservazione e l'eventuale divulgazione dei dati risultanti. I tribunali nazionali devono tenere conto di tali fattori nel valutare la necessità dell'ingerenza nella vita privata della persona interessata (*Gaughran c. Regno Unito*, 2020, § 70). In tale causa (ibid., §§ 96-98), la Corte ha sottolineato che le moderne tecnologie erano più complesse e che i tribunali nazionali non avevano considerato sufficientemente tale aspetto quando avevano esaminato la necessità dell'ingerenza nel diritto al rispetto della vita privata del ricorrente, del quale le autorità avevano scattato una fotografia a seguito di un reato di lieve entità, ed essa era stata conservata anche successivamente alla cancellazione della sua condanna dal casellario, alla scadenza del termine previsto dalla legge.

381. Nella causa *Breyer c. Germania*, 2020 (§ 88), la Corte ha riconosciuto, nell'ambito della lotta contro la criminalità organizzata e il terrorismo, che i moderni mezzi di telecomunicazione e le modifiche delle modalità di comunicazione esigevano l'adeguamento degli strumenti d'indagine. Secondo la Corte, l'obbligo per gli operatori di telefonia mobile di memorizzare le informazioni relative all'abbonato e di metterle, su richiesta, a disposizione delle autorità è, in generale, una risposta appropriata alle modifiche delle modalità di comunicazione e dei mezzi di telecomunicazione.

382. Nella causa *Szabó e Vissy c. Ungheria*, 2016 (§ 68), concernente la sorveglianza in massa delle comunicazioni, la Corte ha riconosciuto che il fatto che i governi ricorressero a tecnologie all'avanguardia, tra cui il controllo massivo delle comunicazioni, al fine di prevenire imminenti attentati, fosse una conseguenza naturale delle forme adottate dall'attuale terrorismo. In tale causa la Corte ha ritenuto che la legislazione che consentiva la sorveglianza in massa non fornisse le

[17] Il presente capo dovrebbe essere letto congiuntamente alle sezioni della presente Guida sulla memorizzazione Memorizzazione di dati personali al fine della prevenzione dei reati alla Raccolta di dati da parte delle autorità mediante sorveglianza segreta.

necessarie garanzie contro gli abusi, poiché le nuove tecnologie rendevano facile per le autorità l'intercettazione di notevoli quantità di dati relativi anche a persone non comprese nella categoria cui mirava originariamente l'operazione. Inoltre, le misure di tale tipo potevano essere disposte dall'esecutivo senza alcun controllo e senza alcuna valutazione della loro rigorosa necessità, e in assenza di un effettivo ricorso giurisdizionale o di altro tipo (ibid., §§ 73-89).

383. Nella causa *Roman Zakharov c. Russia* [GC], 2015 (§§ 302-305), la Corte ha ritenuto che il rischio di abusi inerente a qualsiasi sistema di sorveglianza segreta fosse particolarmente elevato in un sistema nel quale i Servizi segreti e la Polizia potevano accedere direttamente, mediante dispositivi tecnici, a qualsiasi comunicazione di telefonia mobile. La Corte ha constatato la violazione dell'articolo 8, ritenendo che le disposizioni giuridiche russe che permettevano una generalizzata intercettazione delle comunicazioni non fornissero garanzie adeguate ed effettive contro le arbitrarietà e il rischio di abusi, insito in qualsiasi sistema di sorveglianza segreta.

384. Nella causa *Akgün c. Turchia*, 2021 (§§ 178-181), nella quale all'epoca dell'iniziale custodia cautelare del ricorrente la constatazione che egli aveva utilizzato il sistema di messaggistica crittografata ByLock era stata l'unica prova fornita per giustificare il sospetto, ai fini dell'articolo 5 § 1, lettera c), che egli avesse commesso un reato, la Corte ha sottolineato che l'utilizzo di tali prove quale unica base a fondamento di un sospetto poteva porre diverse delicate questioni, in quanto, per la loro natura, la procedura e le tecnologie applicate durante la raccolta di tali prove erano complesse e potevano conseguentemente ridurre la capacità dei tribunali nazionali di accertare la loro autenticità, accuratezza e integrità (si veda il paragrafo 373 *supra*).

