Freedom, Security & Justice: European Legal Studies

Rivista giuridica di classe A

2023, n. 3

EDITORIALE SCIENTIFICA

Rivista quadrimestrale on line "Freedom, Security & Justice: European Legal Studies"
www.fsjeurostudies.eu
Editoriale Scientifica, Via San Biagio dei Librai, 39 - Napoli
CODICE ISSN 2532-2079 - Registrazione presso il Tribunale di Nocera Inferiore n° 3 del 3 marzo 2017

Indice-Sommario
2023, n. 3

Editoriale

Saggi e Articoli

Commenti e Note

CONSERVAZIONE E PRODUZIONE DELLA PROVA DIGITALE NELLA NUOVA DISCIPLINA EUROPEA: IL POTENZIALE DISALLINEAMENTO CON I PRINCIPI ESPRESSI DALLA GIURISPRUDENZA DI SETTORE

Stefano Busillo*

SOMMARIO: 1. Introduzione: la cooperazione giudiziaria, la prova digitale e le peculiari implicazioni per i diritti fondamentali. – 2. Il quadro giuridico internazionale ed europeo sulla cooperazione digitale in ambito penale: le recenti iniziative dell'UE e del Consiglio d'Europa. – 3. Le implicazioni con riferimento al rispetto dei diritti fondamentali e la giurisprudenza europea in materia. – 3.1. La tutela dei diritti secondo le corti europee: i principi di proporzionalità e di necessità della misura quali garanzia per l'individuo – 4. Dubbi di compatibilità con la prassi giurisprudenziale nel futuro della cooperazione giudiziaria digitale. – 4.1. I rischi legati alla geometria variabile ed alla privatizzazione della giustizia nel Regolamento EPOC. – 4.2. Il Secondo Protocollo alla Convenzione sulla criminalità informatica: uno strumento incoerente e (già) obsoleto? – 5. Osservazioni conclusive.

1. Introduzione: la cooperazione giudiziaria, la prova digitale e le peculiari implicazioni per i diritti fondamentali

La cooperazione giudiziaria viene definita quale il concepimento e l'applicazione di meccanismi cooperativi che possano facilitare la lotta contro la criminalità. E, ad oggi, appare in modo del tutto evidente sottoposta ad un processo di digitalizzazione che permetta di contrastare adeguatamente nuove forme di crimine, qualificabili sia come "*cybercrime*" che come meri illeciti tradizionali adattatisi al mondo digitale.

Non è sbagliato evidenziare come la cooperazione giudiziaria sia, in generale, percepita come un elemento su cui la comunità dei consociati debba fare affidamento per

Articolo sottoposto a doppio referaggio anonimo.

* Dottorando di ricerca, *curriculum* internazionalistico-europeo-comparato, Dipartimento di Scienze Giuridiche dell'Università degli Studi di Salerno. Indirizzo e.mail: sbusillo@unisa.it.

Il presente contributo sviluppa e rielabora i contenuti dell'intervento *"Digitalization Process of Judicial Cooperation in Criminal Matters: What Effects for Rule of Law and Human Rights?*", presso il *Congreso internacional de jóvenes investigadores* "*Los derechos humanos como instrument de interacciòn en el Derecho Internacional Público"*, dell'11 luglio 2022, organizzato telematicamente dalle Università di Alcalá (Spagna), Università militare di Nueva Granada (Colombia), Universidad Nacional di Cuyo (Argentina) ed Università "Rafael Landívar" di Città del Guatemala (Guatemala).

preservarsi e ulteriormente svilupparsi. Tuttavia, è anche vero che non ne risulta rafforzata in modo assoluto. Al contrario, rischi possono concretamente presentarsi per i diritti dell'individuo – che rappresentano, tra l'altro, il c.d. Stato di diritto sostanziale[1], e che sono pericolosamente in gioco in un procedimento penale. Per meglio chiarire la relazione esistente tra diritti fondamentali e cooperazione penale digitale, appare di tutta evidenza che la natura della prova digitale (termine assai ricorrente da più anni a questa parte) ricopra un ruolo determinante.

Una prima osservazione concerne il fatto che non esiste una definizione pacifica e strettamente vincolante del termine "prova digitale", dovendosi sottolineare che essa "*does not necessarily relate to electronic crime, cybercrime or e-crime, however,* [it] *seems self-evident*"[2]. Pertanto, al massimo, la definizione in questione deve essere posta in termini funzionali invece che tassonomici, ovvero sulla base delle sue modalità operative e del suo scopo piuttosto che di una categorizzazione indicata da "legislatori" presenti a più livelli.

Essa si porrebbe quale qualsiasi informazione o dato che possa avere significato per le indagini e, più precisamente, includerebbe quelle informazioni o dati immagazzinati, ricevuti o trasmessi da un dispositivo elettronico. Tale genere di prova viene dunque acquisita quando è disposta confisca di detto dispositivo e la conseguente escussione dei contenuti informatici in esso presenti, come nel caso dei *server* di una società attiva nel settore della tecnologia dell'informazione (IT)[3]. Ciononostante – tra i profili di rischio per i diritti fondamentali correlati all'implementazione di nuovi strumenti di cooperazione penale digitale – sono proprio i metodi di individuazione e conservazione della prova digitale a venire inevitabilmente in considerazione. La ragione di ciò è che, sempre più di sovente, i dati informatici arriveranno a costituire prova che, per sua natura, risulta suscettibile di volatilità e modificabilità. E ciò, naturalmente, senza tener conto della peculiare attenzione richiesta al momento della ricerca, della raccolta, ecc. La prova digitale (o elettronica che si voglia) è poi tipicamente di natura transnazionale, slegata dalla giurisdizione territoriale del luogo di commissione del reato o del luogo in cui le indagini siano state eventualmente avviate.

[1] T.H. BINGHAM, *The Rule of Law*, Londra, 2011, p. 66 ss.
[2] S. DEPAUW, *Electronic Evidence in Criminal Matters: How About E-Evidence Instruments 2.0?*, in *European Criminal Law Review*, 2018, n. 1, pp. 66-67.
[3] Una lista non esaustiva delle tecniche di acquisizione della prova digitale è stata predisposta da C. CESARI, *L'impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite*, in *Revista Brasileira de Direito Processual Penal*, 2019, n. 3, pp. 1167-1188, che in essa ricomprende la perquisizione ed il sequestro di documenti digitali, la raccolta in seno al procedimento di e-mail ed SMS, come pure la assai nota pratica di installazione di *spyware* (*trojan*) sui dispositivi personali dell'indagato.

Pertanto, tre aspetti la delineano in maniera caratteristica: la sua peculiare modalità di localizzazione e conservazione[4]; le fonti private[5] da cui di solito origina (*service providers*, prestatori e gestori di servizi); la connotazione transnazionale del procedimento di acquisizione[6]. Tali caratteristiche postulano la necessità di celeri ed efficaci strumenti di indagine. E, di risposta a tale bisogno cambia il quadro giuridico esistente previsto per la prova digitale. Tale quadro giuridico, tuttavia, si fonda su concetti quali territorialità e sovranità[7] che sono costantemente messi in dubbio dalla natura stessa della prova digitale. La conseguenza di ciò non è necessariamente un blocco dell'attività di persecuzione penale, bensì, all'opposto, talvolta una vera e propria assenza di limitazioni alle attività degli inquirenti.

Pertanto, l'unione delle caratteristiche della prova digitale e degli strumenti di persecuzione determina un rischio più che manifesto: in modo quasi scontato, si osserva che, in assenza di forme di controllo, la gestione della prova digitale ed il trattamento di dati informatici può, in via generalissima, minacciare ed effettivamente porre a rischio i diritti fondamentali, quali il diritto alla vita privata ed il diritto alla protezione dei dati. Il rischio in questione potrebbe addirittura configurarsi come superiore rispetto ai benefici per la comunità che derivino dalla "corretta" attivazione della persecuzione penale. Inoltre, la cooperazione giudiziaria digitale, per via di limiti sfumati da esigenze securitarie, sembra porre a repentaglio i diritti dell'individuo tanto quanto, se non di più, della cooperazione giudiziaria tradizionale.

Partendo da quest'ultima affermazione – la quale rappresenta la premessa iniziale che ha portato a questa breve analisi – l'articolo intende far luce, in primo luogo, sul quadro giuridico della cooperazione giudiziaria penale esistente in ambito digitale, con peculiare

---

[4] F. MOLINA, G.D. RODRIGUEZ, *The Preservation of Digital Evidence and Its Admissibility in the Court*, in *International Journal of Electronic Security and Digital Forensics*, 2017, n. 1, pp. 1-18. Ad esempio, nel caso della Corte europea dei diritti dell'Uomo, Terza Camera, sentenza del 25 giugno 2013, ricorso n. 18540/04, *Valentino Acatrinei c. Romania*, par. 71, la Corte ha reso manifesto che la "contaminazione" di dati informatici potrebbe a volte presentarsi come irreversibile, gettando dubbi sulle modalità di acquisizione della prova talvolta adoperate dagli inquirenti. Ciò comporta la necessità di aversi un'attività tecnica impeccabile in qualsiasi fase di raccolta e trattamento della prova digitale: "*In determining whether the proceedings as a whole were fair* [...] *the quality of the evidence must be taken into consideration, including whether the circumstances in which it was obtained cast doubt on its reliability or accuracy*".

[5] M. SIMONATO, *Defence Rights and the use of Information Technology in Criminal Procedure*, in *Revue Internationale de Droit Pénal*, 2014, n. 1, p. 279. La connotazione privata della fonte "*would obviously lead to justifiable accusations of* de facto *privatisation of certain elements of the criminal justice system*" nel pensiero espresso da M. ROJSZCZAK, E-*Evidence Cooperation in Criminal Matters from an EU Perspective*, in *The Modern Law Review*, 2022, n. 4, pp. 1003-1004.

[6] N. SMUHA, *Towards the EU Harmonization of Access to Cross-Border E-Evidence: Challenges for Fundamental Rights & Consistency*, in *European Criminal Law Review*, 2018, n. 1, p. 84: "*Moreover, the presence of e-evidence typically also creates cross-border scenarios, which directly clash with the – still reigning – principle of territoriality*".

[7] La perdità della territorialità è, in quanto tale, una perdita di sovranità come giustamente considerato da A.M. OSULA, *Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data*, in *Masaryk University Journal of Law and Technology*, vol. 9, n. 1, 2015, p. 45; I. ZERBES, *Legal Issues of Transnational Exchange of Electronic Evidence in Criminal Proceedings*, in *European Criminal Law Review*, 2015, n. 3, p. 306; cfr. A. GOLIA, *La sovranità europea alla prova del digitale. I nodi della data retention alla luce di una decisione del Consiglio di Stato francese*, in *Rassegna di diritto pubblico europeo*, 2021, n. 2, pp. 439-453.

attenzione data all'Unione europea (UE) ed al Consiglio d'Europa (CdE) (Paragrafo 2). In particolar modo, dopo aver considerato i motivi che hanno spinto l'Unione ed il Consiglio d'Europa a superare gli strumenti "classici" di cooperazione digitale, verrà presentata la risposta da parte di queste due organizzazioni internazionali, ovvero il Regolamento (UE) 2023/1543, sull'ordine europeo di produzione e conservazione della prova digitale in ambito penale ed il Secondo Protocollo alla Convenzione sul crimine informatico, aperto alla firma dal 2022. Successivamente, il contributo evidenzierà brevemente quali diritti individuali risultano posti a rischio dal processo di digitalizzazione della cooperazione giudiziale penale. Lo scopo della definizione di tale catalogo è consentire di introdurre efficacemente le soluzioni trovate dal legislatore e dalla giurisprudenza per ovviare a indebite violazioni degli stessi (Paragrafo 3). Ciò avverrà, in particolar modo, attraverso l'analisi della *data retention saga* sulla sorveglianza di massa, identificando dei principi generali (proporzionalità e necessità su tutti) che potranno essere applicati per analogia alle novelle dell'UE e del Consiglio d'Europa. Tuttavia, verrà sottolineato nel contributo che tali principi "portanti" del settore vengano riproposti in modo spurio dal "nuovo" quadro giuridico, nel disprezzo della giurisprudenza delle corti (Paragrafo 4). Infine, delle riflessioni conclusive chiuderanno il lavoro attraverso una sintesi dei principali contenuti evidenziati dall'articolo e delle soluzioni suggerite per far fronte alle problematiche previste (Paragrafo 5).

2. Il quadro giuridico internazionale ed europeo sulla cooperazione digitale in ambito penale: le recenti iniziative dell'UE e del Consiglio d'Europa

Una moltitudine di organizzazioni internazionali (OI) hanno provveduto nel corso del tempo a rispondere alla sfida posta dalla digitalizzazione. Come di seguito chiarito, i risultati delle soluzioni sono stati eterogenei. Tuttavia, in maniera omogena le OI hanno mirato alla creazione di *framework* finalizzati allo sviluppo della cooperazione digitale tra gli Stati e ciò, naturalmente, è accaduto anche con riguardo alla cooperazione giudiziaria penale. Tant'è che, sia a livello regionale che globale, è stato intrapreso un processo evolutivo per l'adozione di meccanismi di prevenzione e repressione cooperativa sempre più sofisticati, rispondendo in modo adeguato alle più recenti fattispecie criminose, progressivamente caratterizzate da una dimensione transnazionale.

In tal senso, sembra opportuno fare menzione delle "tecniche speciali di investigazione" di cui all'art. 20, parr. 2 e 3, della Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale del 2000 (UNTOC, nota anche come Convenzione di Palermo)[8]. Sebbene quelle contenute nell'art. 20 siano misure d'indirizzo politico, esse fungono da base giuridica per espandere ed adattare alla realtà contingente

[8] Risoluzione dell'Assemblea Generale 55/25, *United Nations Convention against Transnational Organized Crime*, del 15 novembre 2000. Esempi di tecniche speciali di investigazione disponibili *ex* art. 20 UNTOC sono il controllo della corrispondenza, l'impiego di forme di sorveglianza elettronica e le operazioni sotto copertura.

il quadro giuridico penale. L'articolo lo fa in modo pratico e assai pragmatico in quanto pone il ricorso alle tecniche speciali come una sorta di "regola contenitore" che vada di volta in volta sostanziata a livello domestico[9]. Tuttavia, le disposizioni citate non sono da considerarsi giuridicamente vincolanti in quanto si limitano ad incentivare[10] gli Stati Parte a "stringere, laddove necessario, gli opportuni accordi o intese bilaterali o multilaterali per l'impiego di dette tecniche speciali di investigazione". E da ciò ne deriverebbe una limitata efficacia del trattato in questo specifico ambito.

Per tal motivo, appare doveroso rammentare il valore delle disposizioni di un altro documento, ovvero della Convenzione sulla criminalità informatica (altrimenti nota come Convenzione di Budapest), adottata dal Consiglio d'Europa nel 2001 – a cui vanno affiancati i propri Protocolli aggiuntivi[11].

Nella Convenzione si provvede ad enunciare dapprima quei principi generali che si applicano alla cooperazione internazionale (Titolo 25) e, come logico sviluppo, le singole condotte da perseguire. Non è un caso che la lotta contro "nuove" forme di criminalità transnazionale richieda, non inaspettatamente, l'identificazione di fattispecie comuni (Artt. 1-2 Convenzione di Budapest) come dei modelli da seguire all'interno degli ordinamenti statali. Vieppiù, sono presenti disposizioni che favoriscono lo sviluppo di strumenti informatici mirati, tra le altre cose, all'acquisto di informazioni e prove digitali in modo da favorire quanto il più possibile la persecuzione penale e l'attività di risposta alle emergenze securitarie da parte degli Stati. In tal senso, il Capo III del trattato ricomprende norme generali e speciali per la cooperazione tra le Parti "nella misura più ampia possibile", non solo guardando al *cybercrime* (ovvero crimini contro e per mezzo di dispositivi computerizzati), ma anche a qualsiasi fatto criminoso che implichi il ricorso alla prova digitale, notando un "*ample use of this practice*" da parte degli Stati[12]. Per questa serie di motivi, la Convenzione di Budapest può dirsi come uno strumento di

[9] L'assenza di riferimenti chiari nella disposizione, suggerendo una certa difficoltà nel monitorare l'effettivo *status* di implementazione dell'art. 20 UNTOC e, soprattutto, della sua adeguatezza, è criticata da parte della dottrina. Cfr. N. BOISTER, *The Cooperation Provisions of the UN Convention against Transnational Organised Crime: A 'Toolbox' Rarely Used?*, in *International Criminal Law Review*, 2016, n. 1, p. 5; Y. DANDURAND, J. JAHN, *The Future of International Cooperation Against Transnational Organized Crime. The Undoing of UNTOC?*, 2021, p. 5.

