INTERPRETAZIONE EVOLUTIVA E TECNOLOGIA NELLA GIURISPRUDENZA DELLE CORTI*

CHIARA GRAZIANI**

Sommario

Abstract

This work examines the impact of the technological development in the case law of courts – not only supreme and constitutional, but also ordinary ones – in Western "advanced" democracies. In other words, the author aims to grasp to what extent the evolution of technology tools had an influence on how courts interpret some provisions (especially, but not just, constitutional ones).

In order to restrict the scope of the analysis, this contribution addresses the above-mentioned topic from a specific perspective: that of the use of technology for public security purposes, with a focus on counter-terrorism measures.

The analysis identifies different trends in the approach of courts to technology in their interpretative efforts and argues, first, that a "technologically-oriented interpretation" should be welcome, and, second, that courts should always explicitly clarify that they are interpreting some provisions in the light of the technological evolution. In this way, the importance of the reasoning of judicial decisions would be emphasized, benefitting both policy-makers and civil society.

Suggerimento di citazione

C. GRAZIANI, *Interpretazione evolutiva e tecnologia nella giurisprudenza delle Corti*, in *Osservatorio sulle fonti*, n. 3/2021. Disponibile in: http://www.osservatoriosullefonti.it

* Il contributo costituisce la rielaborazione della relazione tenuta al seminario "Tempo e mutamento nel sistema delle fonti", organizzato dalla *Rivista* e svoltosi il 1° ottobre 2021.

L'Autrice ringrazia i *discussants* per le osservazioni e i commenti in merito alle riflessioni proposte.

** Assegnista di ricerca in Diritto Pubblico Comparato presso l'Università di Milano-Bicocca; *academic fellow* (docente a contratto) presso l'Università Bocconi di Milano.

Contatti chiara.graziani@unimib.it; chiara.graziani@unibocconi.it.

Registrazione presso il Tribunale di Firenze n. 5626 del 24 dicembre 2007
Rivista inclusa nella classe A delle Riviste scientifiche di Area 12 – Direttore Prof. Paolo Caretti
ISSN 2038-5633

1. Introduzione

Il rapporto che esiste tra diritto e tecnologia può essere letto da almeno due macro-angolature[1]. In primo luogo, esso si può inquadrare dal punto di vista del Legislatore, il quale, nel tentativo di tenere dietro al rapidissimo incedere dell'evoluzione tecnologica, si trova spesso a fare fronte a significative sfide. La prospettiva è, in questo caso, principalmente *de iure condendo*, nel senso che l'interazione del diritto con la tecnologia interessa il *law-maker* soprattutto nel momento in cui è necessario adottare un nuovo assetto regolatorio – o modificare quello esistente – per tenere in debito conto lo sviluppo tecnologico[2].

È possibile, in secondo luogo, prendere in esame la relazione tra diritto e tecnologia dal punto di vista delle corti, che, nel proprio ruolo di interpreti del diritto, si vedono impegnate in sforzi esegetici che tengano in considerazione il continuo progresso dei *technology tools*. Si tratta di un'analisi che si può definire, in maniera preponderante, *de iure condito*, perché i giudici, dato un certo quadro normativo già esistente, si trovano a doverne dare una lettura che dia conto del progresso della tecnologia.

Il presente contributo si concentra su questo secondo versante. In particolare, ci si accinge a esaminare come e se il fattore tecnologico abbia contribuito ad orientare le corti nell'interpretazione delle disposizioni – soprattutto costituzionali, ma non solo – applicabili ad un caso pendente. Il lavoro si focalizza su un particolare utilizzo della tecnologia, ossia quello finalizzato a contrastare alcune delle più importanti minacce alla sicurezza[3], che caratterizzano il XXI

[1] Entrambe queste prospettive richiedono un significativo sforzo interdisciplinare, venendo a confronto il mondo del diritto con quello della tecnologia. Sul tema dell'interdisciplinarietà e sulle sfide che essa lancia al diritto, v. A. VEDASCHI, *Diritto comparato e interdisciplinarietà: tra innata vocazione e incompiuta realizzazione?*, in *Dir. pubbl. comp. eur.*, 2, 2021, 301 ss.

[2] Sul rapporto fra tecnologia e politica, v. E. CATELANI, *Evoluzione del rapporto tra tecnica e politica. Quali saranno gli effetti di uno "Stato tecnologico"?*, in *Osservatorio sulle fonti*, disponibile all'indirizzo http://www.osservatoriosullefonti.it/, 2, 2021, 382 ss.

[3] Il concetto di sicurezza è stato oggetto, nel corso del tempo, delle più varie elaborazioni a livello giuridico, filosofico e politologico. Non potendosi compiutamente soffermare sulle origini storiche (su cui v., per tutti, M. BARBERIS, *Non c'è sicurezza senza libertà. Il fallimento delle politiche antiterrorismo*, il Mulino, Bologna, 2017), ci si limita qui a rammentare le principali teorizzazioni *post*-11 settembre 2001. Secondo alcuni Autori, la sicurezza, anche dopo gli attentati terroristici del 2001, deve continuare ad essere concepita come un limite eccezionale alla "regola", che è costituita dal godimento pieno dei diritti e delle libertà. In questo senso, A. PACE, *Libertà e sicurezza. Cinquant'anni dopo*, in *Diritto e società*, 2, 2013, 177 ss. Questa idea riprende e conferma quella propria del periodo storico precedente all'11 settembre 2001, diffusa tra la dottrina italiana, ma pure fra quella francese. V., al proposito, A. PACE, *Il concetto di ordine pubblico nella Costituzione italiana*, in *Arch. Giur.*, CLXV, 1963, 111 ss. e M. HAURIOU, *Précis de droit constitutionnel*, Sirey, Paris, 1929, 62 ss. Una seconda posizione, invece, fa assurgere la sicurezza a vero e proprio diritto soggettivo, bilanciabile con gli altri. In questo senso, G. DE VERGOTTINI, *La difficile convivenza fra libertà e sicurezza: la risposta delle democrazie al terrorismo. Gli ordinamenti nazionali*, in *AIC, Libertà e sicurezza nelle democrazie contemporanee*, Atti del XVII Convegno Annuale dell'Associazione, Bari, 17-18 ottobre 2003, Padova, 2007, 56 ss.; T.E. FROSINI, C. BASSU, *La libertà personale nell'emergenza costituzionale*, in A. DI

secolo fin dagli albori, ovvero il pericolo del terrorismo internazionale[4]. Tale delimitazione del perimetro di indagine si è ritenuta necessaria non solo e non tanto per esigenze di contenimento del contributo, ma soprattutto per assicurare una certa omogeneità dei *case-studies* presi in esame e, di conseguenza, una comparabilità sotto il profilo scientifico che potesse condurre a risultati metodologicamente corretti.

L'analisi si caratterizza per il respiro comparato, prima orizzontale (sez. 2), poi verticale (sez. 3). Sul primo fronte, la comparazione è attuata fra il piano europeo (§ 2.1.) – intendendosi per tale la giurisprudenza delle corti, non solo costituzionali e supreme ma anche di merito, di alcuni selezionati Stati membri – e quello statunitense (§ 2.2.) – con riferimento precipuo al *corpus* giurisprudenziale della Corte Suprema federale.

Per quanto riguarda la comparazione verticale, invece, si prendono in esame le corti sovranazionali, limitatamente, questa volta, alla sola area europea, non essendo gli Stati Uniti incasellati in alcun sistema sovranazionale che implichi la giurisdizione di una corte sovrastatale. Viene quindi esplorato il panorama giurisprudenziale offerto dalla Corte europea dei diritti dell'uomo (§ 3.1) e dalla Corte di giustizia dell'Unione europea (§ 3.2).

Seguono, infine, alcune considerazioni conclusive che rilevano similitudini e differenze negli approcci presi in considerazione.

2. Corti, interpretazione e tecnologia: uno sguardo "orizzontale"

Al fine di esaminare la tematica proposta comparando il contesto europeo e quello statunitense, tre preliminari precisazioni si rendono opportune.