385. Nelle cause *Centrum för rättvisa c. Svezia* [GC], 2021, § 261, e *Big Brother Watch e altri c. Regno Unito* [GC], 2021, §§ 322-323, la Corte ha espressamente ammesso che l'utilizzo di un regime di intercettazione in massa non fosse *per se* contrario all'articolo 8, in considerazione della proliferazione delle minacce che gli Stati affrontavano attualmente da reti di attori internazionali, che utilizzavano internet per comunicare, e dell'esistenza di sofisticate tecnologie che permettevano a tali attori di evitare di essere scoperti. La Corte ha tuttavia sottolineato che, in considerazione del costante sviluppo delle moderne tecnologie della comunicazione, il suo abituale approccio a regimi di sorveglianza mirata avrebbe dovuto essere adeguato per rispecchiare le specifiche caratteristiche di un regime di intercettazione in massa, in ragione del rischio che si abusasse del potere di intercettazione in massa e della legittima necessità di segretezza di tali operazioni. In particolare, la procedura deve essere soggetta a "garanzie da un estremo all'altro", il che significa che, a livello nazionale, in ciascuna fase della procedura avrebbe dovuto essere effettuata una valutazione della necessità e della proporzionalità delle misure adottate; che l'intercettazione in massa dovrebbe essere soggetta fin dal principio a un'autorizzazione indipendente, quando si definiscono l'oggetto e la portata dell'operazione; e che l'operazione dovrebbe essere soggetta a controllo e a un riesame indipendente *ex post facto*.

B. Internet e motori di ricerca

386. I siti internet sono uno strumemto di informazione e di comunicazione particolarmente distinti dai media stampati, specialmente per quanto riguarda la capacità di memorizzare e di trasmettere informazioni (*M.L. e W.W. c. Germania*, 2018, § 91). Alla luce della sua accessibilità e della sua capacità di memorizzare e comunicare enormi quantità di informazioni, internet svolge un importante ruolo nel potenziare l'accesso del pubblico alle notizie e nel facilitare in generale la divulgazione di informazioni (*Times Newspapers Ltd c. Regno Unito (nn. 1 e 2),* 2009, § 27).

387. Il rischio di danno posto dal contenuto e dalle comunicazioni su internet all'esercizio e al godimento dei diritti umani e delle libertà, in particolare al diritto al rispetto della vita privata, è certamente più elevato di quello posto dalla stampa, in particolare in ragione dell'importante ruolo dei motori di ricerca (*M.L. e W.W. c. Germania*, 2018, § 91 e i rinvii ivi citati).

388. Le informazioni contenenti dati personali detenuti dai mezzi di informazione possono essere reperite facilmente dagli utenti di internet mediante i motori di ricerca (ibid., § 97). A causa di tale effetto amplificante sulla divulgazione delle informazioni e della natura delle attività alla base della pubblicazione delle informazioni, gli obblighi dei motori di ricerca nei confronti dell'individuo al quale si riferiscono le informazioni possono differire da quelli dell'entità che le ha originariamente pubblicate (ibid., § 97). Pertanto, in una causa in cui due persone avevano chiesto l'eliminazione dei dati completi della loro identità e delle loro fotografie dagli archivi online di alcuni quotidiani e di alcune stazioni radio dopo che avevano ultimato di espiare lunghe pene detentive per omicidio (ibid., §§ 7, 12, 33), la Corte ha ritenuto che il bilanciamento degli interessi in gioco avrebbe potuto comportare esiti differenti a seconda del fatto che la domanda di eliminazione dei dati personali concernesse l'originale editore delle informazioni, la cui attività era generalmente alla base di ciò che la libertà di espressione era finalizzata a proteggere, o un motore di ricerca il cui interesse principale non era costituito dalla pubblicazione delle iniziali informazioni relative alla persona interessata, bensì, in particolare, dal facilitare l'individuazione di qualsiasi informazione disponibile su tale persona e stabilire un profilo della stessa (ibid., § 97). Si vedano altresì i paragrafi 281 e 282 *supra* della presente Guida per maggiori informazioni sul "diritto all'oblio" nel contesto degli archivi online dei mezzi di informazione contenenti dati personali degli individui, nella causa *M.L. e W.W. c. Germania*.

389. Secondo la Corte, gli archivi di internet contribuiscono a conservare e rendere disponibili notizie e informazioni (*Times Newspapers Ltd c. Regno Unito (nn. 1 e 2),* 2009, § 45). Tali archivi costituiscono un'importante fonte per l'istruzione e la ricerca storica, particolarmente perché essi sono prontamente accessibili al pubblico e sono generalmente gratuiti.

390. La discrezionalità offerta agli Stati nel conseguire un equilibrio tra i diritti concorrenti è maggiore se si tratta di archivi di notizie di eventi passati, piuttosto che di notizie che riferiscono a vicende di attualità (ibid., § 45). Il dovere della stampa di agire in conformità ai principi del giornalismo responsabile, assicurando l'accuratezza delle informazioni pubblicate, è più stringente per ciò che concerne la pubblicazione di informazioni storiche, piuttosto che di informazioni deperibili, in assenza di urgenza di pubblicare il materiale (ibid., § 45).