[10] La Convenzione di Palermo è, indubbiamente, uno strumento di carattere vincolante che ha permesso di superare i limiti di *soft law* di cui è stato fatto ampio utilizzo fino al 2000. Tuttavia, non tutte le disposizioni della Convenzione hanno pari valore e talune ricadono ancora nel c.d. diritto morbido. Da una parte, quelle introdotte dalla formula "ogni Stato adotta", o altro verbo quando richiesto, sono obbligazioni internazionali a tutti gli effetti. Dall'altra, le disposizioni introdotte da "*si incoraggiano gli Stati Parte*" (artt. 18, par. 7 e 20, par. 2, UNTOC) non vincolerebbero gli Stati alla stessa maniera delle precedenti. Disporre di una UNTOC multiforme è un elemento positivo per I. TENNANT, *Fulfilling the Promise of Palermo? A Political History of the UN Convention Against Transnational Organized Crime*, in *Journal of Illicit Economies and Development*, 2021, n. 1, p. 68, il quale definisce la "*flexible, and it invites updates and changes*".

[11] I Protocolli che vanno ad integrare la Convenzione sono: 1) Protocollo addizionale alla Convenzione sulla criminalità informatica, relativo all'incriminazione di atti di natura razzista e xenofobica commessi a mezzo di sistemi informatici (2003) ed il; 2) Secondo protocollo addizionale alla Convenzione sulla criminalità informatica sul rafforzamento della cooperazione e divulgazione delle prove elettroniche (2021), di cui *infra*.

[12] Cybercrime Convention Committee del Consiglio d'Europa, *The Budapest Convention on Cybercrime: benefits and impact in practice*, 13 luglio 2020, T-CY (2020)16, p. 44.

maggior compimento rispetto Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale.

Cionondimeno, il processo legislativo di sistemazione della cooperazione giudiziaria in materia penale nel digitale è tutt'ora in corso, aldilà delle convenzioni internazionali esistenti ed i propri strumenti tradizionali. Ne è un valido esempio l'Unione europea.

Infatti, Eurojust presentava già nel dicembre 2018 una propria iniziativa per la giustizia penale digitale. Scopo dell'iniziativa era la creazione di una piattaforma digitale estesa a tutta l'Unione. In particolare, tale piattaforma avrebbe dovuto consentire – sia alla stessa agenzia UE, sia alla più vasta comunità giudiziaria europea – di relazionarsi *inter se* in modo celere ed efficace, oltre che permettere lo scambio di informazioni e materiale probatorio decisivo per le indagini.

Conseguentemente, nel dicembre 2020, la Commissione ha deciso di avanzare plurime proposte legislative (definito "*toolbox*", pacchetto)[13] sul tema, tra cui l'approvato Regolamento (UE) 2023/2131[14] sullo scambio transfrontaliero di informazioni nei casi di terrorismo ed il Regolamento (UE) 2023/969[15] su una piattaforma di collaborazione per le squadre investigative comuni. Tali atti appaiono incontrovertibilmente preparatori ad un ulteriore salto in avanti a livello tecnologico, ad esempio ottenendo la piena digitalizzazione del *Case Management System* di Eurojust. Altre mirano a disciplinare la raccolta transnazionale della prova digitale nello specifico, che rimaneva un problema endemico nell'Unione, a fronte di un *impasse* legislativo risalante ad almeno due anni prima.

Ed è in tale contesto che si inserisce il Regolamento (UE) 2023/1543 sull'ordine europeo di produzione e conservazione della prova digitale in ambito penale (Regolamento EPOC)[16] – la cui proposta è stata presentata dalla Commissione nel 2018 in risposta ad una richiesta espressa del Consiglio[17] ed inquadrata nel c.d. "*e-Evidence Package*"[18]. Il Regolamento, che si applicherà a decorrere dal 18 agosto 2026, stabilisce

[13] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Digitalizzazione della giustizia nell'Unione europea Un pacchetto di opportunità*, del 2 dicembre 2020, COM/2020/710 final.

[14] Regolamento (UE) 2023/2131 del Parlamento europeo e del Consiglio, *che modifica il regolamento (UE) 2018/1727 del Parlamento europeo e del Consiglio e la decisione 2005/671/GAI del Consiglio, per quanto riguarda lo scambio digitale di informazioni nei casi di terrorismo*, del 4 ottobre 2023, in GUUE Serie L del 11 ottobre 2023.

[15] Regolamento (UE) 2023/969 del Parlamento europeo e del Consiglio del 10 maggio 2023, *che istituisce una piattaforma di collaborazione come ausilio al funzionamento delle squadre investigative comuni e che modifica il regolamento (UE) 2018/1726*, in GUUE L 132 del 17 maggio 2023.

[16] Regolamento (UE) 2023/1543 del Parlamento europeo e del Consiglio, *relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive a seguito di procedimenti penali*, del 12 luglio 2023, in GUUE L 191 del 28 luglio 2023, pp. 118-180.

[17] Consiglio dell'Unione europea, *Conclusions on improving criminal justice in cyberspace*, del 9 giugno 2016, https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf.

[18] Il pacchetto include anche la Direttiva (UE) 2023/1544 del Parlamento europeo e del Consiglio, *recante norme armonizzate sulla designazione di stabilimenti designati e sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove elettroniche nei procedimenti penali*, del 12 luglio 2023, in GUUE L 191 del 28 luglio 2023, pp. 181-190.

le norme in base a cui un'autorità giudiziaria di uno Stato Membro può, nell'ambito di un procedimento penale, emettere un ordine europeo di produzione o un ordine europeo di conservazione. Per mezzo di tale meccanismo, l'autorità potrà pertanto ingiungere ad un *provider* che offra servizi nell'Unione ma che sia stabilito in un altro Stato membro o, alternativamente, rappresentato da un procuratore in un altro Stato membro, di produrre o conservare prove digitali, indipendentemente dall'ubicazione dei dati, tra l'altro in maniera analoga al *Cloud Act* del 2018 oltreoceano[19]. Vincolati al rispetto dei diritti fondamentali quale precondizione per il proprio funzionamento (art. 1, par. 3), tali ordini andrebbero considerati come molto più di una mera innovazione tecnica, volta a venire a capo del problema della "localizzazione" dei dati e quindi della sovranità.

Gli ordini europei di conservazione e produzione (EPOC), che saranno integralmente noti alle sole autorità giudiziarie competenti, verranno presentati in forma di certificato nei confronti di *service providers* privati (destinatari) e consegnati in presenza di procedimenti penali avviati contro persone fisiche o giuridiche, indifferentemente prima o dopo l'esercizio dell'azione penale. Il principale obiettivo dell'ordine emesso è quello di ottenere, per mezzo di una comunicazione elettronica ricevuta dal gestore delle comunicazioni elettroniche, si è detto, una prova digitale, oppure di imporre la conservazione di nomi, domini e numeri IP attivi nell'Unione europea. È fuori dubbio che gli EPOC implichino una straordinaria semplificazione delle procedure esistenti, con una riduzione tangibile dei termini per la consegna della prova richiesta ed una evidente facilitazione nella lotta alla criminalità – offrendo garanzie per la comunità sotto questa prospettiva. Inoltre, pur sovrapponendosi ad esso, gli EPOC non intendono sostituire l'Ordine europeo d'indagine (OEI)[20]. Al contrario, le autorità giudiziarie degli Stati Membri sono legittimate nella scelta dello strumento considerato più adatto al caso di specie. Ciò potrebbe essere giustificato dalla volontà di preferire l'Ordine europeo d'indagine per la richiesta di misure di indagine che includono – senza tuttavia esaurirsi in essa in modo esclusivo – la produzione di una prova digitale da parte di un altro Stato Membro[21].

Per quanto attiene al Consiglio d'Europa, la Commissione per l'efficienza della giustizia (CEPEJ) si è rapportata alla digitalizzazione in modo analogo all'UE. L'organo ha pubblicato il 9 dicembre 2021, il Piano d'azione "*2022-2025 CEPEJ Action plan: Digitalization for a better justice*", mirato a favorire la digitalizzazione del settore e, in

[19] Pub.L. 115-141, *Clarifying Lawful Overseas Use of Data Act*, del 23 marzo 2018. La legge federale in questione consente alle autorità giudiziarie degli Stati Uniti di accedere ai dati archiviati dalle società statunitensi indipendentemente dalla propria collocazione geografica.

[20] Regolamento EPOC, cit., art. 6, par. 2 e considerando 47 sulla differente area di applicazione che consente all'OEI di "trattare" sull'immunità ed i privilegi degli indagati; Direttiva 2014/41/UE del Parlamento europeo e del Consiglio, *relativa all'ordine europeo di indagine penale*, del 3 aprile 2014, in GUUE L 130, del 1° aprile 2014, pp. 1-36. Per un confronto circa i due strumenti v. S. TOSZA, *All Evidence Is Equal, But Electronic Evidence Is More Equal Than Any Other: The Relationship Between the European Investigation Order and the European Production Order*, in *New Journal of European Criminal Law*, 2020, n. 2, pp. 161-183.

[21] Gli EPOC saranno più dettagliatamente esaminati *infra* (Paragrafo 4.1) quale uno dei punti focali del presente contributo.

questo modo, la qualità della giustizia, la quale deve essere trasparente, cooperativa nonché, citando il testo, "umana".

Precedendo queste linee guida, il 17 novembre 2021 il Comitato dei Ministri del Consiglio d'Europa ha adottato il Secondo protocollo addizionale alla Convenzione di Budapest sul rafforzamento della cooperazione e divulgazione delle prove elettroniche, aperto alla firma e ratifica dal maggio 2022. A venti anni dalla Convenzione sulla criminalità informatica (2001), i redattori del Protocollo hanno ritenuto che le disposizioni addizionali previste possano rappresentare un valore aggiunto da un punto di vista sia operativo che politico. Più precisamente, il testo ha la finalità di predisporre un'assistenza reciproca più proficua, contenendo disposizioni che ammettono la *diretta* collaborazione dei prestatori di servizi all'estero in ipotesi di richiesta d'informazioni sulla sottoscrizione di un utente, di richieste di conservazione di dati, nonché di richieste d'emergenza. In altre parole, in maniera non dissimile dal Regolamento EPOC, il Protocollo migliorerà la capacità cooperativa tra gli Stati Parti[22] come pure tra Stati Parti e *service providers* o altri enti.

Tra l'altro, sulla base di una Raccomandazione del febbraio 2019, il Consiglio UE dava mandato alla Commissione di partecipare ai negoziati del Protocollo in questione. Scopo della partecipazione era il conseguimento della più ampia armonizzazione possibile tra le obbligazioni gravanti sugli Stati ed eterogeneamente derivate dal CdE ed UE. In particolare, l'idea era quella di armonizzare il più possibile la Convenzione di Budapest all'*e-Evidence Pakage* proposto dalla Commissione nel 2018[23].

Ma non è tutto: il Protocollo, così come la Convenzione sulla criminalità informatica, riconosce l'importanza ed il valore di una rete telematica costruita sul libero flusso di informazioni, oltre che sul contemporaneo rispetto dei diritti umani e libertà fondamentali. Per tale ragione, è stato necessario includere nel Protocollo un articolo sulle condizioni e garanzie che limitino le possibilità di cooperazione reciproca in favore dei diritti umani in maniera non dissimile dall'art. 15 della Convenzione del 2001, come verrà discusso in seguito (Paragrafo 4.1).

Dunque, il quadro giuridico delle "novelle" introdotte dall'UE e del Consiglio d'Europa presenta tratti salienti assimilabili. In ambedue i casi, il superamento dei meccanismi "tradizionali" ha prodotto un'azione comune volta ad ottenere una maggiore speditezza, il miglioramento dell'accessibilità dei dati presso i prestatori di servizi privati e la previsione di limitazioni espresse, coincidenti con l'obbligo di non violare ingiustificatamente i diritti fondamentali degli interessati

[22] Il Protocollo introduce un totale di sette meccanismi di cooperazione, suddivisi in tre gruppi principali: 1) misure per garantire che le autorità competenti possano indirizzare direttamente le richieste di informazioni ai prestatori di servizi stabiliti in un altro paese; 2) meccanismi per la messa a disposizione delle prove digitali alle autorità degli Stati aderenti al Protocollo; 3) misure volte a rafforzare la cooperazione nell'ambito dei procedimenti penali in corso, per mezzo della creazione di squadre investigative comuni e dell'impiego della teleconferenza durante i lavori d'indagine.

[23] Raccomandazione di decisione del Consiglio *che autorizza la partecipazione ai negoziati su un secondo protocollo addizionale alla Convenzione del Consiglio d'Europa sulla criminalità informatica (STCE n. 185)*, del 5 giugno 2019, COM(2019) 71 final, considerando 4 e ss.

3. Le implicazioni con riferimento al rispetto per i diritti fondamentali e la giurisprudenza europea in materia

Come evidenziato in precedenza, lo sviluppo del quadro giuridico afferente alla prova digitale risponde alle sfide emerse nel settore della ricerca e conservazione della medesima, dando vita a parallelismi con le sfide della conservazione dei dati più che note alla società civile ed alla dottrina. Prevedibile era, ed è, che le problematiche in questione risiedessero essenzialmente nelle ripercussioni sui diritti fondamentali dell'individuo.

Dovesse presentarsi un deficit delle garanzie ordinamentali previste per l'applicazione degli strumenti di cooperazione giudiziaria chiamati in causa, si esporrebbe l'individuo a subire una violazione (o compressione) di una serie di diritti ben specifici. A livello regionale, la Convenzione europea dei diritti dell'uomo (CEDU)[24] e la Carta dei diritti fondamentali dell'Unione europea (CDFUE, Carta di Nizza)[25] tutelano tali diritti, individuati in particolare da: il diritto alla *privacy* (art. 8 CEDU, art. 8 CDFUE); il rispetto per la vita familiare (art. 8 CEDU, art. 7 CDFUE)[26]; come pure il diritto alla libertà delle comunicazioni e della corrispondenza (art. 10 CEDU, art. 10 CDFUE). In modo doveroso, andrebbero ulteriormente menzionati anche i rischi connessi alla violazione del diritto al giusto processo (art. 6 CEDU, art. 47 CFFUE) nell'ipotesi in cui l'indipendenza delle autorità competente non possa essere garantita.

Vero è che in plurimi testi giuridici risulta una diffusa consapevolezza circa il potenziale impatto negativo della cooperazione di settore, ovvero l'indebita violazione o limitazione dei diritti fondamentali di soggetti indagati/imputati o condannati. Altresì, è nei medesimi testi giuridici che viene chiarito che taluni principi possano impedire, o quantomeno ostacolare, gli (eventuali) effetti negativi della cooperazione giudiziaria digitale. Detti principi concretizzano in sostanza sia *garanzie* per i diritti che *condizioni* operative volte a supervisionare l'attività di cooperazione penale transfrontaliera, come evidenziato nel Preambolo del Secondo Protocollo alla Convenzione di Budapest[27]. Del resto, volgendo lo sguardo all'Unione europea, è possibile pervenire alle stesse conclusioni.

---

[24] *Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, del 4 novembre 1950, concepita in seno al Consiglio d'Europa.

[25] *Carta dei diritti fondamentali dell'Unione europea*, del 7 dicembre 2000, quale prodotto normativo dell'Unione europea.

[26] Rispettivamente, vi sono illustri autori che ha notato come l'art. 7 CEDU rappresenti "il *culmine del percorso di codificazione e di costituzionalizzazione del diritto europeo alla protezione dei dati personali*", O. POLLICINO, M. BASSINI, *Art. 8*, in S. ALLEGREZZA, R. MASTROIANNI, F. PAPPALARDO, O. POLLICINO, O. RAZZOLINI (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Milano, 2017, p. 135; e come l'art. 8 CEDU rappresenti una disposizione che più delle altre, tra quelle incluse nel catalogo europeo di diritti e libertà, testimonia il carattere di "*living instrument*" della stessa Convenzione; A. DI STASI, *Introduzione alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, III ed., Milano, 2022, p. 11.

[27] Il testo così riporta: "*Convinced that effective cross-border co-operation for criminal justice purposes, including between public and private sectors, benefits from effective conditions and safeguards for the protection of human rights and fundamental freedoms*".

Il riferimento è al Regolamento EPOC, dov'è ampiamente "pubblicizzato" che l'intero atto mira ad essere operativo senza dover (indebitamente) sacrificare i diritti degli individui coinvolti dalla sua applicazione. Tale concetto è espresso nel considerando 2 del Regolamento: "tali meccanismi dovrebbero essere soggetti a condizioni e garanzie per assicurare il pieno rispetto dei diritti fondamentali e dei principi riconosciuti dall'art. 6 del trattato sull'Unione europea (TUE) e dalla Carta dei diritti fondamentali dell'Unione europea". E di tale proposito è rinvenibile traccia anche all'art. 1, par. 3 del Regolamento EPOC, rappresentante l'oggetto dell'atto stesso[28]. In effetti, tale previsione rappresenta una formula ricorrente negli atti che disciplinano le procedure di cooperazione giudiziaria[29]. Tuttavia, com'è noto, anche in assenza di tale disposto, la Carta sarebbe ugualmente vincolante nei confronti delle autorità nazionali al momento dell'applicazione delle disposizioni di diritto derivato dell'Unione europea *ex* art. 51 CFFUE.