La prima è di tipo generale e costituisce la premessa dell'intera analisi svolta in questo lavoro. Infatti, l'esame del binomio tecnologia-diritto sotto il profilo della sicurezza e dall'ottica giurisprudenziale chiama necessariamente in causa un terzo termine, che deve essere sotteso a qualsiasi ragionamento in merito. Si tratta della tutela dei diritti e delle libertà individuali, che spesso finiscono per essere le "vittime collaterali" di quelle misure volte a garantire la sicurezza dei cittadini che fanno largo utilizzo del fattore tecnologico. È chiaro che "vittime" sono soprattutto quei diritti maggiormente toccati dall'elemento

GIOVINE (a cura di), *Democrazie protette e protezione della democrazia*, Giappichelli, Torino, 2005, 77 ss. Un'ulteriore visione legge la sicurezza come un valore costituzionale, presupposto imprescindibile per il godimento di tutti gli altri diritti e libertà e, quindi, mai soggetto al bilanciamento con gli altri. G. CERRINA FERONI, G. MORBIDELLI, *La sicurezza: un valore superprimario*, in *Percorsi cost.*, 1/2008, 31 ss.

[4] A. VEDASCHI, À la guerre comme à la guerre*? La disciplina della guerra nel diritto costituzionale comparato*, Giappichelli, Torino, 2007.

tecnologico, e cioè la *privacy* e la libertà di espressione, nelle loro diverse declinazioni e accezioni[5].

La seconda precisazione è il portato diretto della prima osservazione e la cala nel contesto della comparazione tra lo scenario europeo e quello statunitense. A tal riguardo, conviene ricordare che i due contesti[6] si distinguono per letture assai diverse – almeno tradizionalmente – delle garanzie della *privacy* e della libertà di espressione[7]. Se negli Stati Uniti il IV Emendamento viene, in via di regola, considerato recessivo dinanzi ad altri interessi contrapposti (la sicurezza è uno di questi)[8], il versante europeo è solitamente indicato come terreno più "fertile" per la tutela della *privacy* (e della correlata, ma più "giovane", *data protection*[9]). D'altro canto, gli Stati Uniti sono visti come la culla del *marketplace of ideas*, grazie a storiche sentenze della Corte Suprema che hanno interpretato il I Emendamento (e in particolare la *free speech clause*) come un diritto quasi assoluto[10]. Tali nette differenze possono certamente essere messe in discussione e, anzi, sono proprio le reazioni giuridiche alle sfide

[5] In particolare, in tema di *privacy*, va rilevato il suo accostamento, soprattutto in epoca contemporanea, con il diritto alla protezione dei dati personali (*data protection*). A questo proposito, si deve notare che, in dottrina, vi sono opinioni divergenti, circa lo statuto giuridico di questi due diritti. Secondo alcuni, la *privacy* e la *data protection* sarebbero due diritti distinti e, quindi, la *data protection* godrebbe di propria autonomia. Nello specifico, mentre il diritto alla *privacy* si limiterebbe a tutelare la "non interferenza" del potere pubblico nella sfera privata, la *data protection* avrebbe una natura maggiormente garantistica, volta a tutelare un novero più ampio di dati rispetto a quelli strettamente attinenti alla sfera personale. In questo senso, O. LINKSEY, *Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order*, in 63 *International and Comparative Law Quarterly*, 2014, 569 ss. Per altri Autori, invece, la *data protection* non sarebbe altro che l'altra faccia della medaglia della *privacy*, ossia la tutela "in positivo" (che implica un *facere* delle autorità pubbliche) o "dinamica" del diritto alla vita privata e personale. V. S. RODOTÀ, *Il diritto di avere diritti*, Laterza, Bari, 397. Per altri ancora, poi, bisogna assumere una posizione intermedia e considerare la *data protection* alla stregua dell'"avanzamento" della *privacy*, resasi necessaria nella c.d. *digital society*. C. DOCKESEY, *Four Fundamental Rights: Striking the Balance*, in 6 *International Data Privacy Law*, 3/2016, 195, 197.

[6] Non è ancora opportuno di parlare di ordinamenti giuridici, dato che l'Europa viene presa in considerazione per alcuni tratti comuni che caratterizzano le corti nazionali di tale area .

[7] D. COLE, F. FABBRINI, *Bridging the transatlantic divide? The United States, the European Union, and the protection of privacy across borders*, in 14 *International Journal of Constitutional Law*, 2016, 255 ss. V., inoltre, L.P. VANONI, *Balancing privacy and national security in the global digital era: a comparative perspective of EU and US constitutional systems*, in *Forum di Quaderni Costituzionali*, disponibile all'indirizzo https://www.forumcostituzionale.it/wordpress/wp-content/uploads/2017/05/vanoni.pdf, 14 giugno 2017.

[8] Per le prime teorizzazioni di un'idea di *right to be let alone*, v. S. WARREN, L. BRANDEIS, *The Right to Privacy*, in 4 *Harvard Law Review* 1890, 193 ss. Circa le (numerose) eccezioni elaborate negli Stati Uniti rispetto alla tutela della *privacy*, v. *infra* nel presente contributo.

[9] Cfr. *supra*, nota 5.

[10] Il primo riferimento, da parte della Corte Suprema degli Stati Uniti, al *marketplace of ideas* deve rinvenirsi nella sentenza *Abrams v. United States*, 250 U.S. 616 (1919). A livello teorico, tuttavia, il concetto era già stato elaborato da J.S. MILL, *On Liberty*, The Walter Scott Publishing Co., Ltd, London and Felling-on-Tyne-New York and Melbourne, 1859.

alla sicurezza *post* 9/ 11 ad averle fatte vacillare; tuttavia, non si può negare che questa impostazione tradizionale in materia di *privacy* e di libertà di espressione nei due contesti di riferimento abbia influenzato gli atteggiamenti delle corti che i seguenti paragrafi vanno a dettagliare.

Il terzo *caveat*, essenziale prima di entrare nel vivo dell'analisi giurisprudenziale, è metodologico. Per quanto concerne l'Europa, i *case-studies* giurisprudenziali trattati nel § 2.1. sono tutti relativi a Paesi dell'Europa occidentale definibili come democrazie mature. La scelta è maturata al fine assicurare una comparabilità con il sistema statunitense, oggetto del § 2.2., che sarebbe stata messa in crisi da eventuali riferimenti – pur importanti e che potrebbero essere l'oggetto di una diversa analisi – a corti di Paesi europei che non rientrano nella categoria sopra indicata[11].

2.1 Il contesto europeo: le corti interne

L'impatto che il fattore tecnologico ha avuto sulle linee interpretative delle corti dei Paesi dell'area europea è vario e piuttosto frammentato. Si possono distinguere perlomeno quattro tendenze, ciascuna delle quali può essere esemplificata da diversi casi concreti.

Un primo *trend* consiste nell'accettazione piuttosto acritica dell'utilizzo della tecnologia nell'ambito delle misure di contrasto alle minacce alla sicurezza e nella rinuncia, per certi versi aprioristica, a trovare una lettura "tecnologicamente orientata" delle garanzie che il diritto nazionale predispone a favore dei diritti e delle libertà individuali. In altri termini, questo orientamento tende a non considerare in modo minuzioso i problemi aggiuntivi che la tecnologia avanzata può porre in relazione a determinate misure giuridiche e a condannarne l'operato senza un *reasoning* chiaro e dettagliato. Si tratta di una sorta di "presunzione di colpevolezza" nei confronti dell'elemento tecnologico, giudicato inidoneo a garantire qualsivoglia diritto, pur in una condizione "di tensione" come è quella dei rischi per la sicurezza. Questo approccio può essere riscontrato, tra le altre, nella pronuncia con cui, nell'aprile 2021, la Corte costituzionale belga ha dichiarato l'incostituzionalità della normativa interna in materia di *data retention* a fini di contrasto del terrorismo[12]. Questa sentenza è stata pronunciata dal giudice delle leggi belga dopo aver ottenuto la risposta ad un rinvio pregiudiziale di interpretazione sollevato dinanzi alla Corte di giustizia dell'Unione europea (CGUE)[13]. Con il rinvio, la Corte costituzionale

[11] V., ad esempio, in tema di *privacy* in Paesi dell'Est Europa, il lavoro di M.A. ORLANDI, *Estonia: sviluppo dell'"e-government", tutela della "privacy" e "cybersecurity"*, in *Rass. dir. pubbl. eur.*, 2, 2019, 383 ss.

