L'acquisizione di dati e comunicazioni crittografate attraverso l'OEI: una nuova sfida per la tutela della privacy?

di Stefano Busillo

Abstract: *The acquisition of encrypted data and communications through EIO: a new challenge for the protection of privacy?* – For several years, the European legislator has been producing legislation that, upstream, weighs and compares the need for confidentiality of encrypted data and that of security. It can be said that this has also happened downstream, through the action of the courts. Hence, this paper aims to analyze the European Investigation Order in the light of the less (*data retention saga*) and more (*EncroChat*) recent European jurisprudence to clarify how this tool is affecting the balance between security needs and the protection of the fundamental right to confidentiality of communications by the suspect/accused person.

Keywords: EncroChat; Encrypted communications; European investigation order; National security; Privacy

1. Introduzione

Lo sviluppo delle nuove tecnologie ha da qualche tempo imposto di riflettere sui possibili usi, anche illegali, che possono promanare dalle stesse, nonché circa le ricadute, positive o negative che siano, sui diritti del cittadino. In particolar modo, assai attuale è il dibattito sul valore dei dati crittografati, rappresentanti un insieme di informazioni soggette ad un processo di trasformazione in un formato sicuro allo scopo di proteggerle da accessi o modifiche da parte di terzi[1]. Talune piattaforme di comunicazione digitale – ad es. la nota WhatsApp, oppure Telegram – hanno da tempo fatto ampio utilizzo della crittografazione (o cifratura, criptazione) predefinita dei dati al fine di garantire la massima riservatezza ai propri utenti. Se non altro, com'è intuibile, tale forma di protezione dei dati può però favorire anche attività criminali, che invero creano nocumento alla società, generando tensione con l'aspettativa dei soggetti a che le proprie comunicazioni private restino tali. Per tal motivo, anche i meccanismi di cooperazione giudiziaria approntati dagli Stati e, soprattutto, dall'Unione europea (UE) necessitano di tener conto di ciò. Tra questi, l'Ordine europeo d'indagine (OEI), istituito per

[1] Una pluralità di definizioni alternative a quella presentata viene elencata da M.A. Dizon, A. Meehan, *Technical Principles and Protocols of Encryption and Their Significance and Effects on Technology Regulation*, in 1 *ICTL* 1, 3 (2024).

DPCE online
ISSN: 2037-6677

mezzo della Direttiva 2014/41/UE (Direttiva OEI)[2], non è stato esente da problematiche applicative riguardanti l'intercettazione e l'utilizzazione di comunicazioni criptate. In effetti, come si avrà occasione di spiegare, tale meccanismo di cooperazione sembra aver acuito la più generica difficoltà di bilanciare uno strumento utile (ed efficace) per la trasmissione delle prove, anche precostituite rispetto al procedimento, e la tutela della riservatezza, in particolar modo delle trasmissioni digitali di dati.

È significativo che le piattaforme per lo scambio di dati crittografati siano di per sé perfettamente legali, potendo esserci motivazioni autentiche e legittime per il loro utilizzo, ad. es. da parte di enti governativi per proteggere dati sensibili; tuttavia, gli altrettanto potenziali vantaggi per la criminalità organizzata non sono passati inosservati agli operatori e alle agenzie di contrasto penale che hanno verificato il loro impiego per la conduzione di attività illecite[3]. In altre parole, le opportunità insite nella crittografazione delle comunicazioni – contemporaneamente un diritto per l'individuo ed un rischio per la sicurezza collettiva – dipendono semplicemente dall'uso che se ne fa, come dalla stessa UE nella Risoluzione del Consiglio «Security through encryption and security despite encryption» del 24 novembre 2020. Pertanto, va preliminarmente fugato il dubbio che la criptazione sia di per sé elemento giustificante un'ingerenza della *privacy*.

Certamente, il sacrificio della riservatezza delle comunicazioni è comunque possibile laddove necessario e proporzionato rispetto ad esigenze di pubblica sicurezza da dimostrarsi caso per caso. Tale problema si è presentato appunto nelle more del caso *EncroChat* – ove un'operazione congiunta da parte di autorità francesi e olandesi, effettuata nell'ambito di una Squadra investigativa comune (SIC), ha generato un acceso dibattito a livello nazionale ed europeo sull'opportunità di utilizzare l'OEI per la trasmissione di prove già formate e contenenti conversazioni criptate. In particolare, la più recente giurisprudenza della Corte di giustizia, oltre ad una serie di chiarimenti sulla portata ed esplicazione del principio del giusto processo nell'ambito dell'OEI, ha eseguito un'attività bilanciamento tra esigenze securitarie e tutela della riservatezza in ipotesi di comunicazioni segrete che merita di essere meglio esplorata.

Alla luce di quanto sinora esposto, la presente indagine intende proporre dapprima, nella Sezione 2 del contributo, un ragionamento sull'attenzione mostrata dall'Unione europea verso i dati e comunicazioni protetti da cifratura, ovvero di alcuni principi che sembrano essere emersi nella regolamentazione del fenomeno. Lo scopo di ciò è introdurre nella successiva Sezione 3 una breve analisi su come il diritto alla riservatezza in questi casi si relazioni con le esistenti disposizioni della Direttiva OEI. Nella Sezione 4 verrà invece introdotta la vicenda *EncroChat*. In merito, l'obbiettivo è scorgere quali siano state le principali problematiche sorte nell'ambito di questa vasta operazione da parte delle autorità competenti e

[2] Dir. UE n. 41/2014 del P.E. e del Cons. del 3-4-2014, relativa all'ordine europeo di indagine penale.

[3] Europol, *First Report on Encryption*, 10-6-2024, 11, https://www.europol.europa.eu/publications-events/publications/first-report-encryption

come le varie corti nazionali abbiano inteso il bilanciamento sinora preso in considerazione. Essa, infatti, si pone come interessante caso di studio per identificare il grado di tutela della riservatezza riconosciuto da parte degli Stati membri UE in presenza di comunicazioni crittografate dapprima decifrate in un certo Stato e, in un secondo momento, trasferite in un altro mediante OEI. A riguardo, le Sezioni 5 e 6 intendono porre l'attenzione sulla conseguente risposta della Corte di giustizia circa aspetti di diritto sostanziale, ovvero sul requisito di proporzionalità in ambito di applicazione di siffatto ordine e sulla effettività della tutela del diritto fondamentale alla riservatezza delle proprie comunicazioni. Infine, nella Sezione 7, verranno delineate le conclusioni dell'indagine cercando di rispondere all'interrogativo inerente a quale sia lo *status* attuale del bilanciamento tra esigenze securitarie, portate avanti attraverso l'OEI, e la *privacy* quando declinata nelle comunicazioni criptate e se da ciò discende una nuova "sfida" rispetto alla tutela della riservatezza.

2. La natura ambivalente della crittografazione e l'indifferenza verso il dato cifrato per l'Unione Europea

Fatta eccezione per qualche atto sporadicamente presentato, l'attenzione riservata alle comunicazioni crittografate da parte dell'Unione Europea si è accresciuta a partire dalla seconda metà degli anni 2010, ove il cd. *First Report on Encryptio*n, datato 10 giugno 2024, rappresenta uno degli ultimi e più emblematici documenti in materia. Complessivamente, l'UE ha prodotto una serie di atti sia di natura politica/programmatica che immediatamente più pratica/di diritto derivato, anche *de jure condendo*, al fine di regolamentare questo tipo di dato. L'identificazione dei temi in essi ricorrenti consente di individuare il valore attribuito dall'Unione alla cifratura, così contribuendo – quando si parla di comunicazioni crittografate – a definire il peso del diritto alla riservatezza in ipotesi di bilanciamento rispetto ad altri interessi ad essa contrapposti.

Anzitutto, curiosamente, non esiste a livello UE una norma definitoria della cifratura. A dispetto degli emendamenti proposti a suo tempo dal Parlamento europeo – i quali definivano i «dati cifrati» come quei «dati personali che, mediante misure tecnologiche di protezione, sono resi inintelligibili a chiunque non sia autorizzato ad accedervi»[4] – la versione finale del GDPR non fornisce una nozione di questi, pur citando la crittografia in diverse disposizioni come requisito di "conformità", ovvero come misura tecnica e organizzativa adeguata a garantire la sicurezza del trattamento dei dati[5]. Tanto dovrebbe comunque bastare ad implicare che il dato cifrato benefici della tutela di cui al Regolamento sulla protezione dei dati. Ciononostante, vi è chi sostiene che «[e]ncrypting personal data can lead to the non-applicability of the GDPR» visto che – citando le conclusioni dell'Avvocato generale (AG) Campos Sánchez-Bordona nel 2016 in una

[4] Posizione del Parlamento europeo definita in prima lettura il 12-3-2014, P7_TC1-COD(2012)0011, art. 4., par. 2 ter.
[5] Art. 32, par. 1, lett. a) del reg. UE n. 679/2016 del 27-4-2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la dir. CE n. 46/1995.

DPCE online
ISSN: 2037-6677

causa afferente ai cd. IP dinamici – solo la natura del mezzo di comunicazione permetterà di stabilire se l'oggetto della comunicazione sia qualificabile come «dato personale», ovvero se questo sia riconducibile ad un preciso utente[6]. Da tale qualificazione discenderà l'applicazione o meno delle tutele del GDPR anche nei confronti delle comunicazioni criptate[7].

Ciò posto, l'elemento caratterizzante la cifratura rimane la sua ambivalenza. La Commissione ha esaminato nel 2017 il ruolo della crittografia nelle indagini penali insieme ai pertinenti portatori d'interessi sotto il profilo tecnico e giuridico ritenendola, da un lato, «fondamentale per garantire la sicurezza informatica e la protezione dei dati personali» e, dall'altro, una sfida lanciata all'UE da parte dei criminali, tenendo in conto che «il ricorso alla crittografia a fini criminosi sarà sempre maggiore nei prossimi anni»[8].

Analogamente, tale percezione è confermata dalla già menzionata risoluzione del 24 novembre 2020, in cui il Consiglio sottolinea dapprima il proprio sostegno allo sviluppo, all'attuazione e all'utilizzo di una crittografia forte quale strumento necessario per tutelare i diritti fondamentali e la sicurezza digitale dei cittadini, dei governi, dell'industria e della società[9]. In un secondo momento, lo stesso rileva la necessità di garantire che le autorità di contrasto competenti siano in grado di esercitare i loro legittimi poteri, sia *online* che *offline*, per proteggere le imprese ed i cittadini da quella criminalità facente uso di comunicazioni criptate. L'idea di base è che «competent authorities must be able to get access to data in a lawful and targeted manner», ove si nota che la parola «targeted» escluderebbe sin da subito qualsiasi tipo di controllo di massa sulle comunicazioni crittografate. Tuttavia, ci sono casi in cui la crittografia rende estremamente difficile o praticamente impossibile l'accesso in maniera mirata alle comunicazioni e la relativa analisi di queste per rintracciare elementi di prova. Pertanto, il documento invita gli Stati membri dell'UE a «join forces with the tech industry» per creare congiuntamente un giusto equilibrio tra l'impiego ed il contrasto della cifratura, oltre che a stabilire un quadro normativo appropriato. Va riconosciuto che, per taluni, il risultato auspicato è fortemente messo in dubbio sia a livello di fattibilità legale che tecnica[10].