391. Il rifiuto dei tribunali di ordinare il ritiro di un articolo che danneggiava la reputazione di un avvocato ed era disponibile negli archivi internet di un quotidiano non è stato considerato in violazione dell'articolo 8 nella causa *Węgrzynowski e Smolczewski c. Polonia*, 2013 (§§ 60-70). La Corte ha ammesso che il ruolo delle autorità giudiziarie non comportava che esse si dedicassero a riscrivere la storia, ordinando l'eliminazione dal dominio pubblico di qualsiasi traccia di pubblicazioni che erano state ritenute in passato, con decisioni giudiziarie definitive, costituire degli attacchi ingiustificati nei confronti di reputazioni individuali (ibid., § 65). Inoltre, l'interesse legittimo del pubblico ad accedere agli archivi pubblici di internet della stampa era protetto ai sensi dell'articolo 10 (ibid., § 65). Era significativo che i tribunali polacchi avessero osservato che sarebbe stato auspicabile aggiungere un commento all'articolo sul sito internet del quotidiano, informando il pubblico dell'esito del primo procedimento. Secondo la Corte, ciò dimostrava che i tribunali nazionali fossero consapevoli dell'importanza che le pubblicazioni disponibili su internet al pubblico generale avrebbero potuto avere per l'effettiva protezione dei diritti individuali e che apprezzassero il valore della disponibilità sul sito internet del quotidiano di informazioni integrali sulle decisioni giudiziarie concernenti l'articolo. L'avvocato non aveva chiesto che fosse aggiunto all'articolo un riferimento alle precedenti sentenze a suo favore (ibid., §§ 66-67).

392. La causa *Biancardi c. Italia,* 2021, §§ 67-70, ha offerto alla Corte la sua prima opportunità di pronunciarsi sulla compatibilità con l'articolo 10 di una sentenza civile nei confronti di un giornalista per non avere deindicizzato delle informazioni sensibili pubblicate su internet, relative a procedimenti penali nei confronti di privati e alla decisione del giornalista di mantenere le informazioni facilmente accessibili, nonostante l'opposizione degli interessati. In tale causa non era sorta la questione di anonimizzare le identità nell'articolo on-line. La Corte ha riscontrato che l'articolo era rimasto facilmente accessibile online per otto mesi successivamente a una formale domanda di eliminarlo da

parte delle persone interessate. La severità della sanzione – responsabilità civile e penale – e l'importo del risarcimento accordato non sembravano eccessivi.

C. Trasferimenti di dati e flussi di dati

393. Nella causa *Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia* [GC], 2017, relativa a flussi massivi di dati personali, i dati fiscali personali relativi a 1,2 milioni di persone erano stati pubblicati su una rivista e successivamente divulgati per mezzo di un servizio di messaggistica di testo. Secondo la Corte, l'esistenza di un interesse pubblico a fornire accesso a, e a permettere la raccolta di, notevoli quantità di dati fiscali a fini giornalistici non significava necessariamente o automaticamente che vi fosse anche un interesse pubblico a divulgare *en masse* tali dati grezzi in forma inalterata senza alcun apporto analitico. Doveva essere operata una distinzione tra il trattamento dei dati a fini giornalistici e la divulgazione di dati grezzi per i quali era stato concesso ai giornalisti un accesso privilegiato (ibid., § 175). In tale contesto, il fatto di proibire la pubblicazione massiva di dati fiscali personali in modo incompatibile con le disposizioni finlandesi e con quelle dell'Unione europea relative alla protezione dei dati non era, in quanto tale, una sanzione, nonostante il fatto che in pratica, le restrizioni imposte alla quantità delle informazioni da pubblicare possono avere reso alcune attività commerciali delle società ricorrenti meno redditizie (ibid., § 197).

394. La causa *Big Brother Watch e altri c. Regno Unito* [GC], 2021 sollevava, *inter alia*, la questione della compatibilità con l'articolo 8 della Convenzione della condivisione dei dati intercettati da Servizi segreti stranieri, in tale causa la US National Security Agency ("NSA"). La Corte ha dichiarato che lo scambio di dati doveva essere disciplinato da chiare regole dettagliate che dessero ai cittadini un'adeguata indicazione delle circostanze in cui, e delle condizioni alle quali, le autorità erano autorizzate a formulare tali domande e che fornissero effettive garanzie contro l'uso di tale potere per eludere il diritto interno e/o gli obblighi degli Stati ai sensi della Convenzione. Quando riceve il materiale intercettato, lo Stato ricevente deve essere munito di adeguate garanzie per l'esame, l'utilizzazione e la memorizzazione; per la sua ulteriore trasmissione; e per la sua cancellazione e distruzione. Tali garanzie erano applicabili anche alla ricezione, da parte di uno Stato contraente, di materiale intercettato sollecitato da un Servizio segreto straniero. Se gli Stati non sempre sapevano se il materiale pervenuto da Servizi segreti stranieri fosse il prodotto di intercettazioni, la Corte ha ritenuto che avrebbero dovuto essere applicati i medesimi criteri a tutto il materiale pervenuto da Servizi segreti stranieri che poteva essere il prodotto di intercettazioni. Infine, un regime che permetteva ai Servizi segreti di chiedere a Stati non contraenti l'intercettazione, o il materiale intercettato, dovrebbe essere soggetto a un controllo indipendente, e dovrebbe sussistere anche la possibilità di un riesame indipendente *ex post facto* (ibid., §§ 498-499).