[12] Corte costituzionale belga, *arrêt* n. 57/2021, 22 aprile 2021.

[13] Corte di giustizia dell'Unione europea (Grande Sezione), *La Quadrature du Net e a. contro Premier ministre e a.*, C-511/18, C-512/18 e C-520/18, 6 ottobre 2020. G. FORMICI, *La* data retention

belga chiedeva al giudice di Lussemburgo se la normativa dell'Unione in tema di protezione dei dati personali ostasse ad una legislazione nazionale che impone ai *providers* la raccolta e conservazione dei metadati delle comunicazioni a fini di prevenzione del terrorismo e di gravi reati transnazionali. Tra i molti motivi del rinvio, la Corte belga sottolineava come vi fosse il rischio che la tecnologia esistente, pur permettendo l'anonimizzazione dei dati nei confronti di qualsiasi soggetto non autorizzato a trattarli, non ne escludesse poi la ri-personalizzazione oppure la perdita prima della trasformazione in dati anonimi, aprendo dunque alla possibilità di abusi e *data breaches*. Pur avendo ricevuto dalla CGUE un riscontro piuttosto aperto e non certo totalmente preclusivo alla normativa interna (si tratta della recente sentenza *La Quadrature du Net and others*, su cui v. *infra*), la Corte belga, una volta trovatasi a dover chiudere il procedimento sul piano nazionale, opta per l'incostituzionalità secca. Più nel dettaglio, sullo specifico punto dell'anonimizzazione, la Corte rileva che, nonostante i *providers* siano in grado di porre in essere questo procedimento, «il y a des raisons de penser que ces données sont susceptibles de perte ou de modification», senza ulteriormente motivare il punto. Si profila, allora, secondo la Corte, una violazione dell'art. 22 della Costituzione belga (diritto alla vita privata e familiare) nonché della normativa dell'Unione europea in materia di *data protection* direttamente applicabile nell'ordinamento interno. Le violazioni rilevate dai giudici del Belgio non si limitano al profilo dell'anonimizzazione; le altre, tuttavia, non hanno una connessione diretta con l'operatività del fattore tecnologico e, pertanto, risultano di minore interesse per questo contributo. Ciò che preme rilevare è che, quando si è dovuta confrontare con il funzionamento delle tecnologie di anonimizzazione, la Corte ha proceduto con un'affermazione piuttosto apodittica e prevenuta nei confronti di queste ultime, senza tentare un'interpretazione che potesse conciliarle con l'articolato costituzionale[14].

saga *al capolinea? Le ultime pronunce della CGUE in materia di conservazione dei metadati per scopi securitari, tra conferme e nuove aperture*, in *DPCE Online*, 1, 2021, 1361 ss.

[14] V., su una posizione simile, la sentenza con cui, nel luglio 2021, l'Investigatory Powers Tribunal britannico ha dichiarato totalmente incompatibile con il diritto dell'Unione la normativa interna in materia di sorveglianza di massa, sempre in risposta ad un rinvio pregiudiziale presentato alla Corte di giustizia dell'Unione europea e risolto da quest'ultima con la sentenza *Privacy International* del 6 ottobre 2020 (si tratta, infatti, di una sentenza "gemella" rispetto alla sentenza *La Quadrature du Net*). V. Corte di giustizia dell'Unione europea (Grande Camera), *Privacy International c. Secretary of State for Foreign and Commonwealth Affairs e altri*, C-623/17, 6 ottobre 2020; *Privacy International v Secretary of State for Foreign and Commonwealth Affairs*, IPT/15/110/CH, 22 July 2021. L'Investigatory Powers Tribunal, con questa decisione, ha motivato l'incompatibilità *per relationem*, facendo ampio riferimento ai principi statuiti dalla Corte di Lussemburgo, senza calarli in modo specifico nel contesto del Regno Unito. Si nota, inoltre, che questa decisione contiene alcune *dissenting opinions*, le quali, però, non sono state rese pubbliche. È pendente, nel momento in cui si scrive questo lavoro, un ricorso

Una seconda tendenza consiste nell'utilizzo, piuttosto raffinato, di tecniche di bilanciamento sicurezza-diritti alla luce dell'aspetto tecnologico, che conduce però alla prevalenza del primo fattore (la sicurezza). Un esempio di questo atteggiamento si può trovare nella decisione con cui, nel settembre 2019, l'Alta Corte di Inghilterra e Galles si è pronunciata in merito alla *facial recognition* utilizzata dalla polizia gallese nell'ambito di grandi eventi pubblici con l'intento di prevenire eventuali pericoli per la sicurezza[15]. A questo proposito, la Corte ha avuto modo di notare come, da un lato, tale tecnologia disponga di un potenziale altissimo a fini preventivi, ma, dall'altro, implichi rischi significativi sul piano della protezione dei dati, essendo basata su algoritmi che consentono un'analisi automatizzata e su ampia scala, peraltro di dati particolarmente delicati quali sono quelli biometrici[16]. Con questa premessa, l'Alta Corte è andata ad analizzare ciascuna garanzia ritenuta dai ricorrenti violata, provando a verificare la compatibilità con la strumentazione tecnologica. Esemplificativo è il passaggio in cui ha dedotto la proporzionalità della misura di sorveglianza (tra l'altro) dal fatto che l'applicazione concreta del *tool* tecnologico fosse stata in grado di evitare "falsi positivi" e che alcuni arresti erano stati possibili solo grazie ad un tale grado di avanzamento della tecnologia. In questo modo, la Corte ha legato il funzionamento tecnico dell'algoritmo di riconoscimento facciale e le valutazioni circa la sua efficacia al principio di proporzionalità, interpretato, dunque, in una nuova luce, consapevole del "modo di funzionamento" dello strumento tecnologico. Né sotto questo profilo né sotto altri l'Alta Corte ha riscontrato violazioni del principio di proporzionalità che, in base alla Convenzione europea dei diritti dell'uomo (CEDU) come "incorporata" nel Regno Unito con lo Human Rights Act 1998[17], deve informare le limitazioni della vita privata e familiare, sia pure per esigenze di sicurezza nazionale. Pur essendo arrivata ad una conclusione prettamente "*pro* sicurezza", la Corte ha mostrato consapevolezza del fattore tecnologico, rinunciando ad un atteggiamento frettolosamente apodittico sul punto[18].

in sede di *judicial review*, presentato da Privacy International, volto a richiedere che sia ordinata la pubblicazione delle *dissenting opinions*.

[15] *R (on the application of Edward Bridges) v The Chief Constable of South Wales and others* [2019] EWHC 2341. Per un'analisi di questa decisione, v. A. PIN, *Non esiste la "pallottola d'argento": l'*Artificial Face Recognition *al vaglio giudiziario per la prima volta*, in *DPCE Online*, 4, 2019, 3075 ss.

[16] Sull'uso dei dati biometrici a fini securitari, v. C. GRAZIANI, *La creazione di* databases *di dati biometrici: l'Unione europea tra sfide alla sicurezza e* data protection, in L.E. RÍOS VEGA, L. SCAFFARDI, I. SPIGNO (a cura di), *I diritti fondamentali nell'era della* digital mass surveillance, Editoriale Scientifica, Napoli, 2021, 171 ss.

[17] Human Rights Act 1998 c. 42. V. G.F. FERRARI, *La Convenzione europea e la sua "incorporation" nel Regno Unito*, in *Dir. pubbl. comp. eur.*, 1, 1999, 125 ss.