Aldilà degli aspetti programmatici, tra gli atti che presentano invece maggiore dimensione operativa, si segnala il Regolamento provvisorio (UE) n. 2021/1232, il quale consente a determinati servizi di comunicazione

[6] Corte giust., c-582/14, *Patrick Breyer c. Bundesrepublik Deutschland*, concl. dell'AG Campos Sánchez-Bordona 12-5-2016, p.ti 68 e 73. Gli IP dinamici sono quegli indirizzi telematici temporaneamente assegnati ai dispositivi e rinnovati con nuovi valori ad ogni accesso di rete, garantendo in questo modo una più difficile tracciabilità dell'utente.
[7] G. Spindler, P. Schmechel, *Personal Data and Encryption in the European General Data Protection Regulation*, in 7(2) *JIPITEC* 163, 167-168, 176 (2016).
[8] COM(2017)608 final.
[9] Notevoli sono i passaggi in cui descrive la cifratura quale «an anchor of confidence in digitalisation and in protection of fundamental rights and should be promoted and developed» and «it is evident that all parties benefit from encryption technology». Sulla tutela dei "nuovi" diritti digitali, v. P. De Pasquale, *Verso una Carta dei diritti digitali (fondamentali) dell'Unione europea?*, in *Dir. Un. Eur.*, 2022, 1, 163 ss.
[10] M. Koomen, *The Encryption Debate in the European Union: 2021 Update*, in *Carnegie Endowment for International Peace*, 31-3-2021.

interpersonale di derogare su "base volontaria" alle norme stabilite in materia di riservatezza dei dati per consentire loro di rilevare e segnalare materiale pedopornografico *online*. Il Regolamento ha una certa rilevanza da un punto di vista della criptazione dei dati. Infatti, da una parte, essa è pienamente riconosciuta quale diritto individuale da tutelare e da non ledere indebitamente[11]. D'altra parte, una deroga assai precisa al diritto alla riservatezza, ovvero una giustificata ingerenza, è contemplata in caso di reati connessi alla pornografia minorile. La Direttiva *e-privacy*, oggetto della deroga, stabilisce infatti regole che garantiscono il diritto alla vita privata in relazione al trattamento dei dati personali negli scambi di dati nel settore delle comunicazioni elettroniche[12]. Tuttavia, in forza della eccezione istituita dall'art. 3 del Regolamento provvisorio, gli artt. 5, par. 1, e 6, par. 1, della Direttiva *e-privacy* non troveranno applicazione nei casi predetti, conferendo ai fornitori di servizi di posta elettronica e di messaggistica la "facoltà" di scansionare automaticamente tutti i messaggi personali, anche criptati, di ciascun utente alla ricerca di contenuti sospetti da denunciare alla polizia. Inevitabilmente, aldilà del successo dell'atto dovuto alla condanna universale che viene fatta per gli abusi verso i minori, il Regolamento provvisorio contro la pedopornografia non poteva che destare talune reazioni critiche, anche perché l'atto tende a sovvertire completamente un'idea statuita in precedenza dal Parlamento europeo, ossia che la cifratura possa aiutare il minore piuttosto che danneggiarlo[13].Tra i principali elementi di addebito, l'atto è ritenuto inefficace e problematico in partenza sia perché i criminali troveranno semplicemente altre modalità di adescamento dei minori sia perché i «collective benefits that encryption has on privacy, trust, and democracy may outweigh the risks», paventando un non corretto bilanciamento a monte da parte del legislatore[14]. Inoltre, un altro problema risiede nel timore che vi possa essere una normalizzazione di quelle che sarebbero misure di intercettazione e controllo eccezionali, ma che diverrebbero pratica comune accettata da tutti come *fait accomplì*. Viene anche considerato il rischio che il Regolamento possa arrivare di fatto a far perdere utilità e significato alla cifratura in generale[15]. Vi è chi poi, semplicemente, mette in dubbio la replicabilità di questo Regolamento anche

[11] V. considerando 25 del reg. UE n. 1232/2021 del P.E. e del Cons. del 14-7-2021, relativo a una deroga temporanea a talune disposizioni della direttiva 2002/58/CE per quanto riguarda l'uso di tecnologie da parte dei fornitori di servizi di comunicazione interpersonale indipendenti dal numero per il trattamento di dati personali e di altro tipo ai fini della lotta contro gli abusi sessuali online sui minori.
[12] Dir. CE n. 2002/58 del P.E. e del Cons. del 12-7-2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.
[13] Ris. del P.E. del 17-12-2020, sulla strategia dell'UE per l'Unione della sicurezza, 2020/2791(RSP), p.to 16: «[il Parlamento europeo] sottolinea che la cifratura da punto a punto contribuisce alla tutela della *privacy* dei cittadini, compresa la protezione dei minori su Internet».
[14] S. Chousou *et al.*, *Is Encryption a Fundamental Right? A Case Study on CSAM Regulation in the EU*, in 1 *SciencesPo* 1, 33 (2023).
[15] D. Naranjo, *Open Letter: Civil Society Views on Defending Privacy While Preventing Criminal Acts*, in *EDRI*, 27-10-2020. In altre parole, in nome della persecuzione di un *cluster* di reati certamente odiosi, l'intero concetto di crittazione ed il proprio scopo originario, ovvero garantire la riservatezza, salterebbero.

DPCE online
ISSN: 2037-6677

in altri ambiti, descrivendolo come un "successo" dell'UE più unico che raro[16].

Eppure, l'11 maggio 2022 la Commissione europea ha riportato di volere sostituire il suddetto Regolamento provvisorio, proponendone uno nuovo di natura permanente[17]. La notevole differenza tra il Regolamento esistente e quello proposto risiede nella volontà di introdurre stabilmente misure questa volta obbligatorie in capo ai fornitori di servizi allo scopo individuare e segnalare casi di pedopornografia. Alcuni mesi dopo la sua presentazione, il Comitato europeo per la protezione dei dati e il Garante europeo della protezione dei dati hanno adottato un parere congiunto sulla proposta di regolamento, tenendo ampiamente conto dei rischi da esso posti rispetto ai diritti fondamentali[18]. Obbligando la generalità dei fornitori di servizi ad adempiere alle disposizioni dell'atto e creando un regime di controllo potenzialmente sistematico e generalizzato, la principale problematica qui risiederebbe nella percezione che la Proposta di regolamento introduca indirettamente misure di sorveglianza di massa non suffragate da esigenze di sicurezza nazionale, come pure puntualizzato dalla Commissione per le libertà civili, la giustizia e gli affari interni del Parlamento europeo nel novembre 2023, ponendo in una sorta di stallo la delicata vicenda normativa e accertando che circa la tensione esistente tra diritto il riservatezza e la sicurezza non è ancora stata individuata una quadra[19].

Di sicuro interesse è poi anche il Regolamento (UE) 2023/1543 sugli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche – quale strumento di cooperazione giudiziaria *ad hoc* per il recupero di dati e comunicazioni digitali – il quale fa riferimento alla cifratura al proprio considerando 20 e lo fa introducendo due distinti concetti[20]. In primo luogo, è prevista una sostanziale "indifferenza" verso il tipo di dato richiedibile dall'autorità giudiziaria al prestatore di servizi. Sarebbe a dire che non è in alcun modo rilevante per il Regolamento se il dato oggetto dell'ordine sia cifrato o meno, evidentemente suggerendo una prevalenza dell'esigenza securitaria rispetto alla tutela della *privacy* in questi casi. In secondo luogo, è previsto che, una volta richiesto, il prestatore di servizi non sarà comunque obbligato alla decifratura dei dati, residuando una mera facoltà. Si ritiene che quest'ultima statuizione potrebbe essere vista come un elemento volto a tutelare il rapporto di fiducia tra utente e piattaforma – una misura di compromesso con gli *stakeholders* al momento

[16] M. Koomen, cit.: «in the context of combating terrorism and other harmful content, it is far more complex due to legal ambiguities of such content and the violations any scanning system could impose on users' fundamental freedoms».
[17] Proposta di reg. dell'11-5-2022, che stabilisce norme per la prevenzione e la lotta contro l'abuso sessuale su minori, COM/2022/209 final, 2022/0155(COD).
[18] Parere congiunto EDPB-GEPD n. 4/2022 del 28-7-2022, sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce norme per la prevenzione e la lotta contro l'abuso sessuale su minori, par. 100.
[19] Comunicato stampa del P.E., *Child sexual abuse online: effective measures, no mass surveillance*, 14-11-2023.
[20] Reg. UE n. 1543/2023 del P.E. e del Cons. del 12-7-2023, 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.

della negoziazione del Regolamento – oppure come una forma di salvaguardia *in extremis* della riservatezza dei dati, laddove il fornitore di servizi sia "virtuoso" e non opti per cedere il dato già decifrato. Tuttavia, anche tale previsione di non obbligatorietà nel fornire dati "chiari" alle autorità potrebbe venire meno.

Il cd. Gruppo di alto livello, istituito dalla Commissione europea nel 2023[21], ha infatti proposto *inter alia* una raccomandazione per la quale «service providers offering encrypted services must be obliged to find the means to provide data in an intelligible way upon lawful request from law enforcement and judicial authorities»[22]. Viene suggerita pertanto una nuova regola generale per cui, da una richiesta formale e legittima da parte delle autorità – sebbene non sia noto secondo quali parametri – discenderà la trasformazione della facoltà predetta in un vero e proprio obbligo per il prestatore, evidentemente rendendo il profilo securitario ancor più prevalente rispetto alla tutela della riservatezza degli utenti. Tra l'altro, nella raccomandazione si fa riferimento all'espansione della conservazione dei dati ove possibile attraverso un regime armonizzato, poiché «the absence of data retention obligations negatively affects the effectiveness of e-evidence rules»[23].