In ragione di tale esigenza garantista, le misure disposte per la produzione e conservazione della prova – si potrebbe dire diffusamente[30] – rispondono a specifici principi che disciplinano il settore della cooperazione penale transfrontaliera. Questi sono identificabili anzitutto nella proporzionalità e la necessità dei mezzi e delle indagini.

3.1 La tutela dei diritti secondo le corti europee: i principi di proporzionalità e di necessità della misura quali garanzia per l'individuo

A buon ragione, la medesima consapevolezza palesata nel momento legislativo sembra essere condivisa all'interno della prassi delle principali coorti europee. Tant'è che, in ambito di persecuzione penale per mezzi digitali, la Corte di giustizia dell'Unione europea (CGUE) e la Corte europea dei diritti dell'uomo (Corte EDU) hanno nel corso del tempo provveduto a razionalizzare gli stessi principi.

In primo luogo, le corti hanno entrambe convenuto sulla regola generale che qualsiasi forma di limitazione al diritto per il rispetto della propria vita privata e, in particolare, dei propri dati debba avvenire in maniera strettamente necessaria e proporzionata[31]. Con

[28] Art. 1, par. 3 Regolamento EPOC: "Il presente regolamento non ha l'effetto di modificare l'obbligo di rispettare i diritti fondamentali e i principi giuridici sanciti dalla Carta e dall'articolo 6 TUE […] Il presente regolamento si applica senza pregiudizio dei principi fondamentali, in particolare la libertà di espressione e di informazione, compresi la libertà e il pluralismo dei media, il rispetto della vita privata e familiare, la protezione dei dati personali e il diritto a una tutela giurisdizionale effettiva".

[29] V. ad esempio il Regolamento (UE) 2021/693 del Parlamento europeo e del Consiglio, *che istituisce il programma Giustizia e abroga il Regolamento (UE) n. 1382/2013*. del 28 aprile 2021, in GUUE L 156, del 5 maggio 2021, considerando 1.

[30] Nell'ambito delle Nazioni Unite, v. 14° congresso delle Nazioni Unite sulla prevenzione del crimine e sulla giustizia penale, *Kyoto Declaration on Advancing Crime Prevention, Criminal Justice and the Rule of Law: Towards the Achievement of the 2030 Agenda for Sustainable Development*, 7-12 marzo 2021, parr. 64 e 72; in UE, v. Regolamento EPOC, cit., consideranda 2, 15, 24, 38, nonché art. 5, par. 2 ed art. 6, par. 2; nel Consiglio d'Europa, v. Convenzione di Budapest, cit., art. 15, oltre al suo Secondo Protocollo, cit., artt. 2 e 14.

[31] *Inter alia*, con riguardo alla Corte di Lussemburgo, v. Corte di Giustizia, Grande Sezione, sentenza dell'8 aprile 2014, *Digital Rights Ireland*, cause riunite C-293/12 e C-594/12; Corte di Giustizia, Grande Sezione, sentenza del 21 dicembre 2016, *Tele2Sverige e Tom Watson*, cause riunite C-203/15 e C-698/15, par. 96.

riguardo alla Corte EDU, com'è noto, il testo della CEDU non esplicita la necessità dell'utilizzo del principio di proporzionalità per dirimere eventuali conflitti tra la tutela dei diritti fondamentali e la tutela degli obiettivi di interesse pubblico. Tuttavia, la Corte europea dei diritti dell'uomo ha utilizzato il suddetto principio estraendolo, seppur in forma implicita, dallo stesso testo della Convenzione[32].

Simultaneamente, nel caso della Corte di giustizia dell'Unione europea, il richiamo all'art. 52, par. 1 CDFUE[33] consente di comprendere che, "in caso di limitazioni all'esercizio dei diritti e delle libertà riconosciuti" dalla Carta di Nizza, taluni specifici parametri dovranno venire in considerazione[34]. In modo particolare la disposizione fa riferimento al parametro della proporzionalità, declinabile nella idoneità, necessità e proporzionalità (qui in senso stretto) delle misure limitative di diritti non assoluti.

In via più specifica, la Corte di Giustizia enfatizzava *ab origine* che le misure adottate dagli inquirenti *saranno comunque tenute a confrontarsi con forme di limitazione e controllo* (*Schrems I* e *Schrems II*)[35]. Ciò, laddove vi sia un trasferimento di dati transfrontaliero (ed in particolare verso Stati terzi, come gli Stati Uniti), sarebbe previsto[36] anche quando le iniziative dell'UE e dei suoi Stati Membri rispondessero all'obiettivo della lotta al terrorismo ed al crimine organizzato, ovvero al tema della sicurezza nazionale[37]. Perfino in questi casi si ammette(va) che la cooperazione interstatale possa

---

L'attenzione verso la Corte di Strasburgo invece impone di guardare a: Corte europea dei diritti dell'uomo, Grande Camera, sentenza del 4 dicembre 2015, ricorso n. 47143/06, *Roman Zakharov c. Russia*, par. 227 ss.; Corte europea dei diritti dell'uomo, Grande Camera, sentenza del 4 maggio 2000, ricorso n. 28341/95, *Rotaru c. Romania*, par. 47 ss. Cfr. F. ROSSI DAL POZZO, *La giurisprudenza della Corte di giustizia sul trattamento dei dati personali*, in A.A. V.V., *Quaderni AISDUE*, vol. I, Bari, 2020.

[32] M. DE SALVIA, *La Convenzione europea dei diritti dell'uomo*, Napoli, 2001; D.U. GALETTA, *Il principio di proporzionalità nella Convenzione europea dei diritti dell'uomo, fra principio di necessarietà e dottrina del margine di apprezzamento statale: riflessioni generali su contenuti e rilevanza effettiva del principio*, in *Rivista italiana di diritto pubblico comunitario*, 1999, nn. 3-4, p. 743 ss.

[33] Art. 52, par. 1 CDFUE: "Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui".

[34] T. GROPPI, *L'Europa dei diritti*, Bologna, 2001, p. 356.

[35] Progressi in tal senso si sono registrati nella nota "*Schrems saga*", ricomprendente i casi Corte di Giustizia, Grande Sezione, sentenza del 6 ottobre 2015, *Maximillian Schrems c. Data Protection Commissioner*, causa C-362/14 e; Corte di Giustizia, Grande Sezione, sentenza del del 16 luglio 2020, *Data Protection Commissioner c. Facebook Ireland Limited e Maximillian Schrems*, causa C-311/18. Per un'analisi critica della saga in questione, v. M. NINO, *La sentenza Schrems II della Corte di giustizia UE: trasmissione dei dati personali dall'Unione europea agli Stati terzi e tutela dei diritti dell'uomo*, in *Diritti umani e diritto internazionale*, 2020, n. 3, pp. 733-760; M. NINO, *Le prospettive internazionali ed europee della tutela della privacy e dei dati personali dopo la decisione Schrems della Corte di giustizia UE*, in *Il Diritto dell'Unione europea*, 2016, n. 4, pp. 755-788; I. OLDANI, *The Impact of the Schrems II Judgment on International Data Transfers*, in *Quaderni di SIDIblog*, 2020, vol. 7, pp. 547-563.

[36] Tale scelta terminologica deriva dal fatto che, guardando la giurisprudenza analizzata *infra*, il ruolo di attore principale (e prioritario) attribuito alla sicurezza degli Stati Membri sembra essere tutto fuorché eliso dal discorso. Piuttosto, esso è stato al massimo temperato mediante l'imposizione di forme di controllo più stringenti verso le c.d. autorità di "*law enforcement*".

[37] A fronte di una cospicua dottrina in materia, si rimanda *ex multis* a: B. NASCIMBENE, I. ANRÒ, *Primato del diritto dell'Unione europea e disapplicazione. Un confronto fra Corte costituzionale, Corte di Cassazione e Corte di giustizia in materia di sicurezza sociale*, in *Giustizia insieme*, 31 marzo 2022; Ö.H.

comportare un'ingiustificata compressione di diritti fondamentali e dello Stato di diritto ove le condizioni previste dalla regola generale non siano rispettate.

Guardando poi alla Convenzione europea dei diritti dell'uomo, nella giurisprudenza della Corte EDU veniva stabilito in modo similare che, in ipotesi di sorveglianza di massa, forme minime di garanzia dovrebbero essere approntate all'interno della legislazione nazionale di riferimento. Segnatamente, come nel caso *Zakharov*[38] circa le intercettazioni telefoniche, le garanzie minime devono essere costituite da una serie di elementi: la precisione tassativa della natura delle offese che possono giustificare la misura di controllo; la definizione delle categorie di individui assoggettabili ad intercettazioni; i limiti massimi previsti per la durata delle intercettazioni; la definizione delle procedura da adottare per l'esame, dell'uso e della conservazione dei dati ottenuti; le precauzioni da predisporre al momento del trasferimento dei dati ad altri soggetti; e, infine, le circostanze per le quali i dati possono o devono essere eliminati o le registrazioni fisicamente distrutte[39]. Le restrizioni ai diritti individuali, dunque, sono giustificate alla luce dell'art. 8 CEDU soltanto quando siano espressamente previste dalla legge e siano necessarie in una società democratica allo scopo di ottenere determinati scopi legittimi[40].

Un altro passaggio di significativo interesse è rappresentato dalle sentenze emanate dalle due corti in tema di *data retention* piuttosto che di *data production.* Non a caso, la sfida posta dalla conservazione della prova digitale appare inevitabilmente correlata alla più vasta problematica, lungamente dibattuta, della conservazione dei dati.

Storicamente, la CGUE ebbe occasione di dichiarare l'illegittimità della Direttiva 2006/24/CE[41], che per l'appunto prevedeva forme di *data retention*, a causa della

---

ÇINAR, *The Current Case Law of the European Court of Human Rights on Privacy: Challenges in the Digital Age*, in *The International Journal of Human Rights*, 2021, n. 25, pp. 26-51; C. CINELLI, *Sorveglianza digitale, sicurezza nazionale e tutela dei diritti umani*, in *Ordine internazionale e diritti umani*, 2020, n. 3, pp. 588-608; M. OROFINO, *Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione*, in *Rivista di diritto dei media*, 2018, n. 2, pp. 82-104; T. ACKERMANN, K. FENRICH, *Motion and Rest International Law's Responsiveness Towards Terrorism, Mass Surveillance, and Self-Defence*, in *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht*, 2017, n. 77, pp. 745-807; M. RUBECHI, *Sicurezza, tutela dei diritti fondamentali e "privacy": nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)*, in *Federalismi.it*, 2016, n. 23, pp. 1-26; A.D. MOORE, *Privacy, Security, and Government Surveillance: Wikileaks and the New Accountability*, in *Public Affairs Quarterly*, 2011, n. 2, pp. 141-156; S. PEERS, *National Security and European Law*, in *Yearbook of European Law*, 1999, pp. 363-404.

[38] Corte europea dei diritti dell'uomo, Grande Camera, *Zakharov c. Russia*, cit., par. 231. Sull'effettiva portata della sentenza cfr. G. FORMICI, *La digital mass surveillance al vaglio della Corte europea dei diritti dell'uomo: da Zakharov a Big Brother Watch*, in *Federalismi.it*, 2020, n. 23, pp. 43-71; V. RUSINOVA, *A European Perspective on Privacy and Mass Surveillance at the Crossroads*, in *Higher School of Economics Research Paper*, 2019, n. 87, pp. 1-22; L. WOODS, *Zakharov v Russia: Mass Surveillance and the European Court of Human Rights*, in *EU Law Analysis*, 16 dicembre 2016; P. DE HERT, P.C. BOCOS, *Case of Roman Zakharov v. Russia: The Strasbourg Follow up to the Luxembourg Court's Schrems Judgment*, in S*trasbourgObservers*, 23 dicembre 2015.

[39] Corte europea dei diritti dell'uomo, Grande Camera, *Zakharov c. Russia*, cit., par. 231.

[40] Ivi, par. 227.

[41] Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, *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*, del 15 marzo 2006, in GUUE L 105/56 del 13 aprile 2006, pp. 54-63.

violazione degli artt. 7 e 8 CDFUE[42]. La violazione prospettata non si direbbe tuttavia coincidere con "un'incompatibilità assoluta con la Carta di Nizza"[43]. Ad ogni modo, ciò che va notato è che inizialmente il legislatore europeo del tempo, nell'immaginare un quadro normativo comune per la conservazione dei dati, aveva ritenuto che l'art. 8 CEDU – affidandosi ad una *bill of rights* diversa dalla Carta di Nizza – potesse rappresentare non soltanto una disposizione impositiva di limitazioni, ma anche lo strumento per giustificare misure securitarie verso gli individui[44].

Ma, come esplicato in precedenza, la Corte di Giustizia non valutò positivamente le innovazioni introdotto dalle altre istituzioni europee. Alimentando un filone inizialmente "garantista", nella celebre sentenza *Digital Rights Ireland* del 2014[45] la CGUE ritenne di vietare quelle pratiche consistenti nell'imposizione ai gestori di servizi di telecomunicazioni di provvedere in via generale e diffusa alla conservazione dei metadati degli utenti[46]. Nelle intenzioni dei legislatori nazionali, tale conservazione sarebbe stata richiesta per rendere possibili taluni accessi successivi alle informazioni da parte delle autorità competenti di polizia giudiziaria o di *intelligence* contestualmente alla prevenzione, indagine e contrasto a minacce rivolte alla sicurezza pubblica/nazionale[47].

In questo filone vengono ulteriormente in considerazione le sentenze gemelle del 6 ottobre 2020, *Privacy International*[48] e *La Quadrature*[49], in cui i giudici di Lussemburgo

[42] Corte di Giustizia, Grande Sezione, *Digital Rights Ireland*, cit., parr. 38-69.

[43] Come osservato da M. NINO, *La normalizzazione della sorveglianza di massa nella prassi giurisprudenziale delle Corti di Strasburgo e Lussemburgo: verso il cambio di paradigma del rapporto privacy v. security*, in questa *Rivista*, 2022, n. 2, p. 115.

[44] Direttiva 2006/24/CE, cit., considerando 9.

[45] Alle medesime conclusioni, in verità, pervenì la *Bundesverfassungsgericht* tre anni prima, il 2 marzo 2010. Sulla decisione della Corte costituzionale tedesca, v. R. FLOR, *Data retention e limiti al potere coercitivo dello Stato in materia penale: le sentenze del Bundesverfassungsgericht e della Curtea Constituionala*, in *Cassazione Penale*, 2011, n. 5, p. 1954 ss.

[46] Sebbene non inerente al contenuto delle comunicazioni, i metadati – ovvero i dati di traffico (orario, durata, destinatari e frequenza delle comunicazioni), la localizzazione dei *device* dell'utente, gli indirizzi IP, oppure i dati dell'*account* di un utente – rendono senz'altro possibile l'analisi delle relazioni umane tenute da un soggetto e dei luoghi da esso frequentati, consentendo di trarre conclusioni precise sulla vita dello stesso.

[47] Un'analisi della natura della "*dicotomia privacy vs. security*" è stata effettuata da G. NADDEO, *Il difficile bilanciamento tra sicurezza nazionale e tutela dei diritti fondamentali nella "data retention saga" dinanzi alla Corte di giustizia UE*, in questa *Rivista*, 2022, n. 2, pp. 188-217, v. spec. 188-191 e 214, dove si evidenzia un certo *favor* verso la sicurezza a discapito della riservatezza. Sul tema, più in generale, si rimanda anche a S. MARCOLINI, *L'istituto della data retention dopo la sentenza della Corte di Giustizia del 2014*, in A. CADOPPI, S. CANESTRARI, A. MANNA (a cura di), *Trattati giuridici - Cybercrime*, Milano, 2019, pp. 1579- 1582; E. CELESTE, *The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future*, in *European Constitutional Law Review*, 2019, n. 15, pp. 134-157; G. FORMICI, *La disciplina della data retention tra esigenze securitarie e tutela dei diritti fondamentali*, Torino, 2021; A. JUSZCZAK, E. SASON, *Recalibrating Data Retention in the EU The Jurisprudence of the Court of Justice of the EU on Data Retention – Is this the End or is this the Beginning?*, in *Eucrim-The European Criminal Law Associations' Forum*, 2021, n. 4, pp. 238-266.

[48] Corte di giustizia, Grande Sezione, sentenza del 6 ottobre 2020, *Privacy International c. Secretary of State for Foreign and Commonwealth Affairs*, causa C-623/17.