[18] Un simile atteggiamento si riscontra in una decisione, più risalente, della Corte costituzionale tedesca in tema di sorveglianza acustica. 109 BVerfGE 279 (2004). Qui, il Tribunale di Karlsruhe riconosce l'impatto che lo sviluppo della tecnologia può avere non solo sul diritto alla *privacy*, ma

Un terzo *trend* vede anch'esso l'interpretazione bilanciata del complesso rapporto sicurezza-diritti con particolare attenzione per le *technicalities*, ma con un *outcome* diverso rispetto alla tendenza evidenziata *supra*. Si tratta di decisioni che conducono all'indubbia prevalenza del secondo elemento del binomio, ossia i diritti, quasi a sottolineare una "mancanza di fiducia" circa la capacità dell'elemento tecnologico di operare in maniera rispondente al requisito di proporzionalità. Questo atteggiamento si distingue dal primo (quello ascritto alla Corte costituzionale belga) poiché, pur conducendo agli stessi risultati – l'operato del *tool* tecnologico viene ritenuto illegittimo – giunge alla conclusione grazie ad un *reasoning* piuttosto articolato. Esemplare in questo senso è la decisione della Corte d'Appello di Inghilterra e Galles adottata nell'agosto 2020[19], dopo che la decisione prima citata dell'Alta Corte che "salvava" la *facial recognition* era stata impugnata. La sentenza di appello ha riformato la decisione di primo grado, dichiarando il sistema di riconoscimento facciale utilizzato dalla polizia gallese in violazione dell'art. 8 CEDU. Per giungere a questa conclusione, la Corte ha notato, fra l'altro, che l'algoritmo di riconoscimento facciale ha bisogno di essere "allenato" sulla base di specifici *data sets* e che la polizia gallese non era in grado di dimostrare che tali *data sets* non contenessero dei *biases* intrinseci o indotti. Anche i giudici di appello assumono dunque un atteggiamento oculato circa il funzionamento tecnico dell'algoritmo, che li porta, tuttavia, a conclusioni opposte rispetto ai colleghi di primo grado. È interessante osservare che la Corte d'Appello dà un peso minore, rispetto a quella di prima istanza, al fatto che la pratica non abbia restituito falsi positivi. Infatti, sembra voler intendere che il rischio, pur astratto, di *biases* e discriminazioni abbia un peso maggiore rispetto ad una buona resa concreta[20].

Una quarta postura giurisprudenziale è quella che sembra aderire all'idea di una "interpretazione tecnologicamente orientata" che si possa dire allo stesso tempo evolutiva e garantistica dei diritti, nonostante queste sentenze non facciano esplicita menzione del c.d. argomento tecnologico (come invece

anche sul più ampio valore della dignità umana. Tuttavia, afferma che, alla luce della gravità dei crimini perseguiti – quelli, per l'appunto, di matrice terroristica – il rischio implicato dallo strumento tecnologico risultasse controbilanciato. Sul tema, R.A. MILLER, *Balancing Security and Liberty in Germany*, in 4 *Journal of National Security Law and Policy*, 2010, 369 ss.

[19] *R (on the application of Edward Bridge) v the Chief Constable of South Wales and others* [2020] EWCA Civ 1058. B. KEENAN, *Automatic Facial Recognition and the Intensification of Police Surveillance*, in 84 *Modern Law Review*, 4, 2021, 886, ss.

[20] V., per un simile *trend*, la decisione con cui la Corte costituzionale tedesca ha dichiarato l'illegittimità costituzionale parziale del programma di *data mining*, posto in essere dalle autorità tedesche a fini di antiterrorismo. Qui, la Corte si è addentrata in un'analisi approfondita dell'utilizzo del c.d. *big data*, rimarcando che, all'aumentare della quantità dei dati, aumenta l'impatto sui diritti fondamentali. 1 BvR 3214/15, 11 December 2020.

faranno altre corti, v. *infra*). Una lettura di questo tipo si può riscontrare nella sentenza con cui, nell'aprile 2021, il Consiglio di Stato francese si è pronunciato su alcune disposizioni interne in materia di *data retention*[21]. Si tratta di una decisione per certi versi "gemella", quanto al tema e al contesto di riferimento, di quella belga vista *supra*. Infatti, il Consiglio di Stato francese aveva precedentemente presentato alla CGUE una domanda di pronuncia pregiudiziale che coinvolgeva la normativa interna sulla *data retention* a fini di antiterrorismo e la relativa causa era stata riunita dalla Corte di Lussemburgo con quella afferente alla normativa belga, dando luogo ad una pronuncia unica – per l'appunto, la decisione *La Quadrature du Net* – nell'ottobre 2020[22]. Per quanto attiene all'aspetto squisitamente tecnologico dei sistemi di *data retention* utilizzati, il supremo consesso giurisdizionale amministrativo francese si interrogava circa la compatibilità con il quadro euro-unitario di una normativa interna che prevedesse il trattamento e l'analisi dei metadati conservati con modalità automatizzate. Come nel caso belga, dopo aver ricevuto riscontro dalla CGUE, il Consiglio di Stato francese ha dovuto pronunciarsi per chiudere il caso a livello nazionale. A tale proposito, i giudici amministrativi di Palais-Royal hanno dimostrato una lodevole capacità di leggere le garanzie dei diritti interne in considerazione della tecnologia. Da un lato, la CGUE aveva ritenuto che l'utilizzo di tecniche di analisi automatizzate dei dati fossero incompatibili con il *corpus* di diritto dell'Unione in materia di protezione dei dati, nonché che esse potessero avere un effetto deterrente sulla libertà di espressione. Dall'altro lato, però, il Consiglio di Stato non ha accettato in maniera acritica la posizione della CGUE e, pur nel rispetto di essa, ne ha dato un'applicazione ragionata. Il supremo giudice amministrativo ha affermato che è opportuno distinguere tra diversi ambiti di applicazione della stessa tecnologia: i c.d. crimini ordinari gravi; i crimini ordinari non qualificabili come gravi; il terrorismo (*rectius*, l'ambito della sicurezza nazionale). Solo nell'ultimo caso, il Consiglio di Stato ha intravisto una possibilità di utilizzo di questo *tool* tecnologico, mentre negli altri due casi ha giudicato opportuno che le autorità si astengano e ricorrano a mezzi di sorveglianza meno intrusivi. In questo modo, la *stessa* tecnologia viene sottoposta a diversi *standard* di giudizio a seconda del grado di rischio per l'altro termine del bilanciamento, ossia la sicurezza. In tal modo, la tecnologia entra a pieno titolo nel bilanciamento, come se fosse un

[21] Consiglio di Stato francese, N° 393099, 21 aprile 2021. A. VEDASCHI, *"Customizing" La Quadrature du Net: The French Council of State, National Security and Data Retention*, in *BRIDGE Blog*, disponibile all'indirizzo https://bridgenetwork.eu/2021/05/05/customizing-la-quadrature-du-net-the-french-council-of-state-national-security-and-data-retention/, 5 maggio 2021; V. J. ZILLER, *Le Conseil d'Etat se refuse d'emboiter le pas au joueur de flûte de Karlsruhe*, in *Blogdroiteuropéen*, disponibile all'indirizzo https://blogdroiteuropeen.com/2021/04/23/le-conseil-detat-se-refuse-demboiter-le-pas-au-joueur-de-flute-de-karlsruhe-par-jacques-ziller/, 23 aprile 2021.

[22] V. *supra*, nota 13.

fattore di carattere giuridico e non meramente tecnico. Così facendo, il Consiglio di Stato francese ha dimostrato una sensibilità attenta a parametrare l'intrusività dell'elemento tecnologico al pericolo per l'elemento giuridico, asservendo il primo al secondo, e non viceversa[23].

Questi quattro *trends* identificati mostrano che l'assunto per cui la tutela della *privacy* risulta sempre preponderante nel contesto europeo non pare più essere così assoluto[24]. Si è visto come la tecnologia stia guidando molte corti verso nuove tecniche di bilanciamento che sembrano stare cambiando la nozione stessa di *privacy*. In parole più chiare, se prima la si poteva considerare a pieno titolo un diritto soggettivo, ora essa sta mutando in qualcosa di molto simile ad un interesse legittimo. In altre parole, si dà per scontato che esistano delle interferenze, nell'era della tecnologia e delle minacce alla sicurezza, rispetto alle quali l'individuo è in una posizione di soggezione e può solo legittimamente aspettarsi che le intrusioni dell'autorità pubblica avvengano secondo procedure corrette e senza violare il principio di proporzionalità.