A riguardo, l'idea di un mirato «lawful access» ai dati cifrati da parte delle autorità, sebbene ritenuta di dubbia compatibilità con la Carta di Nizza per il Comitato europeo per la protezione dei dati ed osteggiata dalla società civile[24], appare senz'altro supportata da Europol e dalla polizia nazionale degli Stati membri UE. Quest'ultimi richiamano l'attenzione delle imprese IT e dei governi affinché provvedano rispettivamente «to build in security by design» e «to put in place frameworks that give us the information we need to keep our publics safe»[25]. E, in effetti, la cooperazione con l'industria di settore coniugata in un nuovo quadro giuridico specializzato pare essere anche uno degli elementi salienti – rubricato «Going dark: Access to digital data» – del *non-paper* proposto dalla Svezia al Consiglio nel giugno 2024[26].

[21] Decisione della C.E. del 6-6-2023, *setting up a high-level group on access to data for effective law enforcement*, C (2023) 3647 final.
[22] *Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement* del 21-5-2024, in part. racc. 27(iii). Anche se non dettagliato allo stesso modo, così anche *First Report on Encryption*, cit., 49: «Extended search capabilities and means for targeted lawful access could be beneficial in capturing encrypted data». Le raccomandazioni in questione si estenderebbero oltre l'ambito applicativo del Regolamento sugli ordini di produzione e conservazione della prova digitale.
[23] Tuttavia, la ris. del Cons. del 24-11-2020, on Encryption – Security through encryption and security despite encryption, rev1, p.to 5, esplica che, in materia di dati cifrati, «Competent authorities must be able to access data in a lawful and targeted manner». L'utilizzo del termine «targeted» potrebbe servire ad "escludere" che, nelle intenzioni del legislatore europeo, possano essere disposte operazione di sorveglianza di massa in ipotesi di criptazione delle comunicazioni.
[24] Dich. n. 5/2024 del Comitato europeo per la protezione dei dati del 4-11-2024, *on the Recommendations of the HighLevel Group on Access to Data for Effective Law Enforcement*, 5; cfr. la lettera di risposta alle raccomandazioni da parte della ONG European Digital Rights, *EU Police Data Plans Pose Substantial Security and Privacy Threats*, 11-12-2024.
[25] Europol, *Joint Declaration of the European Police Chiefs*, 21-4-2024.
[26] Doc. n. 10493/24 del Cons del 5-6-2024, *on a New SecEUrity Package – Information from Sweden*, 3.

DPCE online
ISSN: 2037-6677

Il documento fornisce una panoramica sulle posizioni governative in materia, dato che i suoi contenuti sono stati condivisi chiaramente da alcuni Stati membri, ad es. l'Estonia. Ciò che rileva in particolare è che la proposta svedese assume un'inflessione fortemente ostile alla tutela della riservatezza dato che ritiene necessario un cambiamento radicale di prospettiva nella lotta contro il terrorismo e la criminalità organizzata, in quanto troppe proposte sono state in precedenza "annacquate" («watered down») da considerazioni sui diritti fondamentali, divenuti a questo punto sacrificabili.

Da ultimo, vengono in considerazione un recente chiarimento sulla Proposta di regolamento per l'identità digitale europea, che agevola la criptazione delle credenziali degli utenti sui *browser*[27]; il Regolamento Prüm II, che sostiene alacramente l'impiego della cifratura per la tutela dei dati sui sistemi di *data exchange* adoperati dalle forze di polizia[28]; ed il *Cyber Resilience Act* dell'UE, adottato nell'ottobre 2024, che mira a far ottenere una maggiore sicurezza ai *software* ed agli *hardware* inclusivi di elementi digitali, predisponendo una serie di obblighi per i fabbricanti che operano nello Spazio economico europeo[29]. In particolare, incentrato sulla sicurezza informatica e sulla riduzione delle vulnerabilità, il *Cyber Resilience Act* prevede un proprio Allegato I sui «Requisiti essenziali di cibersicurezza» in cui si fa indicazione delle modalità di *design* e produzione dei prodotti con elementi digitali, richiedendo che questi debbano proteggere «la riservatezza dei dati personali o di altro tipo conservati, trasmessi o altrimenti trattati, ad esempio criptando i pertinenti dati a riposo o in transito mediante meccanismi all'avanguardia, e utilizzando altri mezzi tecnici» (Parte I, par. 2, lett e).

Il riferimento diretto alla cifratura in tutti questi casi è interessante poiché consente di attestare che l'UE intende prevedere e perfino incentivare un concetto di "*cybersecurity by design*" da infiltrazioni indebite, ovvero quelle di matrice criminosa, e – al contempo – una cybersicurezza che può essere, sempre "*by design*", oggetto di legittimo accesso da parte degli inquirenti. Pertanto, alla luce di quanto suesposto, si deve ritenere che lo sviluppo del diritto dell'Unione con riguardo alla crittografia confermi sì la sua ambivalenza, ma che stia anche virando verso posizioni favorevoli alla sicurezza e che profili di rischio per la *privacy* sono già emersi o emergeranno per tale motivo. Di conseguenza, è utile comprendere se questa stessa tendenza possa avere ripercussioni pratiche o parallelismi nei meccanismi di cooperazione giudiziaria UE in ambito penale.

[27] Ris. del P.E. del 29-2-2024, sulla proposta di regolamento del Parlamento europeo e del Consiglio che modifica il reg. UE n. 910/2014 per quanto riguarda l'istituzione di un quadro per un'identità digitale europea, COM (2021)281, 2021/0136 (COD), in part. Allegato «Dichiarazione della Commissione sull'articolo 45 in occasione dell'adozione del Regolamento (UE) 2024/1183».

[28] Reg. UE n. 982/2024 del P.E. e del Cons. del 13-3-2024, sulla consultazione e lo scambio automatizzati di dati per la cooperazione di polizia, artt. 8, 13, 17, 22 e 53, par. 3, lett. j).

[29] Reg. UE n. 2847/2024 del P.E. e del Cons. del 23-10-2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali.

3. La declinazione della privacy nell'Ordine europeo d'indagine penale: un rischio "genetico" e taluni correttivi giurisprudenziali

Con specifico riferimento all'Ordine europeo d'indagine penale, sono venute infatti in rilievo alcune criticità relative all'intercettazione di dati crittografati con ricadute sulla riservatezza delle stesse. Consistente in una decisione giudiziaria emessa o convalidata da un'autorità competente di uno Stato membro per compiere uno o più atti di indagine specifici in un altro Stato membro, l'OEI gode di ambito applicativo ampissimo, in quanto emanabile sostanzialmente per qualsiasi tipologia di prova. L'ordine è oggetto di emissione non solo per disporre il trasferimento di una prova che dovrà essere generata dall'attività dello Stato di esecuzione, ma anche «per ottenere prove già in possesso delle autorità competenti dello Stato di esecuzione» (art. 1, par. 1 Direttiva OEI).

A tal riguardo, esso rappresenta espressione del principio di mutuo riconoscimento delle decisioni giudiziarie e, per estensione, com'è possibile notare già in questa sede, anche delle prove trasferite in virtù della procedura che lo riguarda. Il riferimento al principio di mutuo riconoscimento – come introdotto nella cooperazione in materia penale dal Consiglio di Tampere (1999) e di seguito positivizzato dall'art. 82, par. 1 TFUE, base giuridica della Direttiva OEI – non è casuale. Del resto, "l'obbligo" di esecuzione di un ordine d'indagine da parte dello Stato di esecuzione implica l'esistenza di una procedura al contempo sia transnazionale che "automatica", entrambi fattori che possono accrescere il rischio di limitazione indebita, nel senso di non proporzionata, dei diritti fondamentali dell'indagato o imputato.

In particolare, la fase preliminare del procedimento penale, in cui opera principalmente l'Ordine europeo d'indagine, appare assai delicata sotto questo punto di vista; tant'è che è la stessa Corte di giustizia UE ad aver chiarito circa l'OEI che «la potenziale violazione dei diritti fondamentali» è «insita nell'adozione dei provvedimenti aventi natura probatoria»[30]. Coerentemente, il legislatore eurounitario fa ampio riferimento a ciò nel testo della Direttiva, ove anzitutto stabilisce che l'atto non fa venir meno «l'obbligo di rispettare i diritti fondamentali e i principi giuridici sanciti dall'articolo 6 TUE, compresi i diritti di difesa delle persone sottoposte a procedimento penale, e lascia impregiudicati gli obblighi spettanti a tale riguardo alle autorità giudiziarie» (art. 1, par. 4 Direttiva OEI)[31]. In sostanza, quale conseguenza di tale riferimento, viene imposto *ex* art. 6, par. 3 TUE il rispetto del contenuto della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 1950 (CEDU), nonché *ex* art. 6, par. 1 TUE anche quello della Carta dei diritti fondamentali dell'Unione Europea del 2000 (Carta di Nizza).

[30] Corte giust., c-852/19, *Gavanozov*, sent. 11-11-2021, p.to 50.

[31] Ciò appare in linea con i rischi profilati dalla giurisprudenza di Strasburgo in merito all'acquisizione di prove straniere, su cui v. Corte EDU, no. 43286/98, *Rodriguez c. Paesi Bassi*, 27-6-2000: «the Court considers that the Convention does not preclude reliance, at the investigating stage, on information obtained by the investigating authorities from sources such as foreign criminal investigations. Nevertheless, the subsequent use of such information can raise issues under the Convention where there are reasons to assume that in this foreign investigation defence rights guaranteed in the Convention have been disrespected».

DPCE online
ISSN: 2037-6677

Oltre ai «diritti di difesa» menzionati espressamente dall'art. 1 Direttiva OEI – di cui agli artt. 6 e 13 CEDU ed agli artt. 47 e 48 Carta di Nizza – ai fini della presente indagine si intende richiamare l'attenzione sul necessario rispetto del diritto alla riservatezza enucleato nell'art. 8 CEDU, nonché negli artt. 7 e 8 Carta di Nizza ed art. 16 TFUE[32]. Tale diritto, per taluni, sarebbe addirittura «perhaps the most threatened fundamental right in the pre-trial stage of criminal proceedings»[33]. E tale preoccupazione, in effetti, sembra essersi accresciuta per via dal progresso tecnologico[34] al punto da avere spinto il legislatore europeo – in origine criticato per non avere incluso disposizioni *ad hoc* in merito[35] – a prevedere nel testo finale della Direttiva una disciplina peculiare per l'intercettazione delle telecomunicazioni (artt. 30 e 31 Direttiva OEI). In tal senso, vi è chi pure ha notato che l'attenzione verso la riservatezza da parte della Direttiva è divenuta a quel punto «disproportionate», comparando l'ampia considerazione data a questo diritto rispetto alla scarsità di riferimenti precisi ai diritti di difesa, genericamente citati e null'altro[36]. Tuttavia, si ritiene che tale osservazione debba considerarsi oggi per lo più superata alla luce della più recente giurisprudenza della Corte di giustizia sull'OEI (in particolare *EncroChat*, *infra*). Ne sono motivo, da una parte, una serie di chiarimenti a livello giurisprudenziale sulla portata ed esplicazione del principio del giusto processo nell'ambito dell'Ordine d'indagine europeo penale e, dall'altra parte, il fatto che il bilanciamento tra esigenze securitarie e tutela della riservatezza nel corso degli anni sembra aver favorito il primo di questi due termini.