Elenco delle cause citate

La giurisprudenza citata nella presente Guida rinvia alle sentenze o alle decisioni pronunciate dalla Corte o ai rapporti della Commissione europea dei diritti dell'uomo ("la Commissione").

Salva diversa indicazione, tutti i riferimenti riguardano una sentenza di merito pronunciata da una Camera della Corte. L' abbreviazione "(dec.)" indica che la citazione rinvia a una decisione della Corte e "[GC]" che la causa è stata esaminata dalla Grande Camera.

Nell'elenco che segue le sentenze delle Camere non definitive ai sensi dell'articolo 44 della Convenzione sono contrassegnate da un asterisco. L'articolo 44 § 2 della Convenzione prevede: "La sentenza di una Camera diviene definitiva (a) quando le parti dichiarano che non chiederanno il rinvio del caso dinnanzi alla Grande Camera; oppure (b) tre mesi dopo la data della sentenza, se non è stato chiesto il rinvio del caso dinnanzi alla Grande Camera; oppure (c) quando il collegio della Grande Camera respinge una richiesta di rinvio formulata ai sensi dell'articolo 43". Nei casi in cui il collegio della Grande Camera accoglie la richiesta di rinvio la sentenza della Camera non diviene definitiva e non ha pertanto effetti giuridici; la sentenza che diviene definitiva è la successiva sentenza pronunciata dalla Grande Camera.

I collegamenti ipertestuali alle cause citate nella versione elettronica della Guida rinviano alla banca dati HUDOC (http://hudoc.echr.coe.int) che permette di accedere alla giurisprudenza della Corte (sentenze e decisioni della Grande Camera, delle Camere e dei Comitati, cause comunicate, pareri consultivi e sintesi giuridiche tratte dai bollettini informativi sulla giurisprudenza), e della Commissione (decisioni e rapporti) nonché alle risoluzioni del Comitato dei Ministri.

La Corte pronuncia le sentenze e le decisioni in inglese e/o in francese, le sue due lingue ufficiali. La banca dati HUDOC contiene anche le traduzioni di numerose importanti cause in quasi trenta lingue non ufficiali, nonché collegamenti a circa un centinaio di raccolte giurisprudenziali online prodotte da terzi. All the language versions available for cited cases are accessible via the 'Language versions' tab in the HUDOC database, a tab which can be found after you click on the case hyperlink.

—A—

A.B. c. Paesi Bassi, n. 37328/97, 29 gennaio 2002
A.P., Garçon e Nicot c. Francia, nn. 79885/12 e altri 2, CEDU 2017
Adomaitis c. Lituania, n. 14833/18, 18 gennaio 2022
Akgün c. Turchia, n. 19699/18, 20 luglio 2021
Allan c. Regno Unito, n. 48539/99, CEDU 2002-IX
Alexandridis c. Grecia, n. 19516/06, 21 febbraio 2008
Alkaya c. Turchia, n. 42811/06, 9 ottobre 2012
Alpha Doryforiki Tileorasi Anonymi Etairia c. Grecia, n. 72562/10, 22 febbraio 2018
Amann c. Svizzera [GC], n. 27798/95, CEDU 2000-II
Anchev c. Bulgaria (dec.), nn. 38334/08 e 68242/16, 5 dicembre 2017
André e altri c. Francia, n. 18603/03, 24 luglio 2008
Antoneta Tudor c. Romania, n. 23445/04, 24 settembre 2013
Antović e Mirković c. Montenegro, n. 70838/13, 28 novembre 2017
Apostu c. Romania, n. 22765/12, 3 febbraio 2015
Armonienė c. Lituania, n. 36919/02, 25 novembre 2008
Associazione «21 Dicembre 1989» e altri c. Romania, nn. 33810/07 e 18817/08, 24 maggio 2011
Associazione per l'integrazione europea e i diritti umani ed Ekimdzhiev c. Bulgaria, n. 62540/00, 28 giugno 2007
Avilkina e altri c. Russia, n. 1585/09, 6 giugno 2013