2.2 Il contesto statunitense: la Corte Suprema degli Stati Uniti

Esaminato il quadro europeo, conviene focalizzare l'attenzione sul versante statunitense. Qui, è noto come la c.d. *third party doctrine* caratterizzi tradizionalmente la giurisprudenza che riguarda (non solo ma anche) le misure di sorveglianza di massa in ottica di tutela della sicurezza nazionale. Senza ripercorrere l'intera casistica, basti ricordare come, per molti anni, la Corte Suprema abbia ritenuto "affievolite" le garanzie del IV Emendamento nel caso in cui un soggetto volontariamente ceda dei dati ad una terza parte[25]. Con un approccio totalmente differente da quello europeo, basato sul principio della *purpose limitation*[26], i giudici statunitensi hanno argomentato come la cessione di dati da

[23] V. pure l'approccio che il Consiglio di Stato francese ha utilizzato, sebbene in un contesto emergenziale parzialmente diverso – ossia quello della crisi sanitaria da Covid-19 –, in tema di impiego di droni per verificare che la popolazione si conformasse ai divieti di circolazione imposti dalle autorità. V. Consiglio di Stato francese, N°s 440442, 440445, 18 maggio 2021.

[24] C. GRAZIANI, *Privacy vs. sicurezza tra Stati Uniti ed Europa nell'era del terrorismo internazionale: un esempio di «circolazione inversa» di modelli?*, in *Rass. dir. pubbl. eur.*, 2, 2019, 365 ss.

[25] V. *Katz v. United States*, 389 U.S. 347 (1967); *United States v. Miller*, 425 U.S. 435 (1976); *Smith v. Maryland*, 442 U.S. 735 (1979). V., sulla *third party doctrine* e sulle sue applicazioni successive agli anni '70, L.P. VANONI, *Il Quarto emendamento della Costituzione americana tra terrorismo internazionale e* datagate*: Security v. Privacy*, in *Federalismi.it*, 1, 2015.

[26] Come noto, il principio di *purpose limitation* indica che, quando dei dati personali vengono trattati, il soggetto a cui essi pertengono (*data subject*) ha il diritto che lo scopo del trattamento sia esplicitamente chiarito. Di conseguenza, tali dati non possono essere trattati per scopi ulteriori rispetto a quelli prestabiliti. A livello di Unione europea, il principio di *purpose limitation* è specificato dall'art. 5(1)(b) del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (c.d. General Data Protection Regulation – GDPR). Sul GDPR, in particolare con riferimento ai suoi profili in relazione

parte di un soggetto (il c.d. *data subject*) a terzi di varia natura (banche, compagnie telefoniche, *Internet service providers*, ecc.) faccia sì che il primo non debba più nutrire alcuna «reasonable expectation» di riservatezza, pure nel caso tali terzi diffondano quei dati per finalità diverse rispetto a quelle per cui li avevano originariamente raccolti. Se si cala questo principio nello scenario della sorveglianza posta in essere dal potere federale a scopi di tutela della sicurezza, si ha che il soggetto il quale volontariamente e consapevolmente rende i propri dati disponibili ad un terzo (ad esempio un *provider* di servizi Internet) deve aspettarsi l'accesso, da parte delle autorità pubbliche, a tali informazioni. Pertanto, tale sorveglianza può essere attuata senza che l'autorità – solitamente la polizia o i servizi di *intelligence* – debba ottenere alcun *warrant* da un giudice (come invece richiederebbe il IV Emendamento).

A ciò si aggiunge un'altra specifica *doctrine* diffusa tra le corti statunitensi: si tratta della c.d. *special needs doctrine*. In base ad essa, quando vi sono specifiche necessità di carattere urgente (come un pericolo per la sicurezza nazionale) e sarebbe impossibile, per ragioni di tempo o di praticabilità, ottenere un *warrant* di una corte, si può procedere ugualmente.

Con la diffusione delle più avanzate tecniche di sorveglianza, il quadro giurisprudenziale delineato è rimasto praticamente inalterato[27], perlomeno fino al 2018, quando si è notato un cambio di rotta da parte della Corte Suprema, nel noto caso *Carpenter v. United States*[28]. Nella decisione *Carpenter*, per la prima volta, la Corte ha effettivamente fatto utilizzo di quello che può essere chiamato l'"argomento tecnologico" per dare una nuova interpretazione del IV Emendamento, nonché della ormai consolidata *third party doctrine*.

Il caso riguardava la costituzionalità o meno della normativa federale, rappresentata dallo Stored Communications Act[29], che obbligava i *providers* a fornire, su richiesta, i metadati relativi alle comunicazioni degli utenti ad un'autorità governativa, qualora questa fosse impegnata in un'attività di prevenzione e repressione del crimine. La richiesta governativa non necessitava di essere supportata da alcun *warrant* di un organo giurisdizionale. Nel caso di specie, si trattava della richiesta di dati di geolocalizzazione del cellulare di alcune persone ricercate – per reati che, lo si ricorda, non avevano direttamente a che fare con la sicurezza nazionale, ma potevano configurarsi come crimini ordinari. Si trattava indubbiamente di una nuova categoria di dati, poiché, fino a pochi

all'intelligenza artificiale, G. MOBILIO, *L'intelligenza artificiale e le regole giuridiche alla prova: il caso paradigmatico del GDPR*, in *Federalismi.it*, 27 maggio 2020.

[27] V., ad esempio, nelle decisioni *Kyllo v. United States*, 533 U.S. 27 (2001); *United States v. Jones*, 132 S. Ct. 945 (2012).

[28] *Carpenter v. United States*, 585 U.S. ____ (2018). V., in dottrina italiana, a commento di questo caso, V. FANCHIOTTI, *"Carpenter v. U.S.": si amplia la tutela contro la "global police surveillance"*, in *Giur. it.*, 10, 2018, 2262 ss.

[29] Pub. L. 99–508.

anni prima, i cellulari non includevano sistemi GPS capaci di tracciamento continuativo e preciso. Inoltre, il potenziale incrocio dei dati di geolocalizzazione può condurre alla rivelazione di informazioni ulteriori rispetto al posizionamento geografico. Si possono rilevare, tra l'altro, le persone incontrate, la tempistica di permanenza in un determinato luogo, il mezzo utilizzato per raggiungerlo; incrociando la geolocalizzazione con i dati bancari è poi possibile conoscere dati di rilievo circa operazioni commerciali o finanziarie.

Secondo gli organi giurisdizionali che, prima della Corte Suprema, si erano pronunciati sul caso, esso rientrava nell'ambito di applicazione della *third party doctrine*: qualunque individuo che sottoscrive un contratto con un operatore di telecomunicazione rinuncia volontariamente e consapevolmente alla propria aspettativa di *privacy*[30]. Ciononostante, la maggioranza della Corte Suprema (costituita da soli cinque giudici, ossia il Chief Justice Roberts, redattore, e i giudici Breyer, Ginsburg, Kagan e Sotomayor) ha adottato una differente lettura. Ciò che Roberts ha chiarito in prima battuta è che la *third party doctrine*, è stata elaborata in un periodo storico – tra la fine degli anni '60 e l'inizio degli anni '70 – assai differente, si potrebbe dire incomparabile, rispetto a quello attuale. In quegli anni, lo sviluppo della tecnologia era decisamente inferiore. Di conseguenza, le informazioni cedute (e cedibili) erano assai diverse e avevano una portata meno invasiva rispetto a quelle attuali. Grazie alle potenzialità di *crossing* prima evidenziate, nonché alla rapidità dell'opera di analisi resa possibile da *devices* automatizzati o semi-automatici e alla capacità di raccogliere enormi quantità di informazioni in pochissimo tempo (c.d. *big data*), la sorveglianza sui dati in questione può facilmente diventare massiva e generalizzata, coinvolgendo di fatto un numero di soggetti assai più alto rispetto agli individui ricercati. Perciò, secondo la Corte, queste evoluzioni tecnologiche devono indurre i giudici a mettere da parte «a mechanical interpretation»[31] del IV Emendamento, basata sull'applicazione pedissequa e acritica di *doctrines* risalenti nel tempo, che lascerebbero i cittadini «at the mercy of advancing technology»[32]. Al contrario, bisogna fare perno su interpretazioni più flessibili che tengano conto delle situazioni contingenti derivanti dallo sviluppo della tecnologia. Quindi, se negli anni '70 era possibile ritenere che non fosse necessario un *warrant* perché il Governo chiedesse alle banche di cedere limitate e controllabili informazioni relative alle operazioni di una persona fisica o giuridica, la stessa tesi non è sostenibile con riferimento alle informazioni di localizzazione che, nel 2018, un telefono cellulare è in grado di registrare e che sono conservate

[30] United States District Court for the Eastern District of Michigan, *United States v. Carpenter*, No. 12-20218 (2013); United States Court of Appeals for the Sixth Circuit, *United States v. Carpenter*, 819 F.3d 880 (2016).