Ciò posto, come noto, l'OEI presenta una pluralità di disposizioni poste a presidio dei diritti fondamentali dell'indagato/imputato, ove talune sono considerabili di cornice[37] mentre altre più immediatamente operative. Sotto quest'ultimo profilo, l'adeguata circoscrizione delle "condizioni" per cui le

[32] Tant'è che per B. Cortese, *La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona*, in *Dir. Un. Eur.*, 2012, 2, 313, è con l'introduzione di questa disposizione, occorsa grazie alla modifica dei trattati del 2007, che l'UE ha maturato una competenza specifica in materia di dati e, per effetto di ciò, la possibilità di definire la portata del diritto alla *privacy* in tale contesto. Dalla prospettiva della Convenzione europea dei diritti dell'uomo, invece, l'art. 8 CEDU rappresenterebbe una disposizione che più delle altre, tra quelle incluse in questo catalogo europeo di diritti e libertà, testimonia il carattere di «living instrument» della stessa Convenzione. Così A. Di Stasi, *Introduzione alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, Milano, 2022, 11.

[33] I. Armada, *The European Investigation Order and the Lack of European Standards for Gathering Evidence: Is a Fundamental Rights-Based Refusal the Solution?*, in 6(1) *New J. Eur. Crim. Law* 8, 9 (2015).

[34] Sul punto v. M.A. Biasiotti, F. Turchi, *Introduction: Setting the Scene on EIO and the Interaction Between Law and Technology*, in Id. (Eds), *European Investigation Order. Law, Governance and Technology Series*, Cham, 2023.

[35] Parere del Garante europeo della protezione dei dati del 18-10-2010, *Opinion on European Investigation Order*, p.to 28; C. Heard, D. Mansell, *The European Investigation Order: Changing the Face of Evidence-Gathering in EU Cross-Border Cases*, in 2(2) *New J. Eur. Crim. L.* 353, 365 (2011).

[36] R. Garcimartín Montero, *The European Investigation Order and the Respect for Fundamental Rights in Criminal Investigations*, in 1 *Eucrim* 45, 46 (2017).

[37] Cfr. i considerando 10, 12, 18, 19, 39 della Direttiva OEI.

autorità competenti possono ricorrere a misure investigative invasive risulta fondamentale per l'espletamento del generico dovere di rispetto dei diritti fondamentali richiesto dall'art. 1 Direttiva OEI.

Con riguardo agli obblighi specifici dell'autorità dello Stato di emissione, è possibile prendere atto del contenuto dell'art. 6, par. 1 della Direttiva, tale che l'autorità possa disporre l'ordine "solamente" quando sono ritenute soddisfatte le condizioni di necessità e proporzionalità, «tenendo conto dei diritti della persona sottoposta a indagini o imputata» (lett. a), nonché di equivalenza, ovvero laddove l'atto o gli atti di indagine richiesti possano essere emessi alle medesime condizioni in un caso interno analogo (lett. b). Quanto alla prima delle due condizioni, definibile una valutazione in concreto, è possibile rilevare la riproposizione della regola generale di cui all'art. 52, par. 1 della Carta di Nizza, che stabilisce – ad eccezione dei diritti assoluti, come quello alla vita – l'ammissibilità della compressione di quei diritti compresi nella Carta a condizione che la misura sia proporzionata e necessaria all'interesse perseguito ed al mezzo impiegato, il quale deve essere il meno invasivo possibile. Circa la regola del "caso interno analogo", quale valutazione astratta, la *ratio* di tale requisito è invece evitare che siano eluse le norme nazionali in materia di ricerca probatoria, magari facendo ricorso ad omologhe misure più intrusive di altro Stato che, altrimenti, non sarebbero state ammissibili nel proprio[38]. A far da contraltare all'accentramento della procedura nelle mani dell'autorità d'emissione[39], sono previste specifiche disposizioni facenti capo all'autorità di esecuzione. Dando contesto alla summenzionata (semi)automaticità, l'autorità di esecuzione «può», *ex* art. 11, par. 1, lett. f), rifiutare il riconoscimento o l'esecuzione dell'ordine per una molteplicità di ragioni, tra cui «seri motivi per ritenere che l'esecuzione dell'atto di indagine richiesto nell'OEI sia incompatibile con gli obblighi dello Stato di esecuzione ai sensi dell'articolo 6 TUE e della Carta». L'ipotesi appena commentata può considerarsi come un caso di limitazione, se non di «deroga», come espresso dalla Corte di giustizia in *Gavanazov I*[40], del principio del reciproco riconoscimento delle decisioni giudiziarie.

Significativo è anche il fatto che, in forza di mezzi d'impugnazione equivalenti a quelli disponibili in un caso interno analogo, le ragioni di merito dell'emissione dell'OEI possono essere impugnate dall'interessato presso lo Stato d'emissione, «fatte salve le garanzie dei diritti fondamentali nello Stato di esecuzione» (art. 14, par. 1). In accordo con certa giurisprudenza di Lussemburgo, in particolare *Gavanazov II*[41], tale diritto di ricorso deve essere effettivo, ovvero garantito concretamente dall'ordinamento nazionale dello Stato membro di emissione a pena di non

[38] Si tratterebbe, in altre parole, di un vero e proprio *forum shopping* da parte degli inquirenti, ove si abuserebbe di una legislazione straniera più invasiva verso i diritti dell'indagato. Sul punto v. l'analisi di M. Daniele, *Ricerca e formazione della* prova, in R.E. Kostoris (cur.), *Manuale di procedura penale europea*, Milano, 2017, 469.

[39] Tra l'altro, la Corte EDU sembra sostenere tale scelta secondo cui, in regime di mutuo riconoscimento delle decisioni giudiziarie, il rispetto dei diritti fondamentali debba essere di competenza dello Stato d'emissione (v. Corte EDU, no. 56588/07, *Stapleton c. Irlanda*, 4-5-2010, p.to 29).

[40] Corte giust., c-324/17, *Gavanazov I*, concl. dell'AG Yves Bot 11-4-2019, p.to 59.

[41] Corte giust., c-852/19 *Gavanazov II*, sent. 11-11-2021, p.ti 31-34, 45, 50 e 62.

DPCE online
ISSN: 2037-6677

emissibilità dell'OEI[42]. Lo scopo di tale previsione sanzionatoria è assicurare, in presenza di «ingerenze nel diritto di ogni persona al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni», che il soggetto interessato possa avvalersi della tutela prevista dall'art. 14[43]. La disposizione, specialmente in considerazione del rafforzamento occorso grazie alla prassi giurisprudenziale, è da considerarsi assolutamente positiva.

Tuttavia, alla luce di quanto esposto, ci si deve chiedere se la giurisprudenza intervenuta in materia di dati da parte delle corti europee – eventualmente in maniera mirata anche sulle comunicazioni criptate – abbia comunque aggiornato il parametro di proporzionalità cui sia l'autorità di esecuzione che di emissione debbano necessariamente informarsi. In particolar modo, ciò è determinante per temperare l'ampio margine di discrezionalità ammesso in favore dell'autorità di emissione che, se del caso, sarebbe tenuta ad uniformarsi ad una valutazione sulla proporzionalità dell'ingerenza della riservatezza già "fissata" dalla giurisprudenza internazionale ed europea.

3.1 L'attività di bilanciamento occorsa nella *data retention saga* ed in *Podchasov c. Russia*

A partire dal 2014, il volume di pronunce riconducibili alle corti europee in materia di protezione dei dati è aumentato costantemente, fornendo un quadro sempre più chiaro della possibile portata e dei limiti della conservazione e dell'accesso ai dati delle comunicazioni. In particolar modo, ciò è avvenuto in tema di sorveglianza di massa. Mentre i dati personali di milioni di europei continuavano ad essere conservati dagli Stati membri, la Commissione risultava riluttante nell'intervenire in merito, rifiutandosi di avviare eventuali procedure di infrazione contro gli Stati che facessero ricorso a questo genere di controllo diffuso. La linea adottata dalla Commissione ha trovato poi conferma nella giurisprudenza della nota *data retention saga*, riconducibile sia all'attività creativa della Corte di Strasburgo che di Lussemburgo[44]. In accordo con tale filone giurisprudenziale, in

[42] Ivi, p.to 62: «l'art. 6 della direttiva 2014/41 osta all'emissione […] qualora la normativa di tale Stato membro non preveda alcun mezzo d'impugnazione». Per un'analisi sulla portata delle sentenze *Gavanazov I* e *II*, si permette di rinviare a S. Busillo, *Mutual Recognition in EU Criminal Judicial Cooperation and Its 'Conditional Application' under CJEU's Caselaw on the European Investigation Order (EIO)*, in T. Russo, A. Oriolo, G. Dalia (cur.), *Solidarity and Rule of Law*, Berlin, 2023, 263-277.

[43] Corte giust., *Gavanazov II*, cit., p.ti 31 e 34. A tal riguardo, F. Liguori, *Il principio di mutuo riconoscimento nell'ambito della cooperazione giudiziaria in materia penale: le condizioni di ammissibilità dell'Ordine europeo di indagine penale*, in *Quad. AISDUE*, 2024, 1, 7, fa notare che tale precisazione potrebbe comunque non essere sufficiente in termini di effettività siccome la «disciplina processual-penalista di uno Stato membro potrebbe impedire a degli individui residenti in un diverso Paese dell'Unione di contestare in tale Stato membro la legittimità del procedimento di acquisizione di uno specifico esito probatorio».

[44] Per la Corte europea dei diritti dell'uomo, v. Corte EDU, Grande Camera, no. 58170/13, 62322/14 e 24960/15, *Big Brother Watch e altri c. Regno Unito*, 25-5-2021, p.to 345; Corte EDU, Grande Camera, no. 35252/08, *Centrum för Rättvisa c. Svezia*, 25-

sostanza, i requisiti di necessità e proporzionalità che ammettono un'ingerenza nella riservatezza degli individui non escludono la predisposizione di misure di sorveglianza di massa quando contrapposte a «forme gravi di criminalità o della prevenzione di gravi minacce per la sicurezza pubblica» (scopo legittimo) ed in presenza di efficaci garanzie contro il rischio di abusi e di arbitrii nelle fasi di adozione della misura, della sua esecuzione e del controllo successivo[45].