Axel Springer AG c. Germania [GC], n. 39954/08, 7 febbraio 2012
Axel Springer SE and RTL Television GmbH c. Germania, n. 51405/12, 21 settembre 2017
Aycaguer c. Francia, n. 8806/12, 22 giugno 2017

—B—

B.B. c. Francia, n. 5335/06, 17 dicembre 2009
Batiashvili c. Georgia, n. 8284/07, 10 ottobre 2019
Bărbulescu c. Romania [GC], n. 61496/08, 5 settembre 2017 (estratti)
Bédat c. Svizzera [GC], n. 56925/08, CEDU 2016
Beghal c. Regno Unito, n. 4755/16, 28 febbraio 2019
Benedik c. Slovenia, n. 62357/14, 24 aprile 2018
Ben Faiza c. Francia, n. 31446/12, 8 febbraio 2018
Bernh Larsen Holding AS e altri c. Norvegia, n. 24117/08, 14 marzo 2013
Biancardi c. Italia, n. 77419/16, 25 novembre 2021
Big Brother Watch e altri c. Regno Unito [GC], nn. 58170/13 e altri 2, 25 maggio 2021
Biriuk c. Lituania, n. 23373/03, 25 novembre 2008
Bogomolova c. Russia, n. 13812/09, 20 giugno 2017
Boljević c. Serbia, n. 47443/14, 16 giugno 2020
Brunet c. Francia, n. 21010/10, 18 settembre 2014
Breyer c. Germania, n. 50001/12, 30 gennaio 2020
Buck c. Germania, n. 41604/98, CEDU 2005-IV
Buturugă c. Romania, n. 56867/15, 11 febbraio 2020
Bykov c. Russia [GC], n. 4378/02, 10 marzo 2009

—C—

C.C. c. Spagna, n. 1425/06, 6 ottobre 2009
Cakicisoy e altri c. Cipro (dec.), n. 6523/12, 23 settembre 2014
Canonne c. Francia (dec.), n. 22037/13, 2 giugno 2015
Caruana c. Malta (dec.), n. 41079/16, 15 maggio 2018
Catt c. Regno Unito, n. 43514/15, 24 gennaio 2019
Cemalettin Canlı c. Turchia, n. 22427/04, 18 novembre 2008
Centre for Democracy and the Rule of Law c. Ukraine c. Ucraina, n. 10090/16, 26 marzo 2020
Centrum för rättvisa c. Svezia [GC], n. 35252/08, 25 maggio 2021
Cevat Özel c. Turchia, n. 19602/06, 7 giugno 2016
Christine Goodwin c. Regno Unito [GC], n. 28957/95, CEDU 2002-VI
Ciubotaru c. Moldavia, n. 27138/04, 27 aprile 2010
Coban c. Spagna (dec.), n. 17060/02, 25 settembre 2006
Copland c. Regno Unito, n. 62617/00, CEDU 2007-I
Cossey c. Regno Unito, 27 settembre 1990, Serie A n. 184
Craxi c. Italia (n. 2), n. 25337/94, 17 luglio 2003

—D—

D.L. c. Bulgaria, n. 7472/14, 19 maggio 2006
Dalea c. Francia (dec.), n. 964/07, 2 febbraio 2010
DELTA PEKÁRNY a.s. c. Repubblica ceca, n. 97/11, 2 ottobre 2014
Demirtepe c. Francia, n. 34821/97, CEDU 1999-IX (estratti)

Deveci c. Turchia (dec.), n. 42785/11, 28 giugno 2022
Dimitras e altri c. Grecia, nn. 42837/06 e altri 4, 3 giugno 2010
Dimitrov-Kazakov c. Bulgaria, n. 11379/03, 10 febbraio 2011
Doerga c. Paesi Bassi, n. 50210/99, 27 aprile 2004
Dragan Petrović c. Serbia, n. 75229/10, 14 aprile 2020
Dragojević c. Croazia, n. 68955/11, 15 gennaio 2015
Drakšas c. Lituania, n. 36662/04, 31 luglio 2012
Drelon c. Francia, nn. 3153/16 e 27758/18, 8 settembre 2022
Dudgeon c. Regno Unito, 22 ottobre 1981, Serie A n. 45
Dumitru Popescu c. Romania (n. 2), n. 71525/01, 26 aprile 2007
Dupuis e altri c. Francia, n. 1914/02, 7 giugno 2007

—E—

Editions Plon c. Francia, n. 58148/00, CEDU 2004-IV
Editorial Board of Pravoye Delo e Shtekel c. Ucraina, n. 33014/05, CEDU 2011 (estratti)
Egeland e Hanseid c. Norvegia, n. 34438/04, 16 aprile 2009
Ekimdzhiev e altri c. Bulgaria, n. 70078/12, 11 gennaio 2022
Elberte c. Lettonia, n. 61243/08, CEDU 2015
Erdem c. Germania, n. 38321/97, CEDU 2001-VII (estratti)
Ernst e altri c. Belgio, n. 33400/96, 15 luglio 2003
Eternit c. Francia (dec.), n. 20041/10, 27 marzo 2012