[31] *Carpenter v. United States*, cit., II.

[32] *Ibid.*

dai *service providers*. L'accesso a questi dati da parte della autorità pubbliche integra, per la Corte, una vera e propria operazione di *search* ai sensi del IV Emendamento e richiede, per poter essere attuata, un *warrant* preventivamente emesso da un organo giurisdizionale.

Carpenter può essere considerata la dimostrazione che la classica posizione "tiepida" del sistema statunitense rispetto alla tutela della *privacy* non va più vista alla stregua di un dogma infallibile, giacché, grazie alla considerazione calibrata del funzionamento dei *tools* tecnologici, la Corte Suprema è stata in grado di distaccarsi da tale assunto.

La sentenza *Carpenter* è nondimeno assai controversa negli Stati Uniti. Ciò si nota, *in primis*, dal fatto che la maggioranza che è giunta ad adottarla, seppur compatta (non ci sono *concurring opinions* che arrivino allo stesso dispositivo con motivazioni diverse[33]), è risicata, con solo cinque giudici su nove. Alcuni dei quattro giudici dissenzienti (Alito, Gorsuch, Kennedy e Thomas) hanno, con varie argomentazioni, ritenuto applicabile la *third party doctrine* relegando lo sviluppo tecnologico ad un ruolo più marginale rispetto a quanto fatto dalla maggioranza[34]. Inoltre, sebbene la presa di posizione della maggioranza sia lodevole, a giudizio di chi scrive, preme notare che i giudici non hanno chiarito in maniera esplicita la futura applicazione della *Carpenter doctrine* (se in questi termini se ne può parlare)[35]. In altre parole, cosa ne è della sorveglianza, con gli stessi strumenti tecnologici, attuata non in relazione a reati c.d. ordinari, ma a crimini di stampo terroristico o altri gravi reati che abbiano portata transnazionale? In mancanza di indicazioni da parte della Corte Suprema, si potrebbe argomentare in due sensi opposti. Affermare che, essendo coinvolta *la stessa* tecnologia, il *reasoning* di *Carpenter* (applicazione piena delle garanzie del IV Emendamento) può essere replicato inalterato; oppure ritenere che, essendo le minacce alla sicurezza caratterizzate da un maggiore grado di gravità rispetto al crimine ordinario – i ricorrenti del caso *Carpenter* erano ricercati per mero

[33] Ma v. le peculiarità del *dissent* di Gorsuch, *infra*, nota 34.

[34] Secondo l'opinione dissenziente di *Justice* Kennedy, si tratta di dati che, pur se utilizzati a fini di prevenzione del crimine, vengono ceduti nell'ambito di operazioni commerciali e, quindi, non vi sarebbe ragione di ritenerli al di fuori dell'ambito di applicazione della *third party doctrine*. Per *Justice* Thomas, poi, bisogna ritenere che il diritto alla *privacy* possa essere negato a condizione che, *a priori*, l'autorità pubblica renda chiaro che esso non venga applicato al caso di specie. Ancora, secondo *Justice* Alito, si può parlare di *search* solo nel momento in cui vi sia un'interferenza della parte pubblica in una *proprietà* privata del cittadino; e, per Alito, i dati non rientrano nel concetto di proprietà. Da ultimo, *Justice* Gorsuch adotta un'opinione che, pur essendo formalmente dissenziente, somiglia maggiormente ad un'opinione concorrente, poiché concorda con la maggioranza, ma utilizza argomenti diversi. Gorsuch ritiene che i dati di geolocalizzazione debba essere considerati come proprietà di una persona e, perciò, non possono essere sottoposti ad una *search* in mancanza di un *warrant*.

[35] V., sul tema, M. TOKSON, *The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018-2021*, forthcoming in *Harvard Law Review*, disponibile in SSRN all'indirizzo https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3932015.

furto – l'interesse della sicurezza deve fare premio sulla "interpretazione tecnologicamente orientata" (e, di conseguenza, sui diritti individuali).

La comparazione tra gli approdi della giurisprudenza statunitense e quelli della giurisprudenza – nazionale – di area europea mostra che la prima è stata in grado, più della seconda, di usare il fattore tecnologico per distanziarsi da approcci di tipo tradizionale assai consolidati, e di esplicitarlo in modo chiaro. C'è da augurarsi che lo stesso *trend* prosegua e che sia in grado di resistere ai cambi di equilibrio all'interno della Corte Suprema degli Stati Uniti.

3. Corti, interpretazione e tecnologia: uno sguardo "verticale"

Dopo aver analizzato il tema oggetto di indagine secondo le prospettive nazionali di due "mondi", rispettivamente quello europeo e quello statunitense, è utile spostarsi sul piano sovranazionale. Ciò consente di vedere se (ed eventualmente come) i *trend* precedentemente osservati siano stati influenzati da pronunce di corti sovra-statali. Come già rilevato in Introduzione, questo tipo di indagine, e quindi di comparazione, può essere svolta solo per quanto riguarda l'area europea, visto che non esistono sistemi sovranazionali di cui gli Stati Uniti fanno parte (*rectius*, essi aderiscono alla Organization of American States, ma non hanno mai ratificato la Convenzione interamericana dei diritti umani né accettato la giurisdizione della Corte interamericana dei diritti dell'uomo).

Focalizzandosi solo sull'area europea, conviene prendere in esame prima la giurisprudenza della Corte europea dei diritti dell'uomo (Corte EDU) e poi quella della CGUE. Tale ordine di analisi dipende dal fatto che la Corte EDU può fare conto su un sostrato giurisprudenziale più ampio, dato essa opera a pieno titolo come "corte dei diritti" da tempo maggiore rispetto alla CGUE, influenzando, in alcuni casi, le posizioni della CGUE. Inoltre, si deve notare che il sistema del Consiglio d'Europa è rimasto l'unico, tra i due analizzati, ad inglobare ancora il Regno Unito, dato il suo recente recesso dall'esperienza dell'Unione europea[36].

Naturalmente, è opportuno tenere in considerazione il diverso impatto delle decisioni delle due corti, che dipende dalle loro diverse competenze, in ultima analisi rapportabili alla ben nota differente natura dell'Unione europea rispetto al Consiglio d'Europa. Se le decisioni della Corte EDU possono

[36] Si deve però rilevare che, nel corso delle negoziazioni in vista della *Brexit*, il Regno Unito aveva più volte paventato la possibilità di recedere dalla Convenzione europea dei diritti dell'uomo. Tuttavia, il Trade and Cooperation Agreement fra il Regno Unito e l'Unione europea, adottato il 24 dicembre 2020, impegna il Regno Unito a continuare a rispettare la CEDU (v. Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part, art. 524). Sul punto, F. COWELL, *The Brexit deal locks the UK into continued Strasbourg Human Rights court membership*, in *LSE Blog*, disponibile all'indirizzo https://blogs.lse.ac.uk/brexit/2021/01/17/the-brexit-deal-locks-the-uk-into-continued-strasbourg-human-rights-court-membership/, 17 gennaio 2021.

portare solo ad una condanna in termini pecuniari dello Stato, la CGUE possiede un più ampio ventaglio di competenze che le permette di relazionarsi a vario titolo con gli Stati membri. Nonostante ciò, entrambe le corti hanno inciso in modo significativo, stabilendo, in modo più o meno diretto, forme di dialogo con i giudici nazionali.