Pertanto, la *data retention saga* già potrebbe di per sé aggiornare il contenuto delle disposizioni della Direttiva OEI. In caso di richiesta di materiale probatorio da prodursi – o già prodotto – per mezzo di una sorveglianza di massa, verrebbe stabilito dunque che l'autorità di emissione possa disporre l'ordine solo se giustificato dalla necessità di tutelare la sicurezza pubblica, o comunque a fronte di reati gravi. Diversamente, la misura richiesta non sarebbe da considerarsi proporzionata e necessaria. Aldilà di questo specifico apporto, se non altro, l'insieme delle pronunce cui si fa riferimento non consentirebbe comunque di risolvere eventuali dubbi circa il problema del bilanciamento tra le esigenze securitarie e la tutela della *privacy* in ipotesi di comunicazioni criptate, nonché definire l'attuale *status* della proporzionalità in regime di OEI per questo tipo di dato.

Infatti, i ragionamenti e le giustificazioni promanate dalla Corte di giustizia e dalla Corte europea dei diritti dell'uomo finora individuate nella *data retention saga* afferiscono ad un tipo di ingerenza "quantitativa". Ciò che rilevava per le Corti, e che aggravava la situazione di fatto, era il numero di soggetti coinvolti (appunto, una sorveglianza di massa) da cui è discesa la necessità di dotarsi di un parametro "netto" di necessità e proporzionalità dell'ingerenza. Al contrario, nel caso delle comunicazioni criptate, si parlerebbe di una rilevanza "qualitativa" dell'ingerenza. Non si tratta più di una pluralità, magari molto ampia, di soggetti lesi, ma potenzialmente anche di un solo individuo che abbia deciso di fare ricorso a comunicazioni criptate poiché – così si può assumere – desideroso di un maggior livello di riservatezza. Pertanto, è necessario prendere in considerazione quelle pronunce che tengano conto di un'ingerenza che sia considerata più grave non già per il numero di individui coinvolti, bensì per il grado della lesione procurata. Ad esempio, nella decisione della Corte EDU *Podchasov c. Russia*, del febbraio 2024[46], quest'ultima si è espressa sull'istituzione di un sistema

5-2021, p.to 259. Per la Corte di giustizia dell'Unione Europea, v. Corte giust., c-511/18, c-512/18 e c-520/18, *La Quadrature du Net*, sent. 6-10-2020; Corte giust., c-623/17, *Privacy International*, sent. 6-10-2020; Corte giust., c-746/18, *H.K. Prokuratuur*, sent. 2-3-2021; Corte giust., c-140/20, *Commissioner of An Garda Síochána*, sent. 5-4-2022; Corte giust., c-793/19 e c-794/19, *SpaceNet*, sent. 20-11-2022. Per un commento su tale prassi giurisprudenziale, v. 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 *FSJ*, 2022, 3, 105; Id., *La disciplina internazionale ed europea della* data retention *dopo le sentenze* Privacy International *e* La Quadrature du Net *della Corte di giustizia UE*, in *Dir. Un. Eur*, 2021, 1, 93.

[45] V. Corte giust., *Prokuratuur*, cit., p.to 35, sull'interpretazione dell'art. 15, par. 1 della dir. CE n. 2002/58, ovvero sulla nozione di «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».

[46] Corte EDU, no. 33696/19, *Podchasov c. Russia*, 14-2-2024.

DPCE online
ISSN: 2037-6677

di conservazione dei dati che consentiva alle forze dell'ordine di "precettare" la decrittografia dei dati raccolti. Più precisamente, il ricorrente, un utente di Telegram, impugnava la decisione delle autorità russe che aveva imposto alla piattaforma di rendere "in chiaro" le proprie comunicazioni cifrate, creando una situazione di sorveglianza di massa *de facto* vista l'esistenza di un ordine generalizzato riguardante tutti i fruitori della piattaforma. Da una parte, da un punto di vista della "quantità", la Corte ha – al contrario del desiderio di alcuni[47] – ribadito l'ammissibilità della sorveglianza di massa in senso generale. Veniva tuttavia eccepito che, nel caso di specie, la sorveglianza imposta dalle autorità russe ad un operatore privato che offriva servizi di chat crittografate ai propri utenti non potesse essere consentita sulla base di motivi tecnico-procedurali. Specificamente, veniva eccepito che misure meno intrusive avrebbero potuto portare al medesimo risultato.

Dall'altra parte, sotto il profilo della "qualità" dell'ingerenza, la sentenza è preziosa perché si sofferma sulla proporzionalità delle interferenze gravanti sulle comunicazioni criptate. Essa ha infatti precisato che, nell'era digitale, la criptazione delle comunicazioni è particolarmente apprezzabile visto il suo contributo ad «ensuring the enjoyment of other fundamental rights, such as freedom of expression»[48] e che, pertanto, tale elemento debba essere tenuto in conto al momento della disposizione di un'interferenza della riservatezza. Tant'è che il «Podchasov case is straightforward: encryption is vital to the protection of the right to privacy»[49].

In teoria, adottando una visione funzionalistica per la cifratura ed imponendo di "tener in considerazione" anche dei diritti ulteriormente coinvolti, la sentenza *Podchasov c. Russia* informerebbe i criteri di valutazione, *ex* art. 6, par. 1 Direttiva OEI, da parte di quell'autorità di emissione che intenda ottenere dati contenenti comunicazioni criptate. In pratica, non si ritiene che nella sentenza venga fissato un parametro netto

[47] E. Tuchtfeld, *No Backdoor for Mass Surveillance: The European Court of Human Rights Protects the Right to Encrypted Communication*, in *VerfBlog*, 29-2-2024, il quale sostiene che la Corte avrebbe potuto riesaminare il tema della *bulk data retention* e sancirne la illegalità.

[48] Corte EDU, *Podchasov c. Russia*, cit., p.to 76. Cfr. anche ris. del P.E. del 3-10-2017, sulla lotta alla criminalità informatica, 2017/2068(INI), p.to 17, la quale adotta una visione altrettanto funzionalistica, anche se più economico-pratica, sottolineando che «la limitazione dell'utilizzo degli strumenti crittografici o l'indebolimento della loro forza creerà vulnerabilità che possono essere sfruttate per fini criminali e ridurrà la fiducia nei servizi elettronici, il che, a sua volta, danneggerà la società civile e l'industria».

[49] M. van 't Schip, F. Zuiderveen Borgesius, *Podchasov v. Russia: the European Court of Human Rights Emphasizes the Importance of Encryption*, in *EULawAnalysis*, 20-4-2024. Cfr. K. Singh, S. Singh, A. Raj, *The ECtHR in Podchasov v. Russia – Preserving Encryption and Denying Backdoors*, in *Oxford Human Rights Hub*, 27-8-2024, che indicano la sentenza come uno «strong statement against the breakdown [of encryption]»; R. Lakra, *Cracking the Code: How Podchasov v. Russia Upholds Encryption and Reshapes Surveillance*, in *EjilTalk!*, 13-3-2024, il quale afferma che «*Podchasov* is a landmark decision, which safeguards encryption, which has become *sine qua non* for secure and confidential communication in the digital age». In effetti, l'Unione non può ignorare questa sentenza siccome, per la clausola di equivalenza di cui all'art. 52, par. 3 della Carta di Nizza, i diritti enucleati nella Carta (artt. 7 e 8) dovrebbero avere la stessa portata ed una tutela di pari livello (o superiore) rispetto ai diritti della CEDU (art. 8) ed annessa sua giurisprudenza.

come già fatto per la sorveglianza di massa, ove veniva fatto chiaramente riferimento alla natura del reato («grave») o alla entità dell'interesse da bilanciarsi con la *privacy* («sicurezza nazionale»). Pertanto, a fronte di questo limitato apporto, maggiori speranze di definire l'attuale bilanciamento tra riservatezza e sicurezza, nonché i rischi, in seno all'Ordine europeo d'indagine devono essere riposte nell'analisi dell'altrettanto recente caso *EncroChat* dinanzi la Corte di giustizia.

4. Il caso *EncroChat*: la potenziale identificazione con una sorveglianza di massa e brevi cenni alle prime pronunce nazionali

Dal 1° aprile 2020 sino al 13 giugno 2020 le autorità di Francia e Paesi Bassi hanno condotto una rilevantissima operazione che ha portato all'intercettazione di dati e comunicazioni criptate provenienti dai server e dai criptofonini della società *EncroChat*. Le stime suggeriscono che è stata eseguita un'attività di sorveglianza su circa 60.000 carte SIM, fornite da un operatore olandese, le quali risultavano registrate nel sistema omonimo e che utilizzavano internet per consentire chiamate, messaggi, ecc. Precisamente, i telefoni in cui queste erano alloggiate venivano sottoposti ad un aggiornamento *software* fittizio, che ha portato all'inoculazione di un *trojan* installato dalla polizia, quindi senza l'ausilio dell'operatore telefonico. Al netto della cooperazione internazionale ed interdisciplinare in seno alla SIC franco-olandese, che ha determinato il successo dell'operazione, un fatto peculiare è che lo Stato francese non richiedeva alcun tipo di assistenza giudiziaria presso gli Stati membri in cui erano ubicati i diversi soggetti coinvolti dall'attività captativa in questione, né provvedeva a notificare loro l'esecuzione delle suddette operazioni (artt. 30 e 31 Direttiva OEI).

Dopo la collazione dei primi dati, risultava che il 63,7% dei telefoni attivi in Francia era stato sicuramente utilizzato per scopi criminali, mentre i restanti dispositivi erano parzialmente inattivi o non ancora valutati. Tenuto conto delle statistiche ottenute nel primo mese dell'operazione, la procura della Repubblica francese e il tribunale competente hanno ipotizzato che gli utenti di *EncroChat* fossero «quasi esclusivamente clientela criminale»[50], di fatto dando vita ad una presunzione di illegalità per le attività condotte dai rimanenti utenti. In un secondo momento, le autorità francesi, tipicamente su OEI proveniente da altre autorità europee a quel punto informate dell'operazione, hanno provveduto ad un'attività di trasferimento dei dati allo scopo di lasciar condurre o proseguire efficacemente azioni penali in altri Stati. Circa le modalità di acquisizione delle comunicazioni, la Francia ha deciso di apporre il segreto di Stato al fine di preservare le opportunità investigative future.

Quest'ultima circostanza, sebbene ovviamente incisiva per i diritti di difesa, non dovrebbe essere inammissibile in via di principio ai sensi della

[50] Comunicato stampa congiunto di Eurojust ed Europol, *Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe*, 2-7-2020; Comunicato stampa di Europol, *Dismantling encrypted criminal EncroChat communications leads to over 6 500 arrests and close to EUR 900 million seized*, 27-6-2023.