[49] Corte di giustizia, Grande Sezione, sentenza del 6 ottobre 2020, *La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatife, Igwan.net c. Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées*, cause riunite C-511/18, C-512/18 e C-520/18. Sulle sentenze la dottrina si è espressa riccamente, v. *ex multis* M. TZANOU, S.

riaffermarono, prima di tutto, che la *data retention* rientra nell'ambito applicativo del diritto dell'Unione europea, fugando dubbi sulla competenza della stessa Corte a giudicare in materia. Tale competenza non viene meno perfino nei casi in cui la conservazione dei dati sia mirata a tutelare la sicurezza nazionale. Del resto – chiarisce la Corte – l'obbligo imposto ai gestori di servizi e la conseguente possibilità di accesso ai dati rappresentano un perfetto esempio di trattamento dei dati effettuato da parte da privati e non già di attività esclusivamente eseguite da parte di autorità statali[50]. In altre parole, la Corte eccepisce l'incompatibilità con il diritto dell'Unione europea di forme di conservazione generale *indiscriminate* di dati di traffico e di localizzazione. La conseguenza di ciò è che la *proporzionalità* e la *necessità* della misura adottata siano necessarie a prescindere dal tipo di indagine e di provvedimento adottato nel caso di specie. Dunque, tali principi (trasversali) necessitano di essere applicati alle forme di conservazione generalizzata e non unicamente a quelle di natura individualizzata (come nel caso degli EPOC ed OEI).

Diversamente, in netta discontinuità con i contenuti della propria precedente sentenza *Zakharov*, la Corte EDU ha avuto modo di stabilire nel caso *Big Brother Watch*[51] del 2021 che l'intercettazione generalizzata di dati personali da parte di servizi di *intelligence* (per motivi evidentemente securitari) non è intrinsecamente contraria alle disposizioni contenute nella CEDU[52]. Ma anzi, la sorveglianza di massa rappresenterebbe uno strumento di vitale importanza nell'identificazione delle minacce alla sicurezza nazionale dal momento che scelte operative diverse da queste non assicurerebbero ai servizi di *intelligence* risultati apprezzabili allo stesso modo. In altri termini, la decisione di

---

KARYDA, *Privacy International and Quadrature du Net: One Step Forward Two Steps Back in the Data Retention Saga?*, in *European Public Law*, 2022, n. 1, pp. 123-154; M. NINO, *La disciplina internazionale ed europea della data retention dopo le sentenze Privacy International e La Quadrature du Net della Corte di giustizia UE*, in *Il Diritto dell'Unione europea*, 2021, n. 1, pp. 93-124; J. SAJFERT, *Bulk data interception/retention judgments of the CJEU – A victory and a defeat for privacy*, in *European Law Blog*, 26 ottobre 2020 ; M. ZALNIERIUTE, *The Future of Data Retention Regimes and National Security in the EU after the Quadrature Du Net and Privacy International Judgments*, in *ASIL Insights*, vol. 24, n.28, 2020.

[50] Corte di giustizia, Grande Sezione, *Privacy International*, cit., par. 47. Coerentemente a tale valutazione, v. Corte di giustizia, Grande Sezione, sentenza del 21 dicembre 2016, *Tele2 Sverige AB c. Postoch telestyrelsen e Secretary of State for the Home Department c. Tom Watson and others*, cause riunite C-203/15 e C-698/15; nonché Corte di giustizia, Grande Sezione, sentenza del 2 ottobre 2018, *Secretary of State for the Home Department c. Tom Watson and Ministerio Fiscal*, causa C-207/16.

[51] Corte europea dei diritti dell'uomo, Grande Camera, sentenza del 25 maggio 2021, ricorsi nn. 58170/13, 62322/14 e 24960/15, *Big Brother Watch e altri c. Regno Unito*, par. 323, sui sono interessanti le analisi di M. ZALNIERIUTE, *Procedural Fetishism and Mass Surveillance under the ECHR: Big Brother Watch v. UK*, in *VerfBlog*, 2 giugno 2021; G. TIBERI, *Il caso Big Brother Watch quale cambio di paradigma nel bilanciamento tra sicurezza e tutela dei diritti fondamentali?*, in *Quaderni Costituzionali*, 2018, n. 4, pp. 931-933; T. CHRISTAKIS, *A Fragmentation of EU/ECHR Law on Mass Surveillance: Initial Thoughts on the Big Brother Watch Judgment*, in *European Law Blog*, 20 settembre 2018; e di G. Naddeo, *Il difficile bilanciamento tra sicurezza nazionale e tutela*, cit., p. 208-209, ove si nota che la sentenza ha rappresentato un temporaneo punto di convergenza in materia tra la corte di Lussemburgo e quella di Strasburgo.

[52] V. a tal proposito l'analisi di M. NINO, *La normalizzazione della sorveglianza*, cit., p. 120, il quale considera che il riconoscimento della compatibilità della sorveglianza di massa con la Convenzione sia equivalente a provocare la legittimazione e normalizzazione di forme di intercettazione indiscriminata e priva di reali limiti temporali. Da tale compatibilità, alla luce dei principi di necessità, di specificità e di uso limitato dei dati, può e deve emergere logicamente più di un dubbio.

implementare una sorveglianza di massa allo scopo di identificare e prevenire minacce alla sicurezza e attacchi ad interessi nazionali fondamentali rientra nel margine d'apprezzamento delle singole autorità Statali competenti. Argomentazione ulteriore aggiunta dalla Corte EDU, di sicuro interesse per questa disamina, è che la sorveglianza di massa non costituirebbe in verità una interferenza maggiore nella vita privata del cittadino rispetto a quella riscontrabile mediante l'impiego di intercettazioni mirate ed individualizzate. Si potrebbe affermare che sia stata proclamata dalla Corte la non obbligatorietà della predisposizione e del rispetto garanzie previste per tutelare i diritti individuali. Vieppiù, i contenuti della sentenza *Big Brother Watch* sono stati di seguito saldamente confermati dalla Corte di Strasburgo nel caso *Centrum för Rättvisa*[53].

Le posizioni adottate dalla Corte EDU nel 2021 sul tema sono state fatte proprie dalla CGUE lo stesso anno e nel periodo successivo. Nella sentenza *HK Prokuratuur*[54] la Corte di Giustizia ha identificato, facendo un passo indietro rispetto alla propria giurisprudenza pregressa, l'eccezionale possibilità di far uso di una conservazione di dati generalizzata. Il riferimento è ai c.d. dati esteriori, principalmente condensati nel supporto materiale (oggi raramente di natura cartacea, ma perlopiù informatica) dei tabulati di traffico, che, pur non esaurendo le ipotesi di rilevanza pratica degli stessi, ne rappresentano tuttavia lo strumento privilegiato di impiego nel processo penale. Ad ogni modo, laddove sia necessaria per garantire la sicurezza nazionale – per esempio in ipotesi di contrasto al terrorismo, che indubbiamente costituisce un obiettivo più "elevato" rispetto alla lotta al crimine ordinario – la conservazione generalizzata dei dati esteriori diviene ammissibile. In tale evenienza, dunque, i principi di necessità e proporzionalità quasi verrebbero soddisfatti *a prescindere*, sebbene la sentenza chiarisca che comunque occorrerà un'autorizzazione dell'autorità competente "necessariamente prima che i dati e le informazioni che ne derivano possano essere consultati"[55] (*infra*). Nell'ambito della cooperazione giudiziaria e di polizia è lampante come la pronuncia costituisca una cesura rispetto alla giurisprudenza CGUE previamente richiamata che, al contrario, aveva tendenzialmente dichiarato l'inammissibilità di tale forma di conservazione di dati.

La Corte di Giustizia, inoltre, ha recentemente confermato la validità della eccezione profilata in *HK Prokuratuur* nella sentenza *SpaceNet e Telekom Deutchland* del 20

[53] Corte europea dei diritti dell'uomo, Grande Camera, sentenza del 25 maggio 2021, ricorso 35252/08, *Centrum för Rättvisa c. Svezia*, parr. 254, 264 e 365; su cui si invita a visionare i commenti di M. MILANOVIC, *The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för rättvisa*, in *EJIL:Talk!*, 26 maggio 2021; J. SAJFERT, *The Big Brother Watch and Centrum för Rättvisa judgments of the Grand Chamber of the European Court of Human Rights – the Altamont of Privacy?*, in *European Law Blog*, 8 giugno 2021.

[54] Corte di Giustizia, Grande Sezione, sentenza del 2 marzo 2021, *HK Prokuratuur*, causa C-746/18, parr. 35-50, su cui si sono tra gli altri espressi E. ANDOLINA, *La sentenza della Corte di giustizia UE nel caso H.K. c. Prokuratuur: un punto di non ritorno nella lunga querelle in materia di 'data retention'?*, in *Processo penale e Giustizia*, 2021, n. 5, pp. 1204-1217; M. ARANCI, *L'acquisizione dei dati esteriori delle comunicazioni nel processo penale italiano dopo la sentenza H.K.: alcuni spunti di riflessione sulle prime applicazioni giurisprudenziali*, in *La legislazione penale*, 2021, n. 3, pp. 66-92.

[55] Corte di Giustizia, Grande Sezione, *HK Prokuratuur*, cit., par. 40.

settembre 2022[56], disponendo la necessità che la conservazione dei dati debba essere effettuata unicamente per un lasso di tempo determinato. Si precisa che il termine massimo per la *data retention* debba altresì considerarsi "rinnovabile" per quanto disposto in *Commissioner of An Garda Siochana* dell'aprile 2022[57].

Cionondimeno, ciò che emerge dalla recente giurisprudenza di Lussemburgo è che la rilevante interferenza nei diritti fondamentali coinvolti deve considerarsi giustificata in forza del *superiore interesse* (o necessità) della sicurezza nazionale, sempre nel rispetto di talune condizioni, dovendo soddisfare i principi di proporzionalità ed indipendenza come ridefiniti in *HK Prokuratuur*. L'indipendenza, infatti, è un prerequisito per la corretta valutazione di proporzionalità della misura, ovvero un corollario a quest'ultima. Tant'è che nello stesso caso venivano forniti chiarimenti su dette condizioni ovvero, segnatamente, la gravità del crimine in questione e la presenza (esclusiva) di un *controllo preventivo* da parte di un giudice o un'autorità amministrativa che siano *indipendenti*[58]. Specificamente, veniva escluso che il pubblico ministero, il cui compito è di dirigere il procedimento istruttorio penale e di esercitare, eventualmente, l'azione penale in un successivo procedimento, possa essere competente ad autorizzare l'accesso di un'autorità pubblica ai dati relativi al traffico e ai dati relativi all'ubicazione ai fini di un'istruttoria penale[59]. Tra l'altro, la Corte EDU nel caso *Dumitru Popescu* del lontano 2007, pervenne ad una valutazione assai simile, sebbene specificamente riferita alla Romania e alla presenza di una discrezionalità evidente del PM[60].

In ogni caso, riconoscendo unicamente il controllo preventivo, la CGUE si è invece sostanzialmente discostata dalle conclusioni raggiunge dalla Corte europea dei diritti dell'uomo. Quest'ultima, nel caso *Szabo e Vissy*[61], provvedeva a riconoscere – laddove giustificato da eccezionali circostanze di gravità del crimine – l'ammissibilità di un *controllo successivo ed indipendente* sulla captazione e conservazione di informazioni

[56] Corte di Giustizia, Grande Sezione, sentenza del 20 settembre 2022, *Bundesrepublik Deutschland c. SpaceNet AG e Telekom Deutschland GmbH*, cause riunite C-793/19 e C-794/19, parr. 72-74, 92-106 e 131.
[57] Corte di giustizia, Grande Sezione, sentenza del 5 aprile 2022, *Commissioner of An Garda Siochana*, causa C-140/20, par. 82, su cui si sono espressi *ex multis* F. RESTA, *Dalla conservazione generalizzata a quella mirata e rapida: la Corte di giustizia ridelinea i contorni della data retention*, *in Giustizia insieme*, 7 aprile 2022; M.C. DALY, *Data Retention Rules for Europe - A Headache or a Vindication?*, in *Data Protection Ireland Journal*, 2022, n. 3, pp. 11- 13.
[58] Corte di Giustizia, Grande Sezione, *HK Prokuratuur*, cit., parr. 32-45 e 51.
[59] Ivi, parr. 54-57.
[60] Corte europea dei diritti dell'uomo, Terza Camera, sentenza del 26 aprile 2007, ricorsi nn. 49234/99 e 71525/01, *Dumitru Popescu c. Romania*, parr. 70-73.
[61] Corte europea dei diritti dell'uomo, Quarta Camera, sentenza del 12 gennaio 2016, ricorso 37138/14, *Szabó e Vissy c. Hungary*, par. 77: "*an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure* […] *The ex-ante authorisation of such a measure is not an absolute requirement per se, because where there is extensive post factum judicial oversight, this may counterbalance the shortcomings of the authorisation*". Sulla sentenza, si registra l'opinione di E. PÁSZTOR, *Secret Intelligence Gathering - A Low Threshold Still Too High to Reach. The Gap Between the Level of Privacy Protection in Europe and in Hungary After the Case of Szabó and Vissy v Hungary*, in *ELTE Law Journal*, 2017, n. 1, pp. 99-112.

personali. Tra l'altro, la stessa formulazione circa la gravità del crimine si era già attestata nel caso *Zakharov* previamente citato[62].

Sulla questione della natura del controllo, vista la sua rilevanza nelle riflessioni che seguiranno nel prossimo paragrafo, appare giusto spendersi in un'ulteriore considerazione: il requisito dell'indipendenza del controllo dovrebbe automaticamente comportare l'esclusione di soggetti privati e altri soggetti "di parte" da compiti di supervisione verso atti che dispongano la conversazione dei dati. Nella definizione di autorità indipendente, invece, possono rientrare le autorità non giudiziarie (autorità amministrative, come le agenzie) a condizione che, nuovamente in accordo con la sentenza *Szabo e Vissy*, esse siano senz'altro "*effective*" e "*compatible with the Convention*"[63].

Ad ogni modo, l'esistenza di controllo, *ex ante* o *ex post* che sia, costituisce un elemento non trascurabile della *data retention*. Si tratta di uno strumento utile a verificare la *compliance* della misura operativa nei confronti delle garanzie minime imposte dallo Stato di diritto. Ciò che ne deriva è la sua imprescindibilità, giustificata dalla finalità di tutelare i diritti fondamentali. Pertanto, il controllo (i controlli) della misura adottata deve essere considerato quale parte dell'assioma generale che regola la cooperazione giudiziaria in materia penale.

In conclusione – a fronte della irrinunciabilità dei diritti umani[64] nonché delle regole di bilanciamento dei diritti non assoluti prescritte dall'art. 52 CDFUE e dalla giurisprudenza costante della Corte EDU – si è persuasi dal ritenere che i principi di proporzionalità e necessità, nonché dell'indipendenza dell'autorità di controllo per la misura adottata, così come desunti ed interpretati nella giurisprudenza europea sulla conservazione generalizzata dei dati possano essere similmente applicati per analogia alle "nuove" procedure di cooperazione giudiziaria e di polizia . Tali principi (o criteri operativi), in tal senso, sarebbero da considerarsi quali regole *generali* e *trasversali*[65], una

[62] Corte europea dei diritti dell'uomo, Grande Camera, *Zakharov*, cit., para. 234.
[63] Corte europea dei diritti dell'uomo, Quarta Camera, *Szabo e Vissy*, cit, par. 77.
[64] Ciò non è solo evidente ai sensi del diritto primario dell'Unione, come nel caso degli artt. 2 e 6 del Trattato sull'Unione europea, ma anche dalle garanzie minime predisposte per mezzo del diritto secondario e di atti programmatici, come nel caso della Comunicazione della Commissione del 2 dicembre 2020, *cit.*, sezione 3. In modo simile, la Risoluzione del Parlamento europeo del 3 ottobre 2017, par. 50, sottolinea "la necessità di consentire alle autorità di contrasto di accedere legalmente alle informazioni pertinenti in circostanze limitate laddove tale accesso sia necessario e proporzionato per ragioni di sicurezza e giustizia; sottolinea la necessità che le autorità giudiziarie e di contrasto siano dotate di sufficienti capacità e finanziamenti per condurre indagini legittime".
[65] Curiosamente, nella premessa si era preconizzata l'estensione di tali principi dalle misure generalizzate (sorveglianza di massa) a quelle specifiche (nell'interesse di questo scritto, agli EPOC) perché ciò era nell'interesse dell'indagine svolta. Ma, all'opposto, va riconosciuto che i principi in questione erano originariamente emersi nel contesto delle misure specifiche (OEI) e, soltanto in un secondo momento, traslate nella giurisprudenza sulle misure generalizzate. Il riferimento è alle condizioni e alle garanzie messe in atto al momento della messa a punto dell'ordine europeo di indagine, nel 2014, poco prima dell'inizio *data retention saga* presso la CGUE, che di fatto è venuta ad esistenza nello stesso anno; v. Direttiva 2014/41/UE, cit., considerando 11 e 42 nonché art. 6, par. 1: "L'autorità di emissione può emettere un OEI solamente quando ritiene soddisfatte le seguenti condizioni: a) l'emissione dell'OEI è necessaria e proporzionata ai fini del procedimento di cui all'articolo 4, tenendo conto dei diritti della persona sottoposta

sorta di assioma comune[66], di cui sarà richiesta l'applicazione prescindendo dalla natura del provvedimento, indifferentemente generalizzato (*mass surveillance*) o specifico (es. Ordini europei di produzione e conservazione).