3.1 La Corte europea dei diritti dell'uomo

La Corte EDU ha iniziato ad occuparsi di sorveglianza attuata a scopi di prevenzione del crimine – anche terroristico – almeno dagli anni '70, con la sentenza *Klass and others v. Germany* del 1978[37]. In questa pronuncia, la Corte ha affermato che le minacce alla sicurezza nazionale legittimano le interferenze delle autorità nelle comunicazioni individuali. Si trattava però, nel caso di specie, di intercettazioni telefoniche totalmente individualizzate, ossia attuabili solo nei confronti delle persone nei cui confronti esistessero gravi sospetti di legami con organizzazioni terroristiche. Nel prosieguo degli anni, anche *post*-9/11, la Corte ha continuato ad adottare atteggiamenti piuttosto bilanciati e riflessivi, andando caso per caso a calibrare il grado di intrusività della misura e di generalizzazione della sorveglianza[38].

Una maggiore attenzione per lo sviluppo tecnologico (o perlomeno tecnico-scientifico) si ha con il caso *S. and Marper v. the United Kingdom*[39], del 2008, quando la Corte EDU si è trovata a valutare se la conservazione di dati biometrici (nello specifico, le impronte digitali) e genetici (le tracce di DNA) in *databases* volti a schedare sospetti criminali – non necessariamente terroristi – violi o meno l'art. 8 CEDU. Qui la Corte EDU ha adottato un approccio ermeneutico in un certo senso precursore di quello della Corte Suprema statunitense in *Carpenter*. Infatti, nella costruzione del proprio *reasoning*, i giudici di Strasburgo chiariscono esplicitamente come la modernizzazione della tecnologia debba portare il collegio giudicante a ripensare gli approdi giurisprudenziali fino a quel momento consolidati. Uno Stato – come nel caso in questione il Regno Unito – che gioca un ruolo pioneristico nello sviluppo di una nuova tecnologia e nell'applicazione della stessa a settori delicati come quello della lotta al crimine deve parimenti assumersi «a special responsibility»[40] nella ricerca di inedite forme di bilanciamento con quei diritti che il mezzo tecnologico può intaccare. Si nota, quindi, l'utilizzo di quello che può essere indicato

[37] Corte europea dei diritti dell'uomo (Plenaria), *Klass e altri c. Germania*, n. 5029/71, 6 settembre 1978.

[38] V., ad esempio, Corte europea dei diritti dell'uomo (Terza Sezione), *Weber e Saravia c. Germania*, n. 54934/00; Id., (Quarta Sezione), *Liberty e altri c. Regno Unito*, n. 58243/00, 1° luglio 2008.

[39] Id. (Grande Camera), *S. e Marper c. Regno Unito*, nn. 30562/04 e 30566/04, 4 dicembre 2008.

[40] Ibid., § 112.

come "argomento tecnologico" per richiamare il Legislatore ad una speciale attenzione nella predisposizione di nuove misure.

Nel 2016, in *Szabó and Vissy v. Hungary*[41], la Corte EDU pare mitigare questa posizione. Mentre in *S. and Marper* aveva sottolineato con forza come la tecnologia avanzata dovrebbe implicare un'attenzione particolarmente alta per i diritti, invitando il giudice ad uno scrutinio assai rigoroso, in questa decisione del 2016 essa ha ammesso come l'utilizzo, su ampia scala, di tecnologie definite «cutting-edge» per prevenire i reati di stampo terroristico sia ormai inevitabile. Tuttavia, non ha rinunciato totalmente alle sue precedenti posizioni, specificando che è sempre necessaria la verifica casistica su come il singolo sistema tecnologico interagisce con le garanzie dei diritti. E, nel caso di specie, il bilanciamento attuato dal Legislatore ungherese appariva inappropriato, facendo sì che le misure violino l'art. 8 CEDU, poiché l'uso di *databases* di conservazione dei metadati di comunicazione, peraltro, facenti ricorso all'automazione, non si limitava a soggetti sospettati di legami con il terrorismo, ma coinvolgeva la generalità dei cittadini ungheresi.

Di interesse per l'indagine che si sta conducendo è poi la decisione *Privacy International v. the United Kingdom*[42], del 2020, in materia di poteri di intercettazione dei servizi segreti britannici. In essa, sebbene la Corte EDU abbia concluso per un'inammissibilità per motivi procedurali, non ha mancato di rilevare, in un *obiter dictum*, che più la tecnologia utilizzata diventa sofisticata, più vi è il rischio che essa venga strumentalmente utilizzata dai governi per rendere poco trasparente il proprio operato, sottraendosi al principio di *accountability*.

Questa rapida rassegna mostra come la Corte EDU abbia più volte fatto ricorso all'argomento c.d. tecnologico per giustificare una forma di scrutinio rigorosa, a cui non ha totalmente rinunciato neanche nel momento in cui, con l'acuirsi della minaccia terroristica, si è dovuto prendere atto che i mezzi, anche massivi, di sorveglianza, rappresentano l'unica reazione non utopistica ad un pericolo pervasivo e imprevedibile.

3.2 La Corte di giustizia dell'Unione europea

Il raffronto della giurisprudenza della Corte EDU con quella della CGUE in materia di tecnologia e diritti sotto il profilo della sicurezza pubblica mostra che la Corte di Lussemburgo ha iniziato ad occuparsi del tema molto più tardi rispetto alla Corte di Strasburgo. Ciò risulta indubbiamente legato al peculiare

[41] Corte europea dei diritti dell'uomo (Quarta Sezione), *Szabó e Vissy c. Ungheria*, n. 37138/14, 12 gennaio 2016.

[42] Corte europea dei diritti dell'uomo (Prima Sezione), *Privacy International c. Regno Unito*, n. 46259/16, 7 luglio 2020.

percorso dell'Unione europea con riferimento alla tutela dei diritti, che la ha portata a superare l'iniziale vocazione meramente mercantilistica in tempi relativamente recenti[43]. Se già nel 1978 la Corte EDU, con la sentenza *Klass*, si occupava di misure di sorveglianza – sia pure ad uno stadio albare della tecnologia utilizzata –, la CGUE inizierà a prendere in considerazione il tema negli anni 2000, in particolare nel 2006 con la sentenza *European Parliament v. Council*[44]. Con questa pronuncia, la CGUE ha dovuto esaminare il primo accordo con cui l'Unione europea e gli Stati Uniti disciplinavano lo scambio di dati PNR (Passenger Name Record) dei passeggeri dei voli aerei al fine di sottoporli ad analisi per prevenire eventuali minacce alla sicurezza. Non si tratta, invero, di una sentenza in cui si è particolarmente riflettuto sulla strumentazione tecnologica utilizzata dai sistemi di raccolta e analisi; tuttavia, essa è significativa perché la Corte ha affermato che il *PNR exchange* comporta un non trascurabile impatto sui diritti della persona e, perciò, qualsiasi normativa sul tema deve avere un'appropriata base giuridica che non riguardi solo l'aspetto del mercato interno, ma pure quello della cooperazione in materia di polizia.

La prima decisione in cui la CGUE prende in esame precipuo il funzionamento della tecnologia in ottica di sorveglianza è la notissima *Digital Rights*, del 2014[45]. Nell'enucleare i profili di invalidità della direttiva c.d. *data retention*[46], la Corte di Lussemburgo nota come molti di essi derivino dal fatto che i *tools* tecnologici usati dai *providers* per raccogliere e conservare i metadati ne permettano l'incrocio, cosa che conduce, in ultima analisi, alla possibilità di profilare gli individui. Pur senza esplicitarlo con riferimenti diretti, la CGUE fa notare come gli aspetti più preoccupanti dell'operatività della direttiva conseguano esattamente al *modus operandi* della tecnologia, che, fino a pochi anni

[43] Sul cammino della Comunità (poi Unione) europea verso la caratterizzazione come organismo non solo mercantilistico, ma anche di tutela dei diritti umani, v. V. CASAMASSIMA, *I diritti fondamentali europei tra processi di positivizzazione normativa e ruolo dei giudici (e della politica). Riflessioni intorno ad alcuni recenti sviluppi in materia di rapporti tra Corte costituzionale, Corte di giustizia e giudici comuni*, in *Rivista AIC*, 3, 2019, 404 ss., spec. 411 ss.