DPCE online
ISSN: 2037-6677

CEDU[51]. Affinché sia considerata legittima, una misura limitante i diritti della difesa – ad es. la garanzia del contraddittorio – deve essere strettamente necessaria[52]. Inoltre, al fine di garantire all'imputato un giusto processo, le eventuali difficoltà causate alla difesa devono essere sufficientemente controbilanciate dalle procedure seguite dalle autorità giudiziarie[53]. Tuttavia, né la stretta necessità né i citati "correttivi" sembra siano occorsi nella maggior parte dei casi oggetto di indagine. Pertanto, le operazioni sollevano dubbi in relazione alla disciplina sulla apprensione dei dati e ad alla segretezza delle telecomunicazioni, nonché ai rimedi ammessi nel caso di specie.

Ulteriormente, una delle difficoltà d'inquadramento delle indagini in parola è se queste costituiscano una sorveglianza di massa impropria, come anche tenuto in conto da parte dell'AG Ćapeta nel procedimento dinanzi la Corte di giustizia. Le operazioni, in effetti, avrebbero coinvolto un intero sistema di telecomunicazioni per vari mesi, coinvolgendo una pluralità di utenti che supera le decine di migliaia di unità. Esse integrerebbero *prima facie* una serie di parametri descritti dalla Corte EDU per l'individuazione dei casi di sorveglianza di massa: i) le comunicazioni intercettate abbiano coinvolto una pluralità di individui, la maggior parte delle quali non è di interesse per le autorità competenti; ii) la captazione massiva sia stata generalmente diretta alle comunicazioni internazionali; iii) lo scopo dichiarato dell'intercettazione massiva sia il monitoraggio di comunicazioni di individui posti al di fuori della giurisdizione dello Stato di appartenenza dell'autorità e; iv) l'intercettazione appaia finalizzata alla raccolta di informazioni di *intelligence* all'estero[54].

In prima battuta, va riconosciuto che le autorità hanno operato nei confronti di specifici utenti in modo "proattivo", avendoli già individuati in precedenza. In seconda battuta, è doveroso ricordare che Europol ha individuato tra gli obiettivi dell'operazione anche l'analisi dell'estensione delle reti di criminalità organizzata e che, pertanto, è stato eseguito un monitoraggio sì generalizzato, ma in un ambiente "circoscritto" (il *server*) e con uno scopo predefinito. Ciò ha consentito ad alcuni commentatori di riconoscere che l'operazione presenti invero elementi tipici di una sorveglianza mirata e non già di massa, con la riserva che «it cannot be assumed that the surveillance of such a large number of potential suspects

[51] Nella pronuncia della Corte EDU, Grande Camera, no. 27052/95, *Jasper c. Regno Unito*, 16-2-2000, p.to 52, è chiarito in qualsiasi procedimento penale possono presentarsi interessi concorrenti circa la divulgazione di queste informazioni. In alcuni casi, può essere necessario nascondere determinate prove alla difesa al fine di preservare i diritti fondamentali di altre persone o di salvaguardare un interesse pubblico rilevante, come la sicurezza nazionale o il mantenere segreti i metodi di indagine della polizia sui reati.

[52] Corte EDU, no. 21363/93, 21364/93, 21427/93 e 22056/93, *Van Mechelen e altri c. Paesi Bassi*, 12-4-1997, p.to 58; Corte EDU, no. 39647/98 e 40461/98, Grande Camera, *Edwards e Lewis c. Regno Unito*, 22-7-2004, p.to 46.

[53] Corte EDU, no. 21022/04, *Natunen c. Finlandia*, 31-3-2009, p.to 40.

[54] Corte EDU, *Big Brother Watch e altri c. Regno Unito*, cit., p.ti 344-347; Corte EDU, *Centrum för Rättvisa c. Svezia*, cit., p.ti 258-259.

was based on facts in each individual case»[55]. Tuttavia, da un lato, si ritiene che sia occorsa indebitamente una vera e propria presunzione di attività illecite per "chiunque" usasse *EncroChat* – in parte andando contro il diritto dell'Unione Europea stesso, segnatamente contro il considerando 20 del Regolamento sui servizi digitali del 2022[56] – e che, dall'altro, anche la qualificazione dell'operazione come attività "mirata" sia un fattore non decisivo. Infatti, come in altra sede sostenuto, «a fronte della irrinunciabilità dei diritti umani nonché delle regole di bilanciamento dei diritti non assoluti prescritte dall'art. 52 CDFUE e dalla giurisprudenza costante della Corte EDU» i criteri decisionali per la proporzionalità e la necessità fissati nel filone giurisprudenziale sulla protezione dei dati «sarebbero da considerarsi quali regole generali e trasversali, una sorta di assioma comune, di cui sarà richiesta l'applicazione prescindendo dalla natura del provvedimento, indifferentemente generalizzato (*mass surveillance*) o specifico»[57]. Ne discenderebbe l'applicazione nel caso di specie di tutta la rilevante giurisprudenza europea in materia, con la conseguenza che le autorità francesi avrebbero dovuto necessariamente dimostrare la rilevanza del caso per la «sicurezza nazionale» per giustificare la violazione della riservatezza mediante captazioni di dati informatici criptati – cosa tuttavia solo presumibile e non dimostrabile vista la secretazione delle operazioni in nome della sicurezza nazionale francese.

Ciò posto, l'esistenza di un'operazione su così vasta scala, con ampia mole di dati condivisa tra autorità giudiziarie UE ed extra-UE, non poteva che provocare reazioni miste, registrate in una pluralità di procedimenti

[55] R. Stoykova, *Encrochat: The Hacker with a Warrant and Fair Trials?*, in 46 *FSIDIIN* 1, 3 (2023). V. anche le considerazioni generali di D. Curtotti *et al.*, *Piattaforme criptate e prove penali*, in *SP*, 2023, 6, 173, 183, per i quali, in sostanza, anche quando un'ipotetica indagine non sia diretta ad acquisire flussi comunicativi di sistemi informatici di per sé «determinati» – essendo che comunque tutti i flussi transitano sulla piattaforma – esisterà comunque «un *target* di riferimento, così come esiste ed è sufficientemente individuato un "sistema" da attenzionare, sia pur virtuale ed etereo, quale è il *server*». In effetti, qui è possibile richiamare la pronuncia Corte EDU, Grande Camera, no. 47143/06, *Zakharov c. Russia*, 4-12-2021, p.to 264, ove si fa riferimento, nella emanazione di un decreto autorizzativo delle intercettazioni non solo del destinatario della captazione, ma anche della «la tipologia di ambienti» ove questa viene condotta. In tal senso il *server* potrebbe essere considerato come uno spazio chiuso su cui transitano flussi comunicativi. Tuttavia, gli stessi autori riflettono sul fatto che non si comprende come un giudice possa autorizzare un'attività di intercettazione (telematica) nella consapevolezza che, così facendo, sta automaticamente consentendo la captazione a tappeto di "tutti" i flussi comunicativi veicolati dal *server* oggetto di intercettazione e tutto ciò in assenza dei necessari requisiti stabiliti dalla legge (p. 185).

[56] Reg. UE n. 2065/2022 del P.E. e del Cons. del 19-10-2022, relativo a un mercato unico dei servizi digitali, considerando 20: «Il solo fatto che un servizio offra trasmissioni cifrate o qualsiasi altro sistema che renda impossibile l'identificazione dell'utente non dovrebbe di per sé essere considerato come un'agevolazione di attività illegali».

[57] Sia consentito il rinvio a S. Busillo, *Conservazione e produzione della prova digitale nella nuova disciplina europea: il potenziale disallineamento con i principi espressi dalla giurisprudenza di settore*, in *FSJ*, 2023, 3, 27, 43.

DPCE online
ISSN: 2037-6677

penali paralleli in cui, collettivamente, i giudici di Francia[58], Germania[59], Italia[60], Norvegia[61], Paesi Bassi[62] e Regno Unito[63] sono stati tenuti a rispondere ad incertezze di natura sostanziale e procedurale. In particolare, più corti sono state chiamate a giudicare sia sull'opportunità delle intercettazioni che sull'impraticabilità di esercitare i diritti della difesa a causa dell'impossibilità di conoscere il *modus operandi* degli inquirenti. A tal riguardo, è interessante notare che, secondo taluni, è stato fatto un uso artificioso dell'Ordine europeo d'indagine, impiegato meramente come "timbro" («rubber-stamp») per formalizzare operazioni svolte per lo più in via ufficiosa e riservata[64].

In massima sintesi, ad accentuare un *favor* verso la sicurezza nel bilanciamento tra questa e la riservatezza, le varie pronunce nazionali tendono ad insistere collettivamente sulla costanza di una doppia presunzione su: 1) la legittimità delle operazioni condotte nello Stato straniero di esecuzione dell'OEI, su cui lo Stato d'emissione non potrebbe comunque sindacare; 2) l'illiceità delle attività degli utenti di *EncroChat*, tra l'altro senza doversi ravvisare l'esistenza di requisiti quale il "reato grave" o "indizi concreti" nei confronti di soggetti non ancora identificati come criminali dalle autorità, che ha di fatto reso inopponibile il diritto alla *privacy* degli interessati. Da questa seconda circostanza deriva implicitamente che il grado di necessità e proporzionalità richiesto per la valida emissione degli ordini europei d'indagine nel caso di specie sia di livello inferiore rispetto a quello altrimenti categoricamente previsto dalla nota *data retention saga*. Le pronunce, inoltre, hanno sostenuto la correttezza del bilanciamento operato dalle autorità di emissione dell'OEI non solo in forza delle presunzioni richiamate, ma anche di una pregnante esigenza securitaria, ritenuta nel filone francese non contrastante con i diritti costituzionali del cittadino, tra cui quello alla riservatezza, ma anzi ritenendola espressione di una conciliazione equilibrata tra esigenze di senso opposto[65]. Va però considerato che il filone francese della vicenda *EncroChat* non può dirsi concluso dato che già nel 2020 alcuni degli interessati avevano deciso di rivolgersi alla Corte EDU per chiedere l'accertamento di una violazione del diritto al giusto