In ogni caso, ciò che ne consegue e che rileva è che i principi necessità e proporzionalità, seppur reinterpretati contenutisticamente dalla prassi giurisprudenziale nel corso degli anni, sono adatti a disciplinare le misure impiegate nel settore della conservazione dei dati in qualsivoglia modo declinate, e dunque anche della prova digitale.

4. Dubbi di compatibilità con la prassi giurisprudenziale nel futuro della cooperazione giudiziaria digitale

In considerazione di quanto riportato in precedenza, esiste, dunque, una peculiare settore della cooperazione digitale penale e vi è una diffusa consapevolezza circa la potenziale violazione di diversi diritti fondamentali. La prassi giurisprudenziale ha nel corso del tempo prospettato interpretazioni che tendenzialmente ponessero limiti a tali rischi, limiti concretizzatesi in forme di controllo sulla "meritevolezza" della interferenza nei diritti fondamentali. Tant'è che detti controlli si basano sulla soddisfazione dei principi di necessità e proporzionalità, sorretti da un'indipendenza dell'organo giudicante. A causa dell'importanza dei diritti in gioco, le prescrizioni e limiti in parola possono essere traslati in qualsiasi misura di controllo digitale e, pertanto, anche in casi di cooperazione giudiziaria e di polizia. Tuttavia, alcune discrepanze possono essere individuate tra i contenuti del quadro giuridico che nel futuro disciplinerà la materia della cooperazione penale digitale nella regione (UE e Consiglio d'Europa) ed i principi di

a indagini o imputata; e b) l'atto o gli atti di indagine richiesti nell'OEI avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo".

[66] Tale idea dell'implementazione di un assioma unico è supportata dal contenuto della storica sentenza *Digital Rights Ireland*, ove la CGUE dichiarò l'invalidità della Direttiva sulla conservazione dei dati del 2006 in quanto l'interferenza verso i diritti umani fondamentali (rispetto per la *privacy* e tutela dei dati personali), cagionata dal dovere generico di conservare i dati di traffico e di localizzazione, non veniva limitata ai casi in cui questa fosse strettamente *necessaria* (ergo anche *proporzionata*). Sulla base di tale considerazione, G. CAGGIANO, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, in *Rivista di diritto dei media*, n. 2, 2018, p. 7, ha affermato che, al fine di effettuare il controllo della necessità della misura, i criteri di accesso ai dati da parte delle autorità pubbliche (i soggetti devono essere debitamente autorizzati, l'uso dei dati deve essere necessario, ecc.) devono essere sottoposti a controllo in ogni caso, implicando il requisito di indipendenza dell'autorità di garanzia; cfr. S. PEERS, The data retention judgment: The CJEU prohibits mass surveillance, in EU Law Analysis, 8 aprile 2014; F. VECCHI, *L'ingloriosa fine della direttiva Data retention, la ritrovata vocazione costituzionale della Corte di giustizia e il destino dell'art. 132 del Codice della privacy*, in *Diritti comparati*, 10 giugno 2014; F. FABBRINI, *Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States*, in *Harvard Human Rights Journal*, vol. 28, 2015, pp. 65-95.

interferenza dei diritti individuali che, attraverso la giurisprudenza[67], si è compreso regolare omnicomprensivamente il settore.

4.1. I rischi legati alla geometria variabile ed alla privatizzazione della giustizia nel Regolamento EPOC

I principi summenzionati sono frequentemente richiamati all'interno del Regolamento sull'ordine europeo di produzione e conservazione al fine di un esercizio appropriato dell'attività investigativa[68]. Tuttavia, non è pacifico se tali principi ricalchino realmente quelli interpretati dalla giurisprudenza europea e ne soddisfino le condizioni e requisiti.

In via preliminare, si è detto che il Regolamento (UE) 2023/1543 persegue l'ambizione di creare un quadro giuridico a livello dell'UE per la raccolta di prove elettroniche nel campo della procedura penale e di istituzionalizzare un nuovo paradigma di cooperazione in tale ambito. In base alle disposizioni ivi contenute, infatti, gli ordini in questione verranno trasmessi in forma di "certificati" ai *providers*/destinatari, che sono tenuti alla loro esecuzione. Si tratta pertanto di un contatto diretto tra l'autorità di emissione ed il privato, ovvero il gestore dei servizi/*provider* che, in definitiva, riceve un documento diverso dall'ordine stesso. Come si vedrà, invece, il contenuto di quest'ultimo sarà notificato dall'autorità di emissione alla competente autorità giudiziaria di esecuzione solo in ipotesi circoscritte.

L'emanazione degli ordini è sottoposta a specifici requisiti, ovvero se una misura dello stesso tipo sia disponibile per lo stesso reato all'interno dello Stato di emissione ("caso interno analogo", art. 5, par. 2; art. 6, par. 2).

Nel caso dell'ordine europeo di produzione del *traffico di dati*, è richiesto che il reato per cui l'individuo è indagato sia sufficientemente grave – deve essere pari ad almeno 3 anni nel massimo edittale della pena, o in alternativa essere uno tra i reati elencati al art. 5, par. 4 – da giustificare l'imposizione di una conversazione transfrontaliera dei dati. Tale soglia non è invece prevista per l'ordine europeo di produzione per *dati relativi agli abbonati o identificativi dell'utente* (art. 5, par. 3, "qualsiasi reato"), né per gli ordini di conservazione (art. 6, par. 3: "può essere emesso per tutti i reati").

Vieppiù, soltanto nell'ordine di produzione del *traffico di dati* – ma non già di produzione dei dati relativi agli abbonati o quelli al solo scopo di identificare l'utente – deve esser fatta indicazione dei motivi di proporzionalità e necessità dell'atto[69]. Diversamente, nel caso dell'ordine di conservazione, il requisito di indicazione dei motivi sulla necessità e proporzionalità è richiesto in ogni caso.

---

[67] Non a caso, nelle parole di J. DASKAL, *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues*, in *Journal of National Security Law & Policy*, 2016, n. 3, p. 484, nt. 41, si attesta che questi principi in generale "*reflect an inspirational view of what the law should be, rather than a statement of current binding law*".

[68] In particolare nell'art. 5, par. 2 ed art. 6, par. 2 del Regolamento.

[69] Art. 5, parr. 3 e 4, lett. i). Tuttavia, si consideri tale precisazione non è altresì richiesta nel certificato discendente dall'ordine.

Il combinato disposto esaminato darebbe in verità adito a "*practices that will have an unlawful impact*"[70], intrinsecamente irrispettose del principio di proporzionalità. Infatti, gli ordini europei di produzione distinguerebbero inappropriatamente tra differenti tipologie di dati personali, ammettendo una concessione *sproporzionata* dell'ordine per i livelli di *privacy* ritenuti inferiori dal Regolamento. Ciò avverrebbe sulla base dell'assunto, non verificato in alcun modo, che talune categorie di informazione siano meno sensibili di *default*[71], come nel caso dei dati su abbonati o sull'identificazione dell'utente[72], con la conseguente creazione di c.d. "geometrie variabili" di tutela. L'assenza dell'indicazione dei motivi di proporzionalità e necessità negli ordini di produzione che investono queste categorie di dati ha degli effetti significativi sulla possibilità di rifiuto degli stessi.

La prima conseguenza di tale differenziazione risiede nel diritto ad un controllo effettivo della misura adottata. Assai rilevante è la disposizione di cui all'art. 8 del Regolamento. Secondo il suo primo paragrafo, "qualora un ordine europeo di produzione sia emesso per ottenere dati sul traffico, fatta eccezione per i dati richiesti al solo scopo di identificare l'utente ai sensi dell'articolo 3, punto 10), o per ottenere dati relativi al contenuto" è disposta notifica dell'EPOC da parte dell'autorità di emissione a quella di esecuzione. Lo scopo della notifica è quello di consentire un controllo da parte dall'autorità di esecuzione ai sensi dell'art. 12[73]. Il medesimo articolo ammette infatti, tra i vari motivi, di rifiutare entro 10 giorni dalla notifica[74] l'esecuzione dell'ordine anche quando, "in situazioni eccezionali, sussistono validi motivi di ritenere, sulla base di elementi concreti e oggettivi, che l'esecuzione o l'applicazione dell'ordine comporterebbe, nelle particolari circostanze del caso, una violazione manifesta di un pertinente diritto fondamentale sancito dall'articolo 6 TUE e dalla Carta". Una violazione "manifesta"[75] implica che l'autorità di esecuzione è tenuta a fornire prove specifiche e

[70] M. STEFAN, G. GONZÁLEZ FUSTER, *op. cit.*, p. 50.
[71] Per maggiori informazioni afferenti questo aspetto, v. S. CARRERA, M. STEFAN, *Access to Electronic Data for Criminal Investigations Purposes in the EU*, in *CEPS Papers*, 2020, n. 1, pp. 1-73.
[72] Tale informazione non va sottovalutata poiché potrebbe coinvolgere soggetti potenzialmente sensibili come informatori, giornalisti investigativi, individui che protestano contro i governi nazionali, come notato da A. SACHOULIDOU, *Cross-Border Access to Electronic Evidence: Is There Any Light at the End of the Tunnel?*, in *Trace*, 1° febbraio 2023.
[73] Lo stesso articolo prevede infatti che il rifiuto è ammissibile "[q]ualora l'autorità di emissione abbia notificato l'autorità di esecuzione a norma dell'articolo 8".
[74] Termine ridotto a massimo 96 ore in caso di emergenze *ex* art. 10, par. 4 del Regolamento EPOC.
[75] Il termine è riconducibile al caso Corte di Giustizia, Grande Sezione, sentenza del 5 aprile 2016, *Aranyosi e Căldăraru* cause riunite C-404/15 e C-659/15 PPU, e all'interpretazione ivi contenuta dell'art. 23 della Decisione Quadro 2002/584/GAI del 13 giugno 2002, relativa al Mandato d'arresto europeo e alle procedure di consegna tra Stati membri, in GUUE L 190 del 18 luglio 2002, ove si fa riferimento al differimento eccezionale della consegna del ricercato "se vi sono valide ragioni di ritenere che essa metterebbe manifestamente in pericolo la vita o la salute del ricercato". Sul rapporto tra Mandato d'arresto europeo e Stato di diritto, si rimanda ad A. DI STASI, A. FESTA, *Breaches of the Rule of Law in the EU: What Implications for the Principle of Mutual Trust in the Area of Freedom, Security and Justice?*, in T. RUSSO, A. ORIOLO, G. DALIA (eds.), *Solidarity and Rule of Law. European Union and Its Neighbours in a Globalized World*, vol. 9, Cham, 2023, pp. 153-171.

oggettive che dimostrino che esistono fondati motivi per ritenere che l'ordine violi indebitamente un diritto fondamentale.

Sempre con riguardo al controllo preventivo di cui al combinato disposto degli artt. 8 e 12 del Regolamento, viene anche in considerazione che, nel notificare l'EPOC all'autorità di esecuzione, l'autorità di emissione include solamente "se del caso"[76], così riducendo quelle informazioni supplementari eventualmente necessarie per un motivo di rifiuto.

Da come risulta evidente, il Regolamento prevede al suo art. 8, par. 1, in modo *esclusivo*, l'obbligo di notifica per il solo ordine europeo di produzione del traffico di dati. Ma tale previsione renderebbe, in tutti i rimanenti casi, fattivamente impossibile il controllo (e rifiuto) dell'ordine a norma dell'art. 12[77]. Verrebbe meno un importante strumento di tutela dei diritti fondamentali, tra l'altro espressamente considerati nel dettato legislativo dell'art. 12 del Regolamento[78]. Di conseguenza, gli ordini di produzione dei dati sugli abbonati e sull'identificazione dell'utente, nonché indifferentemente tutti gli ordini di conservazione, non potranno beneficiare di forme di controllo *ex ante* così come richieste dalla giurisprudenza CGUE[79]. Sottraendosi ad un esame del rispetto della proporzionalità e necessità in questi casi (che pure dovrebbero essere descritte nell'ordine di conservazione *ex* art. 6 del Regolamento a differenza di quello di produzione di dati su abbonati e degli ID), viene data vita ad una forma di presunzione di proporzionalità della misura imposta.

Inoltre, l'art. 8, par. 2 descrive talune eccezioni per le quali, quando l'autorità di emissione "abbia fondati motivi di ritenere" che "il reato sia stato commesso, sia in atto o sia suscettibile di essere commesso nello Stato di emissione" o che "la persona i cui dati sono richiesti risieda nello Stato di emissione", l'obbligo di notifica viene meno anche là dove (marginalmente) previsto dal par. 1. Ne deriva che, in particolare, l'eccezione disposta sulla residenza nello Stato d'emissione sia fortemente discrezionale ("ritenere") senza che altre autorità possano verificarne la fondatezza, dato che non riceveranno nessuna notifica. In questo modo, l'assenza di controllo preventivo e la citata presunzione di proporzionalità e necessità risulterebbero ancor più estese, aggravando il quadro della tutela individuale.

Tuttavia, quale contro-argomento, va anche rammentato che il soddisfacimento della "proporzionalità della misura" o "del meccanismo di cooperazione" non coincide automaticamente con il riconoscimento della "proporzionalità e necessità

[76] Art. 8, par. 3 Regolamento EPOC.
[77] Tra l'altro, C. BERTHÉLÉMY, "*E-Evidence" Trilogues: What's Left of Fundamental Rights Safeguards?*, in *EDRi*, 22 novembre 2022, nota che l'art. 8 rimanga colpevolmente silente sul riutilizzo delle medesime informazioni recuperate per mezzo di EPOC da parte dell'autorità emittente, che potrebbe cederle ad altre autorità senza dover disporre notifica di ciò.
[78] Ciò è anche conseguenza della preferenza verso l'autorità d'emissione come centro delle operazioni, ridimensionando il ruolo dell'autorità giudiziaria dello Stato in cui l'esecuzione è richiesta. Tra coloro che hanno criticato tale preferenza predicando un ritorno a meccanismi fondati sul mutuo riconoscimento tradizionale, figura M. CORHAY, *It Is a Long Way to… E-Evidence: EU Reforms in the Collection of Electronic Evidence*, in *Information Law and Policy Centre*, 24 gennaio 2023.
[79] Corte di Giustizia, Grande Sezione, *HK Prokuratuur*, cit., parr. 32-45 e 51.

dell'interferenza", così come intese nei criteri di bilanciamento di cui all'art. 52 CDFUE. Da ciò ne deriva che il Regolamento non è esentato dal rispetto della Carta di Nizza (come del resto richiamato nel suo art.1, par. 3) e che, pertanto, anche in caso di presunzione di proporzionalità, forme di controllo sull'effettiva interferenza dei diritti non possono essere limitate nemmeno in via eccezionale.

Senz'altro va anche riconosciuto che il Regolamento, segnatamente al proprio art. 17, prevederebbe il diritto per gli imputati ed indagati ad un ricorso effettivo *successivo* contro l'ordine di produzione o conservazione ("Procedura di riesame"). Tale ricorso, nell'ambito del procedimento penale di riferimento nello Stato d'emissione, verrebbe presentato "dinanzi a un organo giurisdizionale dello Stato di emissione in conformità al diritto nazionale di tale Stato e include la possibilità di contestare la legittimità della misura, comprese la sua necessità e la sua proporzionalità, fatte salve le garanzie dei diritti fondamentali nello Stato di esecuzione"[80]. Esso potrebbe soddisfare il requisito di avere a disposizione un "*effective control*", qui *ex post*, fissato dalla sentenza *Szabo e Vissy*[81], ma il rischio precedentemente prospettato non sembra superato. Il diritto di presentare ricorso da parte del soggetto interessato suggerisce che la (potenziale) violazione dei diritti fondamentali si sia già materializzata, evadendo la logica di un controllo preventivo[82] di ampia tutela in favore del soggetto implicato in un procedimento penale. Inoltre, l'art. 17 del Regolamento EPOC configura un'iniziativa dell'interessato piuttosto che un mezzo di controllo d'ufficio, magari automatico, instaurato tra l'autorità di emissione e di esecuzione.