[44] Corte di giustizia dell'Unione europea, *Parlamento europeo c. Consiglio dell'Unione europea e Commissione*, C-317/04 e C-318/04, 30 maggio 2006. V. M. MENDEZ, *Passenger Name Record Agreement. European Court of Justice. Annulment of Commission Adequacy Decision and Council Decision Concerning Conclusion of Passenger Name Record Agreement with US Grand Chamber Judgment of 30 May 2006, Joined cases C-317/04 and C-318/04, European Parliament v. Council and Commission*, in 3 *European Constitutional Law Review*, 2007, 127 ss.

[45] Corte di giustizia dell'Unione europea (Grande Camera), *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e altri*, C- 293/12 e C-594/12, 8 aprile 2014. A. VEDASCHI, V. LUBELLO, *Data Retention and its Implications for the Fundamental Right to Privacy*, in 20 *Tilburg Law Review*, 2015, 14 ss.

[46] Direttiva 2006/24/CE del Parlamento europeo e del Consiglio del 15 marzo 2006 riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE.

prima, non sarebbe stata così performante da assicurare incroci quasi istantanei di un'enorme quantità di dati.

A mero titolo di esempio, gli orientamenti in *Digital Rights* vengono ripresi più volte nella giurisprudenza successiva (ad es. *Schrems I* nel 2015[47], *Tele2 Sverige* nel 2016[48], il Parere 1/15 sulla bozza di accordo tra il Canada e l'Unione europea per lo scambio dei dati PNR del 2017[49]). Tutte queste decisioni tengono sempre in debita considerazione il modo in cui la tecnologia lavora per valutare la proporzionalità delle diverse misure di sorveglianza. Una più esplicita attenzione per il fattore tecnologico si riscontra nel Parere 1/15, in cui la Corte si dilunga a riflettere sui rischi dell'automazione, che l'avanzamento della tecnologia permetteva oramai di utilizzare per conservare e analizzare i dati PNR[50].

Nelle due più recenti decisioni che si occupano di questi temi, ossia *La Quadrature du Net and others*[51] e *Privacy International* (entrambe dell'ottobre 2020)[52], la Corte affronta vari temi legati alla tecnologica: di nuovo l'automazione, il problema dell'anonimizzazione e il fatto che, proprio per garantire così alti *standards* tecnologici per portare avanti le proprie *policies* volte alla protezione della sicurezza, le autorità pubbliche statali debbano necessariamente appoggiarsi a soggetti privati, con tutti i problemi che ne derivano. In queste due decisioni di nuovo l'argomento "tecnologico" è silente, ma esistente. La CGUE non lo ha richiamato esplicitamente – come hanno fatto invece la Corte Suprema degli Stati Uniti e la Corte EDU in alcune decisioni – ma si nota uno scrutinio più intenso nei passaggi in cui il ruolo del fattore tecnologico è maggiormente evidente.

Questo *corpus* giurisprudenziale della CGUE ha senza dubbio un'importanza cruciale nel costruire un sistema europeo di tutela dei diritti pur nel momento in cui i pericoli per la sicurezza spingono i Legislatori ad adottare

[47] Corte di giustizia dell'Unione europea (Grande Camera), *Maximillian Schrems c. Data Protection Commissioner*, C-362/14, 6 ottobre 2015. V. ZENO-ZENCOVICH, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Roma Tre Press, Roma, 7 ss.

[48] Corte di giustizia dell'Unione europea (Grande Camera), *Data Protection Commissioner c. Facebook Ireland Limited e Maximillian Schrems*, C-311/18, 16 luglio 2020. C. GENTILE, *La saga "Schrems" e la tutela dei diritti fondamentali*, in *Federalismi.it*, 1, 35 ss.

[49] Corte di giustizia dell'Unione europea (Grande Camera), Parere 1/15, 26 luglio 2017. A. VEDASCHI, *Privacy and data protection versus national security in transnational flights: the EU–Canada PNR agreement*, in 8 *International Data Privacy Law*, 2018, 124 ss.

[50] E. MENDOS KUŞKONMAZ, *Privacy and Border Controls in the Fight against Terrorism. A Fundamental Rights Analysis of Passenger Data Sharing*, Brill, Leiden-Boston, 2021.

[51] Cit., *supra*, nota 13.

[52] Corte di giustizia dell'Unione europea (Grande Camera), *Privacy International c. Secretary of State for Foreign and Commonwealth Affairs e altri*, cit.

normative assai intrusive con riguardo alla *privacy* e alla protezione dei dati personali. Le corti interne hanno reagito a questa giurisprudenza in maniera varia, anche con riferimento alla considerazione dell'elemento tecnologico. È emblematica, a tal proposito, la differente reazione della Corte costituzionale belga e del Consiglio di Stato francese alla sentenza *La Quadrature du Net*: la prima ha implementato la decisione sovranazionale con un'incostituzionalità secca della normativa interna, mentre il secondo ha "ritagliato" quanto espresso dalla Corte di Lussemburgo rispetto all'ordinamento francese[53]. Forse – ma si tratta solo di una supposizione – nel caso in cui la CGUE avesse dettagliato in maniera più esplicita l'argomento "tecnologico", chiarendo quali *caveat* aggiuntivi esso debba comportare, si sarebbe avuto un recepimento più uniforme della sua decisione negli ordinamenti interni dei giudici del rinvio[54].

4. Alcune riflessioni conclusive

Lo scenario che questo lavoro ha delineato mostra almeno due contesti in cui si è fatto un ricorso esplicito e chiaro all'argomento c.d. tecnologico. Si tratta della sentenza *Carpenter* della Corte Suprema degli Stati Uniti e di alcune delle citate sentenze in materia di sorveglianza e sicurezza pubblica della Corte EDU. In questi casi, le corti in questione non solo hanno riservato agli strumenti che si potrebbero definire "a tecnologia avanzata" uno scrutinio particolarmente penetrante, ma hanno anche esplicitato l'uso di questa argomentazione, chiarendo che l'impiego di tecnologie avanzate chiama il giudice al dovere di ripensare approdi giurisprudenziali particolarmente consolidati[55].

La CGUE così come molte corti nazionali – in un'ottica di influenza reciproca, e il dialogo non è mancato neppure con le posizioni della Corte EDU – hanno anch'esse spesso mostrato lo stesso atteggiamento nel merito (garanzie rinforzate in caso di ricorso a nuove tecnologie particolarmente intrusive), ma senza affermarlo esplicitamente nella motivazione della sentenza.

Tale diversità di approccio potrebbe apparire poco rilevante: si potrebbe affermare che ciò che davvero conta è il grado di tutela offerto da una corte, più che l'esplicitazione dei propri argomenti. Tale visione, però, è parziale, perché non considera la centralità che, negli ordinamenti improntati alla *rule of law*, la motivazione di una sentenza ha. Infatti, l'esplicazione chiara del *reasoning* serve non solo a rendere la sentenza controllabile da parte tanto di altri

[53] V. *supra*, § 2.1.

[54] Si veda la "reazione" della corte interna britannica, *supra*, nota 14.

[55] Un primo accenno, invero, di ricorso alla c.d. interpretazione tecnologicamente orientata non manca neanche nel panorama giurisprudenziale italiano, con la sentenza n.135/2002 della Corte costituzionale. Con questa decisione, la Consulta richiama i «progressi tecnici successivi», che devono orientare l'interprete della Costituzione, nonostante il Costituente, nella redazione del testo costituzionale, non abbia potuto naturalmente tenerli in considerazione.

eventuali giudici – si pensi ai gradi di appello – quanto della società civile, ma anche a formare una coscienza collettiva su un dato tema.

Se le corti – come la Corte Suprema degli Stati Uniti e la Corte EDU hanno fatto – esplicitassero sempre in maniera cristallina il fatto che l'evoluzione tecnologica deve portare qualsiasi giudice ad un atteggiamento particolarmente elastico nei confronti dei propri precedenti (e nei sistemi di *common law* e in quelli di *civil law*[56]), ciò aiuterebbe sicuramente la società tutta a considerare in maniera più consapevole l'uso della tecnologia, portando i Legislatori ad essere più oculati nella predisposizione della regolamentazione sul tema.

[56] V. A. PIN, *Precedente e mutamento giurisprudenziale. La tradizione angloamericana e il diritto sovranazionale europeo*, Cedam, Padova, 2017.