—F—

Financial Times Ltd e altri c. Regno Unito, n. 821/03, 15 dicembre 2009
Florindo de Almeida Vasconcelos Gramaxo c. Portogallo, n. 26968/16, 13 dicembre 2022
Foxley c. Regno Unito, n. 33274/96, 20 giugno 2000
Frâncu c. Romania, n. 69356/13, 13 ottobre 2020
Friedl c. Austria, n. 15225/89, Rapporto della Commissione, 19 maggio 1994

—G—

G.S.B. c. Svizzera, n. 28601/11, 22 dicembre 2015
Gafiuc c. Romania, n. 59174/13, ottobre 2020
Gardel c. Francia, n. 16428/05, CEDU 2009
Garnaga c. Ucraina, n. 20390/07, 16 maggio 2013
Gaskin c. Regno Unito, 7 luglio 1989, Serie A n. 160
Gaughran c. Regno Unito, n. 45245/15, 13 febbraio 2020
Gawlik c. Liechtenstein, n. 23922/19, 16 febbraio 2021
Giesbert e altri c. Francia, nn. 68974/11 e altri 2, 1er giugno 2017
Gillan e Quinton c. Regno Unito, n. 4158/05, CEDU 2010 (estratti)
Gîrleanu c. Romania, n. 50376/09, 26 giugno 2018
Godelli c. Italia, n. 33783/09, 25 settembre 2012
Gorlov e altri c. Russia, nn. 27057/06 e altri 2, 2 luglio 2019
Görmüş e altri c. Turchia, n. 49085/07, 19 gennaio 2016
Grant c. Regno Unito, n. 32570/03, CEDU 2006-VII
Greuter c. Paesi Bassi (dec.), n. 40045/98, 19 marzo 2002
Guerra e altri c. Italia, n. 14967/89, *Reports of Judgments and Decisions* 1998-I

Guillot c. Francia, 24 ottobre 1996, *Reports of Judgments and Decisions* 1996-V
Guiorgui Nikolaïchvili c. Georgia, n. 37048/04, 13 gennaio 2009
Güzel Erdagöz c. Turchia, n. 37483/02, 21 ottobre 2008

—H—

Haldimann e altri c. Svizzera, n. 21830/09, CEDU 2015
Halford c. Regno Unito, 25 giugno 1997, *Reports of Judgments and Decisions* 1997-III
Hämäläinen c. Finlandia [GC], n. 37359/09, CEDU 2014
Haralambie c. Romania, n. 21737/03, 27 ottobre 2009
Hájovský c. Slovacchia, n. 7796/16, 1 luglio 2021
Haščák c. Slovacchia, nn. 58359/12 e altri 2, 23 giugno 2022
Hassine c. Romania, n. 36328/13, 9 marzo 2021
Heglas c. Repubblica ceca, n. 5935/02, 1 marzo 2007
Henry Kismoun c. Francia, n. 32265/10, 5 dicembre 2013
Huvig c. Francia, 24 aprile 1990, Serie A n. 176-B

—I—

I. c. Finlandia, n. 20511/03, 17 luglio 2008
I. c. Regno Unito [GC], n. 25680/94, 11 luglio 2006
Iordachi e altri c. Repubblica di Moldavia, n. 25198/02, 10 febbraio 2009
İrfan Güzel c. Turchia, n. 35285/08, 7 febbraio 2017
Ivashchenko c. Russia, n. 61064/10, 13 febbraio 2018

—J—

J.L. c. Italia, n. 5671/16, 27 maggio 2021
J.P.D. c. Francia (dec.), n. 55432/10, 16 settembre 2016
J.S. c. Regno Unito (dec.), 445/10, 3 marzo 2015
Jäggi c. Svizzera, n. 58757/00, CEDU 2006-X
Jarnea c. Romania, n. 41838/05, 19 luglio 2011
Jecker c. Svizzera, n. 35449/14, 6 ottobre 2020
Joanna Szulc c. Polonia, n. 43932/08, § 13 novembre 2012