Il meccanismo proposto pertanto condurrebbe ad una doppia (eventualmente ingiustificata) limitazione di diritti: 1) da una parte, in via primaria, vi sarebbe la limitazione dei diritti di *privacy* e protezione dei dati quale diretto effetto degli ordini di produzione e/o conservazione; 2) d'altra parte, verrebbe limitata la disponibilità dei mezzi utili a *prevenire* eventuali abusi dei diritti di cui al punto precedente, mentre i mezzi di ricorso *successivo* potrebbero considerarsi *sufficienti*. Si tratterebbe dunque della limitazione del diritto a prevenire un danno in presenza di una misura sproporzionata o innecessaria piuttosto che ottenere una riparazione solo dopo che questo sia stato cagionato. Inoltre, il controllo preventivo esistente, è bene ricordare, risulta menomato dalla possibilità di omettere, in maniera discrezionale ("se del caso" *ex* art. 8, par. 3), alcune informazioni – per definizione del Regolamento – supplementari. In definitiva, il quadro afferente al controllo (*ex ante* o *ex post* che sia) sull'esistenza di una misura pienamente proporzionata o necessaria non sembra pienamente soddisfacente, rivelando un eccessivo sbilanciamento in favore dell'autorità di emissione.

E tutto ciò rischia di andare in contrasto contro parte della giurisprudenza della CGUE, quale ad esempio la sentenza *Tele2Sverige*. Tant'è che, con riguardo alla Direttiva

[80] Art. 18, par. 2 Regolamento EPOC, in ciò si configura un parallelismo con l'OEI, v. art. 11, par. 1, lett. f) della Direttiva 2014/41/UE, cit.
[81] Corte europea dei diritti dell'uomo, Quarta Camera, *Szabo e Vissy*, cit., par. 77.
[82] Naturalmente, in questo caso, da parte delle autorità competenti siccome si assume che il soggetto interessato non sia già al corrente delle indagini.

2002/58/CE, relativa alla vita privata e alle comunicazioni elettroniche[83] in essa venne stabilita la fondamentale regola per cui la conservazione di dati *esige* che essa abbia luogo soltanto "quando ciò sia giustificato da uno degli obiettivi previsti dall'articolo 15, paragrafo 1, prima frase, della [Direttiva 2002/58/CE]" ovvero, in qualità di regola generale, si dovrà produrre "una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica".

Tra l'altro, i dati non sono sempre da considerarsi correlati alla tutela della sicurezza nazionale. Pertanto, quando evidentemente non lo sono, non è nemmeno possibile ammettersi l'eccezione di presunta proporzionalità prevista nel caso *HK Prokuratuur*[84], ovvero che i criteri di necessità e la proporzionalità si considerano soddisfatti a prescindere con riguardo ai dati esteriori quando risultano coinvolti interessi securitari nazionali.

In definitiva, è doveroso menzionare l'idea per la quale, in forza di questa categorizzazione normativa, "*practice confusion may arise from the distinction between access data and transaction data*"[85], con una conseguente non-operabilità, o perfino abuso, di questa lamentevole differenziazione. Infatti, la distinzione tra i vari tipi di dati non è sempre univoca e ciò potrebbe portare alla limitazione di importanti garanzie per l'individuo laddove, per esempio, un ordine di produzione formalmente volto ad ottenere i dati degli utenti abbonati – che dà molte meno garanzie all'individuo – richieda nella sostanza anche informazioni sul traffico di dati.

Di converso, mentre nel Regolamento la tutela dell'individuo ha contorni flebili, la tutela delle prerogative Statali appare ben salda[86]. Lo stesso coinvolgimento, quando previsto, dell'autorità d'esecuzione rivelerebbe ragioni di protezione delle aspettative di tutela della sovranità dello Stato d'esecuzione piuttosto che di concreta tutela dell'individuo[87].

In forza dell'ampio coinvolgimento dei privati, altre criticità si ricollegano all'allontanamento dal paradigma tradizionale del mutuo riconoscimento e della mutua

---

[83] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, *relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche*, 12 luglio 2002, in GUUE L 201 del 31 luglio 2002.

[84] Corte di Giustizia, Grande Sezione, *HK Prokuratuur*, cit., parr. 35-50.

[85] M. ROJSZCZAK, *op. cit.*, p. 1007.

[86] Ai sensi dell'art. 5, par. 10 Regolamento EPOC: "[l]'autorità di emissione non emette un ordine europeo di produzione se ritiene che i dati richiesti relativi al traffico, ad eccezione dei dati richiesti al solo scopo di identificare l'utente quali definiti all'articolo 3, punto 10), o i dati relativi al contenuto siano protetti con immunità o privilegi riconosciuti dal diritto dello Stato di esecuzione, o che tali dati siano soggetti in detto Stato a norme in materia di determinazione e limitazione della responsabilità penale relative alla libertà di stampa e alla libertà di espressione in altri mezzi di comunicazione".

[87] M. LASSALLE, *Existe-t-il des garanties européennes relatives à la protection de la vie privée dans le Cadre de l'enquête pénale?*, in *European Papers*, vol. 6, n. 1, 2021, pp. 412: "*Les autres dispositions et motifs de refus* […] *ont pour seul objectif de protéger les principes classiques de la souveraineté des États, les intérêts des États members*".

fiducia tra autorità giudiziarie[88]. Del resto, vi è chi ha cercato di comprendere se gli ordini qui in analisi potrebbero essere concettualizzati come un nuovo tipo di strumento di cooperazione giudiziaria, ove cioè si supererebbe il paradigma della cooperazione tra "autorità" competenti degli Stati Membri, o come un nuovo sottotipo o categoria di strumento di mutuo riconoscimento[89]. In particolare, sarebbe da escludere la configurabilità come strumento di cooperazione giudiziaria in quanto "[u]*nder existing mutual recognition instruments decisions need to come from a judicial (or equivalent) authority in the issuing state and their execution requires the prior involvement of a judicial authority in the Member State where the addressee or the object concerned by the measure is located*" ed il mero coinvolgimento della sola autorità emittente non è sufficiente a tutelare l'interessato da un'indebita violazione di diritti fondamentali[90].

Si pensi al contenuto dell'art. 10, par. 5, per il quale il privato dispone della facoltà di non fornire le informazioni richieste, comunicandone i motivi l'autorità di emissione e di esecuzione "sulla base delle sole informazioni contenute nell'EPOC, che l'esecuzione dell'EPOC possa interferire con le immunità o i privilegi o con le norme sulla determinazione o la limitazione della responsabilità penale relative alla libertà di stampa o alla libertà di espressione in altri mezzi di comunicazione, a norma del diritto dello Stato di esecuzione". L'autorità di emissione riesaminerà l'ordine alla luce delle informazioni fornite dal prestatore di servizi e, laddove necessario, fisserà a quest'ultimo un nuovo termine per la produzione dei dati. Risulta tuttavia evidente che l'individuazione di tali "interferenze" sia assai difficile per il *provider* – il quale non disporrà dell'ordine, bensì del certificato, che si qualifica come un atto non completo a livello contenutistico[91].

Quando, invece, un certificato si presenti come potenzialmente ingiustificato, laddove sia "incompleto o contiene errori manifesti o informazioni insufficienti per eseguirlo"[92], il destinatario provvederà ad inviare un apposito modulo contenente una richiesta di chiarimenti rivolta all'autorità di emissione e, se vi è stata una notifica di esecuzione *ex* art. 8, ne informerà anche l'autorità di esecuzione.

Naturalmente, il requisito, tutt'altro che presumibile, è che in ogni caso il privato abbia la concreta capacità di individuare gli aspetti patologici del certificato pervenutogli

---

[88] Su cui, ad esempio, ha riflettuto S. TOSZA, *Mutual Recognition by Private Actors in Criminal Justice? Service Providers as Gatekeepers of Data and Human Rights Obligations*, 19 settembre 2019.

[89] Á. TINOCO PASTRANA, *Las órdenes europeas de entrega y conservación: la futura obtención transnacional de la prueba electrónica en los procesos penales en la unión europea*, in *Cuadernos de política criminal*, n. 135, 2021, p. 210 e 245: "*La peculiar reinterpretación del principio de reconocimiento mutuo que se incorpora en las versiones iniciales de la propuesta de Reglamento, con la ejecución directa de las órdenes por los representantes legales de los proveedores de servicios, nos hace plantearnos si realmente estamos ante un instrumento de esta índole*".

[90] M. STEFAN, G. GONZÁLEZ FUSTER, *Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters. State of the art and Latest Developments in the EU and the US*, in *CEPS Papers*, n. 7, 2018, p. 28.

[91] Art. 9 Regolamento EPOC.

[92] Art. 10, par. 6 Regolamento EPOC. Per un commento sull'efficacia di questo articolo, cfr. L. MOXLEY, *EU Releases e-Evidence Proposal for Cross-Border Data Access*, in *Inside Privacy*, 8 maggio 2018; V. FRASSEN, *The European Commission's E-Evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?*, in *European Law Blog*, 12 ottobre 2018.

("ritenga", *ex* art. 10, par. 5), in particolare quando il documento sia irrispettoso di specifici diritti oppure incompleto. Il risultato è che il "controllo" da parte dell'autorità competente attivato dal destinatario del certificato non sia la regola, ma una mera eventualità legata alla capacità tecnico-giuridica del destinatario stesso[93]. Ulteriormente, tale tipo di meccanismo di verifica non rientrerebbe nemmeno in un'ipotesi di controllo ai sensi della sentenza *Szabo e Vissy* della Corte EDU: il controllo (qui *ex ante*, tra l'altro) scaturirebbe da una richiesta formale del *provider*/destinatario e non già costituirebbe un'azione d'ufficio preordinata per la garanzia dell'indagato o imputato. Ma, se pure per assurdo questa fosse considerata una piena forma controllo, essa mancherebbe dei requisiti effettività e di indipendenza dell'autorità di controllo, pure richiesti dal punto 77 della sentenza *Szabo e Vissy*[94].

Sebbene in forma più moderata rispetto alla Proposta originale[95], l'Unione europea, dunque, starebbe in questa sede autorizzando il privato – un soggetto inadatto a livello tecnico, non necessariamente competente e prevedibilmente non imparziale – a prendere una decisione sull'invio del modulo di segnalazione. Decisione che potrebbe essere non presa per mero timore delle sanzioni in cui il privato potrebbe incorrere in caso di non esecuzione[96]. Si tratta di una decisione non priva di significato in quanto dalla sua presenza o assenza può derivare una lesione dei diritti fondamentali di un altro individuo, come si è intuito dalla lettera dell'art. 10. Tale disposizione lascia tra l'altro trasparire l'aderenza del legislatore europeo a quella tendenza di privatizzazione e decentramento della tutela dei diritti fondamentali diffusasi dopo l'approvazione del GDPR[97].

---

[93] Né, guardando alla Direttiva (UE) 2023/1544 – attinente alla designazione di stabilimenti designati ed alla nomina di rappresentanti legali ai fini dell'acquisizione di prove elettroniche nei procedimenti penali – vengono individuati requisiti di capacità tecnica imposti al soggetto responsabile. La Direttiva, del resto, serve il mero scopo di individuare quei soggetti di contatto per le autorità, tenuti a subire le opportune sanzioni in caso di non rispetto di un EPOC o di un OEI.

[94] Certamente un'obiezione che si può qui muovere è che i presupposti fattuali della *Szabo e Vissy* sono diversi, ovvero la sorveglianza segretata e generale, mentre qui il provvedimento è individualizzato e sarà successivamente reso noto all'indagato in caso di azione penale.

[95] Nella Proposta il privato avrebbe addirittura dovuto verificare l'aderenza del certificato (e non già dell'ordine, che non perverrebbe in ogni caso) rispetto alla Carta dei diritti fondamentali dell'Unione europea.

[96] Art. 15 Regolamento EPOC. In effetti, la funzione eccessivamente deterrente delle sanzioni è stata sottolineata dal Garante europeo della protezione dei dati, *EDPS Opinion on Proposals Regarding European Production and Preservation Orders for Electronic Evidence in Criminal Matters*, Opinione 7/2019, par. 66; e, per la società civile, da European Digital Rights, *Recommendations on Cross-Border Access to Data Position Paper on the European Commission's Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters*, 25 aprile 2019, pp. 7, 17 e 25.

[97] In tal senso, v. *ex multis* A. ROSANÒ, *La "privatizzazione" nello spazio di libertà, sicurezza e giustizia: tre esempi per una tendenza*, in *Il Diritto dell'Unione europea*, 2020, n. 1, pp. 179-220; V. MITSILEGAS, *The Privatisation of Mutual Trust in Europe's Area of Criminal Justice: The Case of E-Evidence*, in *Maastricht Journal of European and Comparative Criminal Law*, 2018, n. 3, pp. 263-265. Un ulteriore esempio della privatizzazione della tutela dei diritti promanata dal GDPR è la decisione *Google Spain SL*, ove veniva specificato che i motori di ricerca – aldilà della Direttiva *e-commerce*, che ha disposto una serie di esenzioni in favore dei gestori di servizi online – devono essere considerati a tutti gli effetti "*data controllers*". Pertanto, essi sono tenuti all'adeguamento nei confronti della legislazione sulla protezione dei dati, nonché al controllo dei dati indicizzati presso i propri motori di ricerca: Corte di Giustizia, Grande Sezione, sentenza del 13 maggio 2014, *Google Spain SL e Google Inc. c. Agencia Española de Protección*

In conclusione, il Regolamento EPOC si presenta come un atto che riesce nel suo intento di velocizzare l'implementazione di misure di produzione e conservazione dei dati, ma che, per motivi di economia procedimentale e speditezza, sacrifica i diritti fondamentali dell'indagato o imputato in ragione di una propria "geometria variabile" arbitraria e di una chiara privatizzazione. Ripercuotendosi tali aspetti sulla facoltà di beneficiare di un controllo preventivo diffuso – che in sostanza non è sempre ammesso, bensì condizionato dall'esistenza dell'obbligo di notificazione preventiva, non sempre riconosciuto – il Regolamento tende a contrapporsi alla pregressa giurisprudenza della CGUE e della Corte EDU in materia. Infatti, sebbene formalmente l'atto richieda che le misure disciplinate da sé debbano sempre essere proporzionate e necessarie, l'assenza in molti casi di forme di controllo preventivo su tali requisiti comporta l'impossibilità di verifica *ex ante* di tali requisiti – ciò a detrimento del cittadino ed in contraddizione con importanti assiomi creati dalla prassi delle corti.

Pertanto, a partire dal 18 luglio 2026 (data di entrata in vigore del Regolamento) potrebbe essere futuribile un'attività correttiva da parte della giurisprudenza europea. Di converso, viene comunque fatta salva la possibilità che in questi tre anni vi sia invece un ulteriore ampliamento della "tolleranza" mostrata verso l'impiego di misure per la produzione e conservazione della prova elettronica, ricomponendo la frattura qui prospettata[98].

4.2. Il Secondo Protocollo alla Convenzione sulla criminalità informatica: uno strumento incoerente e (già) obsoleto?

Nel novero dei dubbi che sorgono circa il quadro normativo presente e futuro è possibile esaminare con attenzione il Secondo protocollo alla Convenzione di Budapest, quale espressione del *hard law* promanata dal Consiglio d'Europa. Innanzitutto, con riguardo all'accesso a dati relativi al contenuto presso un'altra nazione[99], è l'art. 18 ("*Production order*)" della Convenzione del 2001 a disporre che un altro Stato Parte possa "*access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system*".

de Datos (AEPD) e Mario Costeja González, causa C-131/12, par. 38. Per degli spunti di riflessione sulla sentenza cfr. R. PALLADINO, *Sul diritto all'oblio e la tutela dei diritti fondamentali in internet: ambito di applicazione territoriale e bilanciamento a margine della sentenza Google LLC della Corte di giustizia dell'UE*, in *I Diritti dell'Uomo*, 2019, n. 1, pp. 543-562; G. DE GREGORIO, *The E-Commerce Directive and GDPR: Towards Convergence of Legal Regimes in the Algorithmic Society*?, in *Robert Schuman Centre for Advanced Studies Research Paper*, 2019, n. 36, pp. 1-13.

[98] Come sostanzialmente verificato nell'analisi sulla sorveglianza di massa condotta da parte di M. NINO, *La normalizzazione della sorveglianza di massa*, cit.

[99] Al contrario, al di fuori di situazioni transfrontaliere, la Convenzione al suo *ex* art. 18, par. 1, lett. a), stabilisce che nelle ipotesi di situazioni interne l'ordine di produzione dei dati possa essere ammesso sempre, ma solo con riguardo a dati relativi al contenuto.