[58] Corte costituzionale francese, *déc.* n. 2022-987 QPC *du* 8-4-2022; Corte di cassazione francese, Camera penale, ar. 11-10-2022, n. 21-85.148.
[59] Tribunale regionale superiore di Brema, 1 Ws 166/20, 18-12-2020; Tribunale regionale superiore anseatico di Amburgo, 1 Ws 2/21, 21-3-2021, in part. p.to 82; BGH, 5 StR 457/21, 2-3-2022, p.to 37. Cfr. anche BVerfG,, 2 BvR 2500/09, 2 BvR 1857/10, 7-12-2011, p.ti 115-116.
[60] Cass., Sez. VI, n. 44154, 2-11-2023; Cass., SS.UU., n. 23755, *Giorgi*, 29-2-2024; Cass., SS.UU., n. 23756, *Gjuzi*, 29-2-2024; Cass., Sez. I, n. 13535, 12-3-2024. Cfr. V. Scarlato, *Commento alle sentenze delle Sezioni Unite relative al caso dei c.d. "criptofonini"*, in *Riv. Camm. Dir.*, 2024, 1, 10; L. Filippi, *Le S.U. ammettono le prove francesi sui criptofonini acquisite con l'ordine europeo di indagine*, in *PenaleDP*, 1-3-2024.
[61] Corte suprema norvegese, HR-2022-1314-A, 30-6-2022, p.ti 26, 39 e 42, ove si nota che «privacy protection is generally a strong value in Norway».
[62] Corte Suprema dei Paesi Bassi, n. 913, 13-6-2023, p.to 6.6.
[63] Corte d'appello d'Inghilterra e Galles, [2021] EWCA Crim 128, *A, B, D & C*, 5-2-2021, p.ti 4-5, 56 e 63.
[64] Così T. Wahl, *Germany: Federal Court of Justice Confirms Use of Evidence in EncroChat Cases*, in 1 *Eucrim* 36, 37 (2021).
[65] Corte costituzionale francese, *déc.* n. 2022-987 QPC, cit., p.ti 19-20.

processo (art. 6 CEDU), alla *privacy* (art. 8 CEDU) e ad un ricorso effettivo (art. 13 CEDU). La Corte di Strasburgo ha tuttavia ritenuto nel settembre 2024 che ambedue le domande vadano considerate inammissibili per mancato esaurimento delle vie di ricorso interne *ex* art. 35, par. 1 CEDU[66]. Pertanto, sarà necessario attendere se e come i ricorrenti potranno procedere per portare avanti i propri interessi.

Ad ogni modo, può dirsi che il risultato della combinazione tra le attività immediatamente operative e la valutazione fatta dalle corti nazionali è stato quello di aver accresciuto il rischio di importare un elemento "patologico" a detrimento della riservatezza – come nel caso di materiale probatorio formatosi nello Stato di esecuzione ed eventualmente acquisito in modo indebito – all'interno del procedimento penale dello Stato di emissione, quale effetto inevitabile, ed indesiderato, del principio del reciproco riconoscimento delle decisioni giudiziarie sottostante la Direttiva OEI. Ciononostante, non facendo seguito a quanto sinora rilevato, dalla Germania è originato in un secondo momento il rinvio pregiudiziale che ha portato la "questione" *EncroChat* dinanzi la Corte di giustizia, alla quale si chiedeva un intervento chiarificatore su una molteplicità di punti, tra cui anche l'intercettazione dei dati, la sorveglianza di massa e la tutela dei diritti fondamentali degli intercettati.

5. L'intervento della Corte di giustizia: il disallineamento tra le osservazioni del giudice di rinvio e le conclusioni dell'Avvocato generale

Nella sua decisione del 19 ottobre 2022, il Tribunale del Land di Berlino (*Landgericht Berlin*) ha sospeso un processo contro un imputato perseguito per traffico di droga sulla base di dati recuperati nell'operazione *EncroChat*. Discostandosi dalle altre corti tedesche, già nel 2021 il Tribunale aveva preso una decisione che sosteneva l'inammissibilità dei dati raccolti all'interno di procedimenti penali nazionali. I giudici di Berlino nutrivano dubbi sulla compatibilità dell'OEI d'emissione tedesca con l'art. 6, par. 1, lett. b) Direttiva OEI, in quanto la modalità di indagine in sé non avrebbe potuto essere autorizzata in un caso analogo in Germania. Per quanto riguarda le conseguenze generate da un'eventuale violazione del diritto dell'UE, il Tribunale del Land ha ritenuto che i principi di effettività ed equivalenza (che limiterebbero l'autonomia processuale degli Stati membri in materia probatoria) come interpretati dalla precedente giurisprudenza della Corte di giustizia (*Steffensen*)[67] comportino, quale sanzione, l'inammissibilità delle prove nel caso in esame. Nel merito, lo stesso evidenziava la mancanza di trasparenza da parte delle autorità competenti dato che, a causa della mancata divulgazione sull'approccio tecnico tenuto dalla Francia, non era stato possibile valutare se i dati richiesti fossero integri o alterati. In aggiunta, il rifiuto delle agenzie dell'UE e delle autorità di contrasto

[66] Corte EDU, no. 44715/20 e 47930/20, *A.L. c. Francia* e *E.J. c. Francia*, 24-9-2024.
[67] Corte giust., c-276/01, *Steffensen*, sent. 10-4-2003, in cui viene stabilito che il solo fatto che i dati utilizzati non possano essere verificati dalla difesa tramite un proprio tecnico sarebbe sufficiente per concludere circa la loro inutilizzabilità come prova.

DPCE online
ISSN: 2037-6677

tedesche di consegnare parti del fascicolo alla difesa aveva reso la corretta ricostruzione dei fatti ancora più difficile nel corso del procedimento. Ciò avrebbe impedito sia il controllo *ex ante*, da parte di un'autorità indipendente, sia il controllo *ex post*, sotto forma di esercizio del diritto della difesa mediante la presentazione di prove in contraddittorio tra le parti.

Vieppiù, secondo il Tribunale di Berlino, le altre corti tedesche avevano considerato impropriamente di attribuire maggiore importanza al perseguimento penale a discapito dei diritti fondamentali dei singoli. Secondo il giudice del rinvio, la massima della giurisprudenza della Corte di giustizia che vieta la conservazione generalizzata dei dati – eccetto per reati gravi o per fatti che minaccino la sicurezza nazionale – deve ritenersi applicabile, comportando l'inammissibilità delle prove (*Prokuratuur*)[68]. Pertanto, lo stesso Tribunale ha sottoposto alla Corte un totale di 14 questioni sull'interpretazione della Direttiva OEI. Senza esaminarle tutte nel dettaglio, venivano chieste in particolar modo delucidazioni sul se l'OEI tedesco fosse proporzionato e necessario, considerando che si riferiva alla ricezione di tutti i dati *EncroChat* degli utenti sul territorio tedesco senza che però fossero stati previamente identificati i singoli sospetti. In aggiunta, questione fondamentale per questa disamina, veniva chiesto se, in ipotesi di comunicazioni cifrate, per soddisfare la proporzionalità e la necessità richieste per l'emissione dell'OEI, di cui all'art. 6, par. 1, il giudice nazionale debba constatare la presenza di indizi concreti di un reato grave oppure se siano sufficienti al riguardo indizi relativi all'esistenza di plurimi reati commessi da persone non ancora identificate (seconda questione, lett. a). Veniva ulteriormente chiesto se la Direttiva osti a che un OEI sia stato emesso rendendo inconoscibile l'integrità dei dati ottenuti tramite la misura di intercettazione a causa della riservatezza delle modalità operative (seconda questione, lett. b).

Nell'autunno 2023, l'attività di *amicus curiae* da parte dell'AG Ćapeta sembra in sostanza aver obiettato alle osservazioni del giudice di rinvio[69]. Con riguardo alla valutazione di proporzionalità, viene riconosciuto dall'AG Ćapeta che questa è disciplinata «principalmente dal diritto nazionale», ma anche da quello dell'UE con conseguente applicazione della giurisprudenza europea, se del caso[70]. Tuttavia, nell'ipotesi richiamata dal giudice di rinvio, per l'Avvocato generale non sarebbe applicabile la giurisprudenza rilevante in materia di sorveglianza di massa e tutela dei dati siccome «i dati da trasferire non sono stati raccolti in modo indiscriminato presso l'intera popolazione»[71]. Come in precedenza statuito (*supra* Sezione 4), tale affermazione non è condivisa né nella qualificazione dell'attività come "mirata", né nella impossibilità di applicare la giurisprudenza sulla *data retention*, la quale invece può comunque essere attuata in via analogica.

[68] Corte giust., *Prokuratuur*, cit., p.to 35.
[69] Corte giust., c-670/22, *M.N. (EncroChat)*, conc. dell'AG Tamara Ćapeta 26-10-2023. Per un commento, v. L. Bernardini, *On Encrypted Messages and Clear Verdicts – The EncroChat Case before the Court of Justice (Case C-670/22, MN)*, in *EU Law Live*, 21-5-2024.
[70] Corte giust., conc. dell'AG Tamara Ćapeta, cit., p.ti 82 e 88-95.
[71] Ivi, p.to 96.

Quanto alle conseguenze dell'accertamento che un OEI sia stato emesso in violazione dei requisiti previsti dalla omonima Direttiva, l'Avvocato generale tende a liquidare la questione dato che «il diritto dell'Unione non disciplina l'ammissibilità delle prove nei procedimenti penali»[72]. Senz'altro, viene riconosciuta la competenza dell'UE di legiferare in materia *ex* art. 82, par. 2, lett. a) TFUE, ma ciò non impedisce all'Avvocato generale di sottolineare che «il diritto dell'Unione non attribuisce ai singoli alcun diritto in riferimento all'(in)ammissibilità delle prove. I principi di equivalenza e di effettività non trovano applicazione»[73]. Rimettendo tale valutazione nelle mani del diritto nazionale – mediante mezzi di impugnazione garantiti *ex* art. 14 Direttiva OEI – viene al massimo considerato che, nelle materie in cui si applica il diritto dell'Unione, le disposizioni interne dovranno conformarsi agli artt. 47 e 48 Carta di Nizza[74]. Tuttavia, dalla prospettiva della tutela della *privacy*, questa eventualità non sembra sufficientemente appagante dato che questa non risulta minimamente chiamata in causa; né le conclusioni forniscono una risposta chiara al secondo quesito, lett. a), circa la valutazione di proporzionalità su cui il giudice di rinvio chiedeva un'interpretazione poiché, sì, deve tenersi «conto dei diritti della persona sottoposta a indagini o imputata», ma «la Corte non può sostituirsi all'autorità di emissione o al giudice nazionale dell'impugnazione nella valutazione della proporzionalità di un determinato OEI»[75].