—K—

K.H. e altri c. Slovacchia, n. 32881/04, CEDU 2009 (estratti)
K.S. e M.S. c. Germania, n. 33696/11, 6 ottobre 2016
K.U. c. Finlandia, n. 2872/02, CEDU 2008
Kahn c. Germania, n. 16313/10, 17 marzo 2016
Karabeyoğlu c. Turchia, n. 30083/10, 7 giugno 2016
Kennedy c. Regno Unito, n. 26839/05, 18 maggio 2010
Khadija Ismayilova c. Azerbaigian, nn. 65286/13 e 57270/14, 10 gennaio 2019
Khan c. Regno Unito, n. 35394/97, CEDU 2000-V
Khoujine e altri c. Russia, n. 13470/02, 23 ottobre 2008
Khelili c. Svizzera, n. 16188/07, 18 ottobre 2011
Kinnunen c. Finlandia, n. 18291/91, decisione della Commissione, 13 ottobre 1993

Kinnunen c. Finlandia, n. 24950/94, decisione della Commissione, 15 maggio 1996
Kırdök e altri c. Turchia, n. 14704/12, 3 dicembre 2019
Kiyutin c. Russia, n. 2700/10, CEDU 2011
Klass e altri c. Germania, 6 settembre 1978, Serie A n. 28
Khmel c. Russia, n. 20383/04, 12 dicembre 2013
Konovalova c. Russia, n. 37873/04, 9 ottobre 2014
Köpke c. Germania (dec.), n. 420/07, 5 ottobre 2010
Kotilainen e altri c. Finlandia, n. 62439/12, 17 settembre 2020
Krone Verlag GmbH & Co. KG c. Austria, n. 34315/96, 26 febbraio 2002
Kruglov e altri c. Russia, nn. 11264/04 e altri 15, 4 febbraio 2020
Kruslin c. Francia, 24 aprile 1990, Serie A n. 176-A
Kurier Zeitungsverlag und Druckerei GmbH c. Austria, n. 3401/07, 17 gennaio 2012
Kvasnica c. Slovacchia, n. 72094/01, 9 giugno 2009

—L—

L.H. c. Lettonia, n. 52019/07, 29 aprile 2014
L.L. c. Francia, n. 7508/02, CEDU 2006-XI
Labita c. Italia [GC], n. 26772/95, CEDU 2000-IV
Lambert c. Francia, n. 23618/94, *Reports of Judgments and Decisions* 1998-V
Lavents c. Lettonia, n. 58442/00, 28 novembre 2002
Leander c. Svezia, 26 marzo 1987, Serie A n. 116
Libert c. Francia, n. 588/13, 22 febbraio 2018
Liberty e altri c. Regno Unito, n. 58243/00, 1 luglio 2008
Liblik e altri c. Estonia, n. 173/15 and 5 others, 28 maggio 2019
Liebscher c. Austria, n. 5434/17, 6 aprile 2021
López Ribalda e altri c. Spagna [GC], nn. 1874/13 e 8567/13, 17 ottobre 2019
Lüdi c. Svizzera, n. 12433/86, Serie A n. 238
Lupker e altri c. Paesi Bassi, 18395/91, decisione della Commissione, 7 dicembre 1992

—M—

M.B. c. Francia, n. 22115/06, 17 dicembre 2009
M.C. c. Regno Unito, n. 51220/13, 30 marzo 2021
M.D. e altri c. Spagna, n. 36584/17, 28 giugno 2022
M.G. c. Regno Unito, n. 39393/98, 24 settembre 2002
M.K. c. Francia, n. 19522/09, 18 aprile 2013
M.L. e W.W. c. Germania, nn. 60798/10 e 65599/10, 28 giugno 2018
M.M. c. Regno Unito, n. 24029/07, 13 novembre 2012
M.N. e altri c. San Marino, n. 28005/12, 7 luglio 2015
M.P. c. Portogallo, n. 27516/14, 7 settembre 2021
M.S. c. Svezia, 27 août 1997, *Reports of Judgments and Decisions* 1997-IV
MGN Limited c. Regno Unito, n. 39401/04, 18 gennaio 2011
Magyar Helsinki Bizottság c. Ungheria [GC], n. 18030/11, CEDU 2016
Malanicheva c. Russia (dec.), n. 50405/06, 31 maggio 2016
Malone c. Regno Unito, 2 agosto 1984, Serie A n. 82
Marchiani c. Francia (dec.), n. 30392/03, 27 maggio 2008
Matheron c. Francia, n. 57752/00, 29 marzo 2005
McGinley ed Egan c. Regno Unito, 9 giugno 1998, *Reports of Judgments and Decisions* 1998-III

—N—

—O—

—P—

Petrova c. Lettonia, n. 4605/05, 24 giugno 2014
Pinto Coelho c. Portogallo (n. 2), n. 48718/11, 22 marzo 2016
Polanco Torres e Movilla Polanco c. Spagna, 34147/06, 21 settembre 2010
Prado Bugallo c. Spagna, n. 58496/00, 18 febbraio 2003
Pruteanu c. Romania, n. 30181/05, 3 febbraio 2015