Dunque, quale prodotto di "*a direct cooperation and widened access rights*"[100] tra privato e autorità, il soggetto legalmente autorizzato alla *disclosure* dei dati – generalmente il gestore dei servizi telematici – dovrebbe fornire il proprio consenso alle richieste avanzate caso per caso dalle pubbliche autorità competenti. Evidentemente anche in questo caso si sottende una competenza tecnico-giuridica della materia da parte del gestore, la quale è assolutamente non scontata. Si ripresenta, in altre parole, l'idea di privatizzazione della giustizia e dei problemi suesposti riguardo il Regolamento EPOC.

Quanto al Secondo protocollo alla Convenzione, del 2021, si è detto che questo mira al rafforzamento a tutto tondo della cooperazione e divulgazione delle prove elettroniche.

Per quanto concerne gli Stati Membri dell'Unione europea, tale Protocollo non potrà essere applicato nell'ambito della disciplina regolata già dal diritto dell'Unione. Nonostante la ridotta portata applicativa in questi specifici casi, l'atto troverà comunque applicazione in trasferimenti realizzati tra Stati Membri dell'UE (nonché parte del Secondo Protocollo) e Stati terzi.

Tuttavia, nei confronti di quegli scenari futuri derivanti dall'applicazione del Protocollo, il Parlamento europeo ha espresso serie preoccupazioni sui lavori portati avanti dal Comitato competente per la Convenzione di Budapest, tale che lo sviluppo del Protocollo aggiuntivo porti con sé "rischi e sfide che il *cloud computing* comporta per i diritti fondamentali", aggiungendo la necessità che il Consiglio d'Europa debba "garantire la compatibilità delle disposizioni dell'articolo 32 della convenzione sulla criminalità informatica [relativo all' 'accesso transfrontaliero ai dati informatici archiviati previo consenso o quando sono pubblicamente disponibili'], così come la sua interpretazione negli Stati membri, con i diritti fondamentali, compresa la protezione dei dati e, in particolare, le disposizioni sui flussi transfrontalieri di dati personali" [101].

Sebbene lo stesso Secondo Protocollo converga verso la legislazione dell'Unione (segnatamente verso il GDPR) per quanto concerne alcune sue istanze[102], tali preoccupazioni sembrerebbero essersi riflesse nel suo contenuto effettivo. Anticipando la possibilità che nazioni al di fuori del Consiglio d'Europea potessero divenirne parte, i redattori del Protocollo hanno preferito non stabilire in esso una concezione rigida della proporzionalità e necessità delle misure, disponendo che questi principi saranno *interpretati* dagli Stati Parte secondo l'*acquis* del Consiglio d'Europa[103]. In ragion di ciò, l'art.13 del Secondo Protocollo – sulla base dei contenuti dell'art. 15 della Convenzione

[100] S. DEPAUW, *op. cit.*, p. 72. L'autore precisa che in tale previsione esistono specifiche problematiche attinenti alla corretta localizzazione dei dati, ovvero della nazione in cui chiederne la produzione, in quanto essa non è sempre "*self-evident*", come pure la legalità della condotta tenuta dal gestore di servizi "*from a data protection point of view*".

[101] Risoluzione del Parlamento europeo *sullo sfruttamento del potenziale del cloud computing in Europa*, 2013/2063(INI), del 10 dicembre 2013, parr. 72-73

[102] M. BUCCARELLA, *Digitalizzazione della cooperazione giudiziaria internazionale in materia penale e tutela dei dati personali nel diritto UE: alla ricerca di una compatibilità (im)possibile*, in questa *Rivista*, n. 2, 2023, p. 226, nota come, circa eventuali incidenti di sicurezza, l'art. 14, par. 7 del Secondo Protocollo disponga un obbligo di comunicazione alle competenti Autorità nazionali ed agli interessati. Tuttavia, l'obbligo di comunicazione lascia spazio ad un'eccezione "che solleva non pochi interrogativi" in ipotesi di rischi per la sicurezza nazionale a fronte della difficile definizione di questo concetto.

[103] *Explanatory Memorandum to the Draft Second Additional Protocol*, n. 80, par. 84, lett. c.

sulla criminalità informatica – stabilisce che "*each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Protocol are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties*".

Dunque, peculiare attenzione è data alle "*conditions and safeguards*" presenti nell'ordinamento interno del singolo Stato Parte. Siccome le misure adottate in forza del Secondo Protocollo (regolate dal Capo II) con tutta probabilità implicheranno il trasferimento di dati, garanzie e tutele *ad hoc* dovranno essere previste dal diritto interno a livello costituzionale (o comunque derivate dal diritto internazionale adeguato nell'ordinamento nazionale). Difatti è il Capo III, al suo art. 14, che richiede in maniera espressa agli Stati Parti di intraprendere tali accorgimenti, preparando gli ordinamenti interni alla corretta applicazione dell'intero Protocollo.

In particolare, ai sensi dell'art. 14, par. 1, lett. a), ciascuna Alta Parte contraente è tenuta ad eseguire il trattamento dei dati ottenuti in virtù del Secondo Protocollo nel rispetto di garanzie individuate espressamente nei paragrafi 2-15 dello stesso articolo. Tra queste forme di tutela figurano la necessità di garantire la proporzionalità e la necessità nel mantenimento dell'integrità e veridicità dei dati allo scopo di far beneficiare l'indagato di un trattamento dei propri dati che sia pienamente legittimo[104]. Viene altresì richiesto di identificare pedissequamente i dati sensibili[105], predisporre rimedi giudiziali in favore dell'indagato[106] e di ricreare dei meccanismi di controllo[107]. Eppure, i parr. 2-15 ed i principi di salvaguardia in essi contenuti non sempre saranno soggetti ad applicazione: talune eccezioni, dettagliate nell'art. 14, par. 1, lett. b e c, sono infatti ammissibili.

E, in verità, una di queste spicca nettamente sulle altre, dal momento che le tutele e garanzie imposte dall'art. 14 non sono considerate perentorie laddove lo Stato Parte richiedente e quello di appartenenza del soggetto richiesto siano "*mutually bound by an international agreement that establishes a comprehensive framework between those Parties for the protection of personal data*"[108].

---

[104] Art. 14, par. 3 Secondo Protocollo: "*Each Party shall take reasonable steps to ensure that personal data are maintained with such accuracy and completeness and are as up to date as is necessary and appropriate for the lawful processing of the personal data, having regard to the purposes for which they are processed*".

[105] Art. 14, par. 4 Secondo Protocollo: "*Each Party shall retain the personal data only for as long as necessary and appropriate in view of the purposes of processing the data pursuant to paragraph 2. In order to meet this obligation, it shall provide in its domestic legal framework for specific retention periods or periodic review of the need for further retention of the data*".

[106] Art. 14, par. 13 Secondo Protocollo.

[107] Art. 14, par. 14 Secondo Protocollo: "*Each Party shall have in place one or more public authorities that exercise, alone or cumulatively, independent and effective oversight functions and powers with respect to the measures set forth in this article. The functions and powers of these authorities acting alone or cumulatively shall include investigation powers, the power to act upon complaints and the ability to take corrective action*".

[108] Più precisamente, l'art. 14, par. 1, lett. b., chiarisce che "[i]*f at the time of receipt of personal data under this Protocol, both the transferring Party and the receiving Party are mutually bound by an international agreement establishing a comprehensive framework between those Parties for the protection of personal data, which is applicable to the transfer of personal data for the purpose of the prevention, detection,*

Tali accordi di settore potranno dunque applicarsi a richieste di "*law enforcement*"[109], divenendone la base normativa principale in luogo del Protocollo stesso. È lo stesso Consiglio d'Europa, nell'*Explanatory Report*, a fornire degli esempi di tali accordi "sostitutivi", riferendosi alla Convenzione 108+ e al c.d. *Umbrella Agreement* tra USA e UE[110].

Ci si dovrebbe, in ogni caso, interrogare sulla natura del "*comprehensive framework*" citato nella disposizione. Un quadro giuridico dovrebbe essere considerato "*comprehensive*" quando in maniera piena ed estesa disciplini la tutela dei dati in caso di trasferimenti di questi – offrendo garanzie in modo omnicomprensivo, come nel caso del quadro giuridico dell'UE. Per le richieste tra due Stati Membri dell'Unione (ambedue già parti del Secondo Protocollo), il diritto UE potrà e dovrà sicuramente applicarsi nei procedimenti di cooperazione giudiziaria in quanto, per effetto della sentenza *Privacy International* si apprende che "i trattamenti di dati personali effettuati a questi stessi fini da privati rientrano nell'ambito di applicazione di quest'ultimo"[111]. Specificamente, ciò dovrebbe accadere anche in ipotesi di applicazione del Secondo Protocollo all'art. 18 della Convenzione di Budapest, sulla collaborazione diretta con i privati. Ci si deve chiedere invece quale sia il diritto da applicarsi in caso di rapporto tra Stato Membro UE e Stato Terzo (anche qui entrambi Alte Parti del Protocollo), in particolar modo chiedendosi se degli accordi di settore possano disapplicare il Secondo Protocollo *ex* art.14, par. 1, lett. b. Il Consiglio dell'Unione europea fortunatamente ha parzialmente fugato questo dubbio, esprimendosi nello specifico sull'*Umbrella Agreement* e sul suo rapporto con il Secondo Protocollo. Dando rassicuranti garanzie, il Consiglio ha manifestato la piena applicabilità dell'*Agreement* nei soli rapporti volti al trasferimento di dati personali tra autorità giudiziarie, sancendo invece la prevalenza del Secondo Protocollo alla Convenzione di Budapest laddove il trasferimento sia richiesto a privati. Viene tuttavia fatta salva la possibilità di aggiornare l'*Umbrella Agreement* di modo che possa coprire anche tali circostanze[112].

---

investigation and prosecution of criminal offences, and which provides that the processing of personal data under that agreement complies with the requirements of the data protection legislation of the Parties concerned, the terms of such agreement shall apply, for the measures falling within the scope of such agreement, to personal data received under the Protocol in lieu of paragraphs 2 to 15, unless otherwise agreed between the Parties concerned".

[109] *Explanatory Report*, cit. par. 222, versione 2021, https://rm.coe.int/0900001680a2aa1c.

[110] Il quale sostituisce il ben noto *Privacy Shield*, dichiarato invalido nel luglio 2020 (sentenza *Schrems II*). L'accordo provvede a "*enable predictable and trustworthy data flows between the EU and US, safeguarding privacy and civil liberties*" nelle parole del Presidente della Commissione europea, Ursula von der Leyen.

[111] *Privacy International*, cit., par. 47.

[112] Decisione (UE) 2022/722 del Consiglio, *che autorizza gli Stati membri a firmare, nell'interesse dell'Unione europea, il secondo protocollo addizionale alla Convenzione sulla criminalità informatica riguardante la cooperazione rafforzata e la divulgazione di prove elettroniche*, del 5 aprile 2022, in GUUE L 134 dell'11 maggio 2022, pp. 15-20, Allegato, par. 4; Decisione (UE) 2023/436 del Consiglio, *che autorizza gli Stati membri a ratificare, nell'interesse dell'Unione europea, il secondo protocollo addizionale alla Convenzione sulla criminalità informatica riguardante la cooperazione rafforzata e la divulgazione di prove elettroniche*, del 14 febbraio 2023, in GUUE L 63 del 28 febbraio 2023, pp. 48-53, Allegato, par. 4.

Ad ogni modo, rendendo il testo fraintendibile, l'art. 14, par. 1, lett. b del Secondo Protocollo non fa un riferimento esplicito ad un vero e proprio requisito di *compliance* agli standard diritto dell'Unione europea, né forse avrebbe potuto in quanto vi era la speranza di far aderire Stati extra-UE ed extra-europei. Ma l'eccezione all'applicazione delle garanzie del Protocollo avrebbe quantomeno dovuto riferirsi direttamente alla Convenzione 108+[113], che pure figura come un esempio nell'*Explanatory Report*. E, ancora, avrebbe potuto imporre agli Stati Parti l'adesione alla citata Convenzione per assicurare che l'eccezione profilata non scada in un "via libera" per qualsiasi parte contraente. Tant'è che l'assenza di riferimenti normativi precisi, ovvero in cosa debba consistere questo "*comprehensive framework"*, potrebbe culminare in una pluralità di Stati Parti impegnati nella stipula di bilaterali[114] allo scopo di eludere le garanzie di proporzionalità e necessità altrimenti imposte dai parr. 2-15 dell'art. 14. Pertanto, ciò rende possibile ad uno Stato Membro dell'Unione europea di provvedere alla formazione di accordi che consentano l'immediato trasferimento e la conservazione dei dati *per qualsiasi reato e per qualsiasi esigenza* in essi previsa. In tal senso, limitandosi ad offrire garanzie e rimedi meramente formali, nonché omettendo i requisiti previsti dal Protocollo, la proporzionalità e la necessità rischierebbero di essere qui ampiamente presunte. Eppure, quella della presunzione di proporzionalità e di necessità costituisce un'eccezione, come desunto dalla sentenza *HK Prokuratuur* e dal correlato filone giurisprudenziale della CGUE[115]. Essa non può rappresentare la regola, magari prevista da un accordo bilaterale di settore.

Similmente, dal lato dello stesso Consiglio d'Europa, la sentenza *Big Brother Watch* della Corte EDU ha autorizzato la sorveglianza di massa in virtù dell'esigenza di sicurezza pubblica. La sentenza, come detto in precedenza, conferma quel paradigma per cui un'interferenza nei diritti umani è ammissibile (addirittura compatibile con la CEDU) quando giustificata da ragioni preminenti, come nel caso della pubblica sicurezza. Ci si chiede pertanto se gli accordi bilaterali, futuribili a dispetto delle garanzie che sarebbero invece state applicate dai parr. 2-15 dell'art. 14, siano effettivamente pronti a rispettare tale paradigma oppure, *a contrario*, legittimare una cooperazione giudiziaria indiscriminata, anche per ragioni "poco alte", ovvero per qualsiasi tipo di reato e qualsiasi tipo di lesione di beni giuridici tutelati[116].

---

[113] Per una panoramica sulla Convenzione in parola si rimanda a G. NADDEO, *Giornata europea della protezione dei dati: la Convenzione 108 compie 40 anni*, in *Iusinitinere*, 28 gennaio 2021.

[114] M. ROJSZCZAK, *op. cit*., p. 1018: "*the Protocol will not result in the establishment of a new, uniform international standard in the field of criminal cooperation, but will lead instead to the creation of many bilateral rules for making electronic evidence available, built on a common framework resulting from the Protocol*".

[115] Corte di Giustizia, Grande Sezione, *HK Prokuratuur*, cit., parr. 35-50; Corte di Giustizia, Grande Sezione, *SpaceNet*, cit. parr. 72-74, 92-106 e 131; Corte di giustizia, Grande Sezione, *Commissioner of An Garda Siochana*, cit.

[116] Secondo M. BUCCARELLA, *op. cit*, p. 231, esisterebbe comunque "un certo grado di vaghezza" che renderebbe le disposizioni di cui all'art. 14 non compatibili con la normativa UE (v. Corte di Giustizia, Grande Sezione, Parere del 26 luglio 2017, 1/15, cfr. M. LEFFI, *L'Accordo PNR tra Canada e UE non prende il volo. Nota sul parere della Corte di giustizia europea a proposito del trasferimento dei dati del codice di prenotazione*, in *Medialaws*, n. 1, 2017, pp. 134-138; G. TIBERI, Il *parere 1/15 della Corte di*

Alla luce di tali possibili risvolti, il Secondo Protocollo risulterebbe automaticamente superato, obsoleto, ma anche causa di forte incoerenza negli ordinamenti statali.

Non a caso, grande apprensione è stata resa nota da parte di esponenti della società civile riguardo il Protocollo e, segnatamente, circa l'art. 14, par. 1, ritenendosi addirittura che possa minare la moderna concezione di tutela dei dati personali[117]. Nello specifico, la disposizione è tacciata di non prevenire che un qualsiasi accordo formalmente stipulato tra Stati Parti possa contenere contenuti illegittimi, limitandosi a richiedere che questi rispettino la legislazione interna sulla tutela dei dati, dando per scontato che gli ordinamenti interni garantiscano necessariamente il rispetto dei principi di proporzionalità, necessità e indipendenza dell'autorità di controllo per la misura adottata imposti nei parr. 2-15. Vi sarebbe stato, in altre parole, un vero e proprio eccesso di fiducia da parte dei redattori.

Con riguardo al principio di indipendenza, quale principio corollario per la corretta valutazione della proporzionalità e necessità delle misure, l'art. 13, par. 14 sancisce l'obbligo di predisporre autorità di controllo dei trasferimenti transfrontalieri di dati in forza dei poteri d'indagine derivati dal Protocollo, ma al contempo proibisce alle Alte Parti di far ricorso a organi indipendenti, intesi come terzi rispetto all'autorità statale. Tale statuizione deriva dalla necessaria caratteristica di pubblicità dell'autorità ("*independent and effective oversight functions and powers"*), ma probabilmente avrebbe dovuto essere maggiormente dettagliata. La presunta indipendenza delle autorità pubbliche è del resto qualcosa da dimostrarsi in concreto, visto che "*many oversight functions can be conducted by government officials housed in the same agencies directing the cross-border investigations being supervised*" secondo chi osserva criticamente il funzionamento degli organi inquirenti[118]. Diversamente, ai sensi dell'art. 13, par. 14 del Secondo Protocollo anche un pubblico ministero, in qualità di "*public authority*" con presunta indipendenza, potrebbe rappresentare il soggetto deputato al controllo della procedura di trasferimento. Ma quest'ultima costituisce un'ipotesi esclusa espressamente dalla sentenza *HK Prokuratuur* della CGUE e più fievolmente obiettata dalla *Dumitru Popescu* da parte della Corte EDU. In aggiunta, i dubbi presentati con riguardo

Giustizia: la prima volta di uno scrutinio di compatibilità di un accordo internazionale con la Carta dei diritti fondamentali, in *Quaderni Costituzionali*, n. 4, 2017, pp. 940-943).

Il tema della vaghezza può essere qui ripresentato per ammettere che, a questo punto, se lo stesso art. 14 risultasse poco definito, allora il rischio di cooperazione giudiziaria indiscriminata non sarebbe fugato nemmeno con la sua applicazione. Infatti, i principi in esso espressi avrebbero presenterebbero limiti assai labili che potrebbero essere sfruttati per generare misure di fatto non proporzionate e non necessarie in accordo con la giurisprudenza europea.

[117] Trattasi del reclamo della *Electronic Frontier Foundation,* nella persona di K. RODRIQUEZ, *EFF to Council of Europe: Cross Border Surveillance Treaty Must Have Ironclad Safeguards to Protect Individual Rights and Users' Data,* in *EFF*, 8 settembre 2021: "*contrary to most other data protection instruments, Article 14 data protection safeguards don't require all processing of personal data be 'adequate, fair and proportionate' to its objective, while Article 13 requires only 'adequate' safeguards and a general respect for the principle of proportionality*"; e, per la nota organizzazione *Human Rights Watch*, di D. BROWN, *Cybercrime is Dangerous, But a New UN Treaty Could Be Worse for Rights*, in *HRW*, 13 agosto 2021: "[…] *even after almost 100 organizations called for transparency in the process. The process also did not allow for sufficient time to provide input on key provisions on data-protection safeguards*".

[118] K. RODRIGUEZ, *op. cit*.

all'indipendenza dell'organo di controllo suggeriscono la nascita di procedure automatizzate *de facto* – come già dichiarato nel *2014 Moraes Report,* [119] che si opponeva alla conclusione nei termini presenti del Secondo Protocollo. Infatti, data l'assenza di una reale indipendenza da parte dell'organo di sorveglianza e controllo, le misure di trasferimenti di dati non potranno che essere convalidate in sede di contestazione, senza che si possa dire che il controllo sia stato effettivo. Ciò contravviene alle regole circa il controllo di garanzia (o *ex ante* o *ex post* secondo la sentenza) previste nel caso *Szabo e Vissy*, in cui si stabilisce che gli "*individual's rights should be subject to an effective control*"[120]. Tale circostanza implicherebbe non soltanto l'incentivazione di misure potenzialmente ingiuste per il futuro ma, addirittura, l'invalidazione degli strumenti di tutela esistenti – si pensi al contenuto della Convenzione 108+ – mettendo a dura prova l'efficacia dei meccanismi di cooperazione giudiziaria digitale in ambito penale.

Per quanto concerne un'eccezione ulteriore, in luogo delle tutele e garanzie offerte dai parr. 2-15 dell'art. 14 Secondo Protocollo, uno Stato Parte richiedente ed uno richiesto – i quali non siano in questo caso vincolati da accordi internazionali formali, come nell'eccezione di cui sopra – potranno mutevolmente accordarsi circa il trasferimento di dati *sulla base di un accordo informale*[121]. L'obbiettivo della disposizione sarebbe assicurare che le Alte Parti conservino una certa flessibilità nel determinare le garanzie a tutela dei dati personali che si applicheranno nei trasferimenti interstatali disposti sulla base del Protocollo. Tuttavia, non esiste alcun riferimento nell'articolo circa la pubblicità di tali accordi, né se questi debbano considerarsi pienamente vincolanti seppure in veste di accordo informale. Vero è che le Parti sono "incoraggiate" alla trasparenza e certezza verso gli individui, i gestori e gli enti coinvolti nei procedimenti di trasferimento *ex* Capo 2, sezione 2. In altre parole, gli Stati vengono incentivati a rendere noto il contenuto degli accordi al pubblico (trasparenza) al fine consentire ai propri cittadini di prendere atto delle regole che disciplinano i trasferimenti transfrontalieri di dati personali (certezza del diritto). Ma la presenza di un suggerimento, e non già l'imposizione attraverso un'obbligazione effettiva, appare francamente insufficiente. Infatti, per via di tale mancanza di trasparenza e certezza, non è soltanto impedito all'individuo di conoscere i meccanismi accordati tra gli Stati Parti, ma diviene fattivamente difficile intraprendere un'azione giuridica (sia essa una forma di ricorso o di reclamo) contro le misure adottate. Ciò, nuovamente, mina il principio di effettività del controllo/supervisione richiesto dalla

[119] Commissione per le libertà civili, la giustizia e gli affari interni, *Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*, del 21 febbraio 2014, 2013/2188(INI), par. 32: "*because it could result unfettered remote access by law enforcement authorities to servers and computers located in other jurisdictions without recourse to MLA agreements and other instruments of judicial cooperation put in place to guarantee the fundamental rights of the individual, including data protection and due process, and in particular Council of Europe Convention 108*".

[120] Corte europea dei diritti dell'uomo, Quarta Camera, *Szabo e Vissy*, cit., par. 77.

[121] Art. 14, par. 1, lett. c. Secondo Protocollo: "*If the transferring Party and the receiving Party are not mutually bound under an agreement described in paragraph 1.b, they may mutually determine that the transfer of personal data under this Protocol may take place on the basis of other agreements or arrangements between the Parties concerned in lieu of paragraphs 2 to 15*".

sentenza *Szabo e Vissy*[122]. Vieppiù, le osservazioni in precedenza fatte verso l'eccezione degli accordi formali (bilaterali) circa l'aderenza al diritto UE ed alla Convenzione 108+ possono essere riproposte riguardo gli accordi informali allo stesso modo. Nel caso del diritto dell'Unione europea la critica è comunque temperata dall'imposizione, da parte della Commissione europea, di una decisione sull'adeguatezza dei bilaterali stipulati da Stati Membri UE[123].

In conclusione, gli scenari prospettabili suggeriscono che tutti i requisiti formali, le condizioni e controlli definiti dalla giurisprudenza europea debbano essere correttamente implementati nella futura normativa. Non a caso, il Regolamento EPOC sembra legato al Secondo Protocollo alla Convenzione di Budapest da un elemento comune: il rischio di una applicazione manchevole o errata dei principi di necessità e di proporzionalità (e preliminarmente di indipendenza dell'autorità di controllo per la misura adottata). In ciò si lascerebbe che il bilanciamento degli interessi in gioco propenda per l'efficienza delle indagini a discapito dei diritti fondamentali dell'indagato o imputato, minando ancora una volta lo Stato di diritto sostanziale.

5. Osservazioni conclusive

Sintetizzando i principali contenuti dell'analisi condotta nel presente contributo, si può innanzitutto affermare che la comunità internazionale, in particolare in ambito europeo, si è dimostrata sensibile alla tematica della raccolta di prove digitali. E, a tal riguardo, si osserva come l'agevolazione per le autorità pubbliche nell'accesso ai dati personali detenuti dai gestori di servizi occupa una posizione prioritaria nell'agenda delle organizzazioni internazionali regionali. Si pensi in tal senso al Regolamento EPOC per l'Unione europea e, dall'altro lato, al Secondo Protocollo alla Convenzione di Budapest per il Consiglio d'Europa. Tuttavia, a causa della natura intrinseca della prova digitale – essenzialmente transfrontaliera, volatile e legata a servizi dei privati – come pure della difficoltà nel bilanciare le c.d. "tecniche speciali d'investigazione", taluni rischi per i diritti fondamentali dell'indagato o imputato si sono concretizzati.

Il processo d'innovazione della cooperazione giudiziaria digitale appare segnato da una discutibile privatizzazione (può esistere, in primo luogo, una mutua fiducia tra Stati e privati?) e ad una diversificazione delle categorie di dati che pare quantomeno arbitraria. Al contempo, tale processo appare necessario. Registratasi nel corso degli anni una frammentazione delle procedure nazionali (spesso unilaterali) volte a sopperire alle mancanze degli strumenti tradizionali, si è generata confusione sia per privati che per i limiti previsti per la tutela dei diritti fondamentali[124]. Eppure, l'approntamento di una normativa di settore richiede di essere condotto in maniera razionale, tenendo in

[122] Corte europea dei diritti dell'uomo, Quarta Camera, *Szabo e Vissy*, cit., par. 77.
[123] Decisione (UE) 2022/722, cit., Allegato, par. 4; Decisione (UE) 2023/436, cit., Allegato, par. 4.
[124] Commissione nel proprio documento *Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward*, maggio 2017, pp. 1-2.

considerazione i limiti fissati dal diritto positivo preesistente e dalla giurisprudenza, con specifico riferimento ai principi di indipendenza, proporzionalità e necessità che devono regolare in modo trasversale l'azione delle autorità competenti.

Senz'altro, è possibile presagire un potenziale conflitto[125] tra le corti europee ed i rispettivi "legislatori", con disputa avente ad oggetto l'applicazione dei principi citati e il ripristino di limiti e garanzie – con un nuovo bilanciamento degli interessi in gioco.

Come potenziale soluzione, taluni hanno suggerito che sia necessario un nuovo strumento internazionale, un trattato, che istituisca un "sistema" volto a concedere volta per volta un mandato sovranazionale basato su requisiti sostanziali e procedurali applicabili a livello globale per l'accesso ai dati. Va da sé che si porrebbero su scala assai ampia questioni di volontà politica, finanziamenti e perfino di supervisione di questo meccanismo. Nel caso dell'Unione europea – testimone dell'attuale tendenza alla *agencification* – la creazione di una nuova Agenzia unicamente responsabile per i rapporti tra autorità giudiziaria in materia digitale sembra invece una soluzione più plausibile, sebbene il Regolamento EPOC preveda già la possibilità di coinvolgere Eurojust nell'esecuzione delle ordinanze[126]. La soluzione appare ammissibile dato che la sentenza *HK Prokuratuur* prescrive, in sostanza, che l'attività di controllo sia svolta da un organo giudiziario o amministrativo che deve essere indipendente – definizione in cui sono ricomprese le agenzie.

In conclusione, le eventuali violazioni dei diritti fondamentali (senza eccezione alcuna per il settore digitale) tendono ad invalidare quegli effetti positivi già prodotti dalla cooperazione in ambito penale. Se la cooperazione digitale necessita di essere realmente efficace nell'era digitale, allora alla presenza di nuovi (e più penetranti) strumenti investigativi devono corrispondere controlli rafforzati sull'attività delle autorità e sui diritti fondamentali coinvolti, al fine di evitare uno squilibrio che possa culminare nella sospensione delle garanzie costituzionali, come avvenuto per la lotta al terrorismo negli anni '70 in Italia e negli USA dopo gli eventi del 2001[127].

[125] Dal lato dell'Unione europea ciò potrebbe essere anticipato, come intuito da M. BUCCARELLA, *op. cit*, p. 235, dalla richiesta di un parere preventivo alla Corte di Giustizia *ex* art. 218, par. 11 TFUE ed avente ad oggetto il Secondo Protocollo alla Convenzione di Budapest. La richiesta dovrebbe essere presentata da parte di uno degli organi coinvolti nella procedura per la stipula di accordi internazionali tra l'Unione e paesi terzi di cui allo stesso art. 218 TFUE.

[126] Art. 5, par. 10 Regolamento EPOC.

[127] Si tratterebbe di una vera e propria applicazione del "diritto penale del nemico", una teoria supposta dal giurista tedesco Günter Jakobs in cui è consentito soggiogare completamente un individuo, che altrimenti rischierebbe di diventare pericoloso. Verrebbe giustificata la possibilità di combattere il criminale-nemico, e prendere le dovute precauzioni, non già secondo le regole del diritto, ma secondo quelle proprie della guerra, riducendo l'individuo a una "non-persona". Infatti, il criminale, colui che non rispetta i diritti altrui, si auto-collocherebbe al di fuori del meccanismo di reciprocità e di tutela, divenendo un nemico della società. A. GAMBERINI, R. ORLANDI (a cura di), *Delitto politico e diritto penale del nemico*, Bologna, 2007, p. 114 ss.

ABSTRACT: Il presente contributo prende in considerazione la cooperazione giudiziaria in ambito penale, che da tempo rincorre un adeguamento normativo mirato a disporre di nuovi meccanismi adatti ad una celere e pronta trasmissione della c.d. prova digitale. Quest'ultima, non a caso, rivela una propria complessità che risiede anzitutto nella sua natura "privata", nonché nei rischi correlati alla violazione dei diritti fondamentali coinvolti, tra cui emerge in particolar modo la *privacy*. A tal riguardo, la normativa europea ha risposto in maniera decisa all'esigenza di un dialogo diretto con i *providers*, ovvero i soggetti direttamente coinvolti nel traffico dei dati d'interesse per le autorità giudiziarie del continente. Tant'è che, con l'intenzione di sorpassare i limiti degli strumenti tradizionali, l'Unione europea ed il Consiglio d'Europa, rispettivamente, si sono dotati, nel luglio 2023, del Regolamento (UE) 2023/1543, sull'ordine europeo di produzione e conservazione della prova digitale in ambito penale e; nel 2021, del Secondo Protocollo alla Convenzione sul crimine informatico. Sebbene formalmente la nuova disciplina europea sia subordinata a non cagionare indebite interferenze nei diritti dell'individuo, il presente contributo intende evidenziare che, da un confronto con la prassi giurisprudenziale sulla *data retention* e sulla *mass surveillance*, emergono invece rimarcabili incongruenze a riguardo. Nel dettaglio, l'analisi ambisce a dimostrare che l'applicazione analogica dei principi di necessità e proporzionalità al neonato Regolamento ed al Secondo Protocollo della Convenzione di Budapest – così come intesi dalla Corte di Giustizia dell'Unione europea e dalla Corte europea dei diritti dell'uomo – renderebbero manifesto un eccesso di "privatizzazione" nella materia oltre che la presenza di "geometrie variabili" nella tutela offerta agli individui.

KEYWORDS: diritti fondamentali – cooperazione giudiziaria – protezione dei dati – Regolamento (UE) 2023/1543 sugli ordini di produzione e conservazione della prova digitale – Secondo protocollo alla Convenzione sul crimine informatico.

PRODUCTION AND PRESERVATION OF DIGITAL EVIDENCE IN THE NEW EUROPEAN LEGAL FRAMEWORK: THE POTENTIAL MISALIGNEMENT WITH THE PRINCIPLES EXPRESSED IN THE SECTORAL CASE LAW

ABSTRACT: This contribution takes a look at judicial cooperation in criminal matters, which has long been pursuing a regulatory adjustment aimed at having new mechanisms suitable for a speedy and prompt transmission of so-called digital evidence. The latter, not surprisingly, reveals its own complexity that resides, among other characteristics, in its “private” nature, as well as in the risks related to the violation of the fundamental rights involved, among which privacy stands out in particular. In this regard, European legislation has responded decisively to the need for direct dialogue with providers, i.e. those directly involved in the traffic of data of interest to the judicial authorities of the continent. So much so that, with the intention of overcoming the limits of traditional instruments, the European Union and the Council of Europe adopted, respectively, Regulation (EU) 2023/1543 on the European order for the production and preservation of digital evidence in criminal matters and, in 2021, the Second Protocol to the Convention on Cybercrime. Although formally the new European regulation is conditional on not causing undue interference in the rights of the individual, this contribution aims to highlight that, from a comparison with the jurisprudential practice on data retention and mass surveillance, significant inconsistencies do in fact emerge. In particular, the analysis aims to demonstrate that the analogical application of the principles of necessity and proportionality to the newborn Regulation and to the Second Protocol of the Budapest Convention – as understood by the Court of Justice of the European Union and the European Court of Human Rights – would lead to an excess of "privatization" in the matter as well as to the presence of “variable geometries” in the protection offered to individuals.

KEYWORDS: data protection – fundamental rights – judicial cooperation – Regulation (EU) 2023/1543 on the European Production and Preservation Orders of Digital Evidence – Second Protocol to the Cybercrime Convention.