In generale, con riguardo alle conclusioni sinora sinteticamente esaminate, sotto alcuni aspetti si osserva una posizione quasi trincerata sulle lacune e zone grigie della Direttiva OEI, quando sarebbe stato invece preferibile chiarirle. Segnatamente, l'Avvocato generale avrebbe potuto restringere l'ampio margine di discrezionalità, specificando taluni criteri di valutazione che le autorità nazionali competenti avrebbero (quantomeno) potuto indicativamente seguire nel bilanciamento tra sicurezza e diritto alle comunicazioni criptate. Inoltre, non sono stati previsti "sbocchi" processuali per un potenziale controllo *ex ante* delle misure, ancor prima che intervenga l'interferenza alla *privacy*. In altri aspetti è poi osservabile un atteggiamento estremamente fermo verso la sovranità statale ed il mutuo riconoscimento, anche perché in via preliminare è stato chiarito che «l'autorità di emissione non può rimettere in discussione la legittimità delle misure mediante le quali

[72] Ivi, p.to 117.
[73] Ivi, p.ti 118-120 e 129. Tale scelta invero potrebbe essere considerata alla luce della «sensibilità che le materie disciplinate nello Spazio [europeo di libertà, sicurezza e giustizia] rivestono per la sovranità degli Stati» tant'è che, «quando si tratta di iniziative effettuate nel quadro della cooperazione giudiziaria penale», trova applicazione il principio di sussidiarietà sancito dall'art. 69 TFUE e, più notoriamente, dall'art. 12 TUE e dal Protocollo 2 allegato al Trattato di Lisbona. Così A. Damato, *La cooperazione giudiziaria in materia penale*, in G. Tesauro (dir.) P. De Pasquale e F. Ferraro (cur.), *Manuale di Diritto dell'Unione europea*, vol. II, Napoli, 2021, 339-340.
[74] Corte giust., conc. dell'AG Tamara Ćapeta, cit., p.to 127. Nel caso di specie, riguardante le comunicazioni, forse sarebbe stato opportuno anche citare gli artt. 7 e 8 Carta di Nizza.
[75] Ivi, p.ti 76 e 83.

DPCE online
ISSN: 2037-6677

lo Stato di esecuzione ha raccolto le prove»[76]. Tant'è che solo in caso di accertamento dell'illegittimità dell'atto sottostante in un procedimento nello Stato d'esecuzione – controllo *ex post* che la persona interessata deve poter instaurare ai sensi del citato art. 14 Direttiva OEI – l'autorità di emissione potrebbe eccepirne l'illegittimità[77]. Infatti, il presupposto che tutti gli Stati membri rispettino i diritti fondamentali può essere certamente «confutato in un caso specifico», senza però che si possa «rimettere in discussione il principio della fiducia reciproca sotteso all'OEI e ad altri strumenti di cooperazione in materia penale»[78]. Pertanto, l'attività dell'AG Ćapeta ha contribuito solo limitatamente a chiarire i dubbi su quei "rischi genetici" legati all'OEI.

6. La mancata identificazione di dettagliati criteri di proporzionalità per l'emissione dell'OEI in ipotesi di comunicazioni criptate quale rischio per la riservatezza

Nella propria sentenza pubblicata il 30 aprile 2024[79], la Corte di giustizia ha in buona parte rispettato i suggerimenti presentati da parte dell'Avvocato generale, divergendo parzialmente solo sui temi legati al giudizio di ammissibilità della prova, che era stato escluso categoricamente dall'ambito applicativo della Direttiva OEI nelle conclusioni di quest'ultimo.

Per quanto concerne la seconda questione, lett. a), del giudice di rinvio – ovvero se, in ipotesi di captazione di comunicazioni crittografate già in possesso delle autorità competenti dello Stato di esecuzione, i requisiti di proporzionalità e necessità *ex* art. 6, par. 1 Direttiva OEI debbano essere soddisfatti solo in caso di presunzione di «reato grave» supportato da indizi concreti – la Corte ritiene che tale requisito non sia previsto dalla Direttiva, contribuendo tra l'altro ad una tendenza confermata in una pronuncia resa il 4 ottobre 2024 e riguardante la Direttiva 2016/680/UE[80]. Di converso, è sufficiente che siano presenti indizi sull'esistenza di plurimi reati commessi da «persone non ancora identificate». Vero è, però, che questi requisiti possono essere previsti nell'ordinamento dello Stato di emissione, alla cui autorità è demandata l'iniziale valutazione di proporzionalità e necessità[81].

[76] Ivi, p.to 22. Sull'argomento, v. G. Dalia, *La natura transnazionale della* digital evidence *tra richieste di cooperazione e pretese di sovranità. Un equilibrio necessario per il contrasto alle nuove forme di criminalità*, in *i-Lex*, 2023, 16, 1, 37.

[77] Corte giust., conc. dell'AG Tamara Ćapeta, cit., p.to 48.

[78] Ivi, p.to 51.

[79] Corte giust., c-670/22, *M.N. (EncroChat)*, sent. 30-4-2024.

[80] Corte giust., c-548/21, *Bezirkshauptmannschaft Landeck*, sent. 4-10-2024, p.ti 96-97, per cui l'accesso da parte della polizia ai dati contenuti in un telefono cellulare non è una misura da riservare necessariamente alla lotta contro i reati gravi, bensì «nei confronti dei reati in generale». L'accesso deve, però, essere disposto *ex ante* da un giudice (o da un'autorità indipendente) con provvedimento motivato e resta soggetto al principio di proporzionalità e del diritto ad un ricorso effettivo *ex post*. Cfr. Corte EDU, no. 4088/21, *Neziric c. Bosnia-Erzegovina*, 5-11-2024, in cui si è arrivati ad un risultato opposto per via della violazione del segreto professionale dell'avvocato ricorrente.

[81] Corte giust., *EncroChat*, cit., p.ti 82-83 e in part. 89.

Ciò posto, al contrario di quanto avvenuto con la sorveglianza di massa, dove si citavano «gli obiettivi della lotta contro le forme gravi di criminalità o della prevenzione di gravi minacce per la sicurezza pubblica»[82] come necessaria giustificazione per tali misure, la Corte ha rifuggito la possibilità di specificare da sé i parametri di cui all'art. 6, par. 1 Direttiva OEI. In caso di comunicazioni criptate, i giudici di Lussemburgo sembrano abbiano inteso di evitare la creazione di una "proporzionalità europea" uniforme per tutti gli Stati, come invece osservato nella *data retention saga*, senza quindi bilanciare in maniera univoca la *privacy* con la sicurezza nel caso in esame[83].

Invero, preme sottolineare che, con riguardo alla riservatezza, le nozioni di cui all'art. 6, par. 1, lett. a) – proporzionalità e necessità – sarebbero di per sé già contenute nell'art. 8 CEDU (regola speciale per questo peculiare diritto) sotto l'espressione «ingerenza […] necessaria in una società democratica», che è stata interpretata nel senso che la norma richiede che qualsiasi intrusione nella vita privata e familiare debba essere non solo prevista dalla legge in forza di scopi legittimi, ma interpretata in modo restrittivo. In più la Corte EDU ha chiarito che l'esigenza di comprimere la riservatezza debba essere stabilita in modo «convincente»[84]. Nel caso della Direttiva, viene evidentemente predisposto un controllo *ex ante* in capo all'autorità di emissione, finalizzato a prevenire che occorra una lesione ingiustificata dei diritti fondamentali dell'individuo, cioè non sorretta da disposizioni nazionali disposte a tutela di interessi significativi quali l'ordine pubblico. Per effetto del principio *forum regit actum*, sottostante l'intera Direttiva, un ordine europeo così "valutato" ed emanato sarebbe presuntivamente legittimo e da ciò discenderebbe l'obbligo di esecuzione da parte dell'autorità di esecuzione. Tuttavia, la valutazione in questione sembra godere di un ampio margine di apprezzamento a beneficio dell'autorità di emissione, dato che la Direttiva non fa alcun riferimento al principio della riserva di legge *ex* art. 8 CEDU, o comunque a "standard valutativi minimi", né si aggancia alla giurisprudenza di Strasburgo che pure ha sancito un obbligo di interpretazione appunto restrittiva delle ingerenze ammissibili nei confronti dei diritti fondamentali[85]. Da una parte, il margine

[82] V. Corte giust., *Prokuratuur*, cit., p.to 35, sull'interpretazione dell'art. 15, par. 1 Dir. CE n. 2002/58, ovvero sulla nozione di «una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale, della difesa, della sicurezza pubblica».

[83] Tuttavia, se pure l'avessero fatto, la direzione intrapresa dal legislatore europeo con il Regolamento provvisorio contro la pedopornografia – ove la cifratura è derogabile per il contrasto a questo tipo di fenomeno criminoso (Sezione 2) – suggerirebbe che la Corte avrebbe, forse, dettato una soglia "meno alta" della sicurezza nazionale attestata nella *data retention saga*.

[84] Corte EDU, Plenaria, no. 5029/71, *Klass e altri c. Germania*, 6-9-1978, p.to 42. Collettivamente, la necessità/proporzionalità, la riserva di legge e la presenza di scopi legittimi (es. sicurezza nazionale e ordine pubblico) costituiscono un «three-steps test» secondo P. Vogiatzoglou, *Mass Surveillance, Prective Policing and the Implementation of the CJUE and ECtHR Requirement of Objectivity*, in 10(1) *EJLT* 1, 5 (2019).

[85] Corte EDU, no. 11801/85, *Kruslin c. Francia*, 24-4-1990, p.ti 27 e 30. In questo modo, nell'interesse dell'indagato o imputato, sarà possibile dare maggiore prevedibilità della legge, ovvero dare certezza al diritto, quale scopo ultimo della riserva di legge di cui all'art. 8, par. 2 CEDU.

DPCE online
ISSN: 2037-6677

d'apprezzamento potrebbe addirittura considerarsi come un elemento decostruttivo della mutua fiducia; dall'altra, l'enfasi posta sul diritto nazionale dello Stato d'emissione implica che notevoli problematiche applicative potrebbero derivare da una disciplina interna che sia carente in materia. Senz'altro, si potrebbe parlare di "eccesso" di tale margine anche perché, si ritiene, quest'ultimo venga scarsamente temperato dall'azione dell'autorità di esecuzione (*infra*), con chiare ripercussioni sulla tutela della riservatezza, alla quale potranno essere opposte abbastanza agevolmente esigenze di sicurezza – come in effetti constatato nella casistica nazionale della vicenda.

Ad ogni modo, quello che residua dalla sentenza *EncroChat* è la sola "proporzionalità nazionale", che varia da Stato a Stato, a seconda dell'ordinamento di questi. Va da sé che da questa frammentazione della idea di "misura proporzionata" deriverà anche una maggiore incertezza del diritto. Cioè, gli indagati o imputati – non potendosi aspettare uniformità valutativa in tutti gli Stati membri sull'opportunità di un'ingerenza nei confronti della propria *privacy* – saranno talvolta più tutelati talvolta meno tutelati, a seconda dello Stato che procede[86]. Sotto questo punto di vista la Corte di giustizia avrebbe magari potuto osare di più, astenendosi dal demandare la questione alle corti nazionali, come pure avrebbe potuto esprimersi sulla natura delle operazioni a differenza di quanto fatto dall'Avvocato generale. A tal riguardo, la qualificazione dell'attività di intercettazione quale sorveglianza di massa avrebbe determinato l