—R—

R.E. c. Regno Unito, n. 62498/11, 27 ottobre 2015
Radio Twist, a.s. c. Slovacchia, n. 62202/00, CEDU 2006-XV
Radu c. Repubblica di Moldavia, n. 50073/07, 15 aprile 2014
Rees c. Regno Unito, n. 9532/81, Serie A n. 106
Reklos e Davourlis c. Grecia, n. 1234/05, 15 gennaio 2009
Ricci c. Italia, n. 30210/06, 8 ottobre 2013
Robathin c. Austria, n. 30457/06, 3 luglio 2012
Roche c. Regno Unito [GC], n. 32555/96, CEDU 2005-X
Roemen e Schmit c. Lussemburgo, n. 26419/10, CEDU 2003-IV
Roman Zakharov c. Russia [GC], n. 47143/06, CEDU 2015
Rook c. Germania, n. 1586/15, 25 luglio 2019
Rotaru c. Romania [GC], n. 28341/95, CEDU 2000-V

—S—

S. e Marper c. Regno Unito [GC], nn. 30562/04 e 30566/04, CEDU 2008
S.V. c. Italia, n. 55216/08, 11 ottobre 2018
Sanoma Uitgevers B.V. c. Paesi Bassi [GC], n. 38224/03, 14 settembre 2010
Samoylova c. Russia, n. 49108/11, 14 dicembre 2021
Šantare e Labazņikovs c. Lettonia, n. 34148/07, 31 marzo 2016
Särgava c. Estonia, n. 698/19, 16 novembre 2021
Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia [GC], n. 931/13, CEDU 2017 (estratti)
Schmidt c. Germania (dec.), n. 32352/02, 5 gennaio 2006
Sciacca c. Italia, n. 50774/99, CEDU 2005-I
Sedletska c. Ucraina, n. 42634/18, 1 aprile 2021
Segerstedt-Wiberg e altri c. Svezia, n. 62332/00, CEDU 2006-VII
Sérvulo & Associados - Sociedade de Advogados, RL, e altri c. Portogallo, n. 27013/10, 3 settembre 2015
Sheffield e Horsham c. Regno Unito, 30 luglio 1998, *Reports of Judgments and Decisions* 1998-V
Sher e altri c. Regno Unito, n. 5201/11, CEDU 2015 (estratti)
Shimovolos c. Russia, n. 30194/09, 21 giugno 2011
Silver e altri c. Regno Unito, 25 marzo 1983, Serie A n. 61
Sinan Işık c. Turchia, n. 21924/05, CEDU 2010
Smirnov c. Russia, n. 71362/01, 7 giugno 2007
Smith e Grady c. Regno Unito, n. 33985/96 e 33986/96, *Reports of Judgments and Decisions* 1999-VI
Société de Conception de Presse et d'Édition c. Francia, n. 4683/11, 25 febbraio 2016
Söderman c. Svezia [GC], n. 5786/08, CEDU 2013
Sommer c. Germania, n. 73607/13, 27 aprile 2017
Sõro c. Estonia, n. 22588/08, 3 settembre 2015
Standard Verlagsgesellschaft mbH c. Austria (n. 3), n. 39378/15, 7 dicembre 2021
Stolkosa c. Polonia (dec.), n. 68562/14, 14 settembre 2021
Succession Kresten Filtenborg Mortensen c. Danimarca (dec.), n. 1338/03, CEDU 2006-V

—T—

—U—

—V—

—W—

Willems c. Paesi Bassi (dec.), n. 57294/16, 9 novembre 2021
Wirtschafts-Trend Zeitschriften-Verlagsgesellschaft mbH c. Austria (n. 2) (dec.), n. 62746/00, CEDU 2002-X
Wisse c. Francia, n. 71611/01, 20 dicembre 2005

—X—

X e altri c. Russia, nn. 78042/16 e 66158/14, 14 gennaio 2020

—Y—

Y. c. Turchia (dec.), n. 648/10, 17 febbraio 2015
Y.B. e altri c. Turchia, nn. 48173/99 e 48319/99, 28 ottobre 2004
Y.G. c. Russia, n. 8647/12, 30 agosto 2022
Y.Y. c. Russia, n. 40378/06, 23 febbraio 2016
Yonchev c. Bulgaria, n. 12504/09, 7 dicembre 2017
Youth Initiative for Human Rights c. Serbia, n 48135/06, 25 giugno 2013
Yvonne Chave née Jullien c. Francia, n. 14461/88, decisione della Commissione del 9 luglio 1991

—Z—

Z c. Finlandia, 25 febbraio 1997, *Reports of Judgments and Decisions* 1997-I
Zoltán Varga c. Slovacchia, nn. 58361/12 e altri 2, 20 luglio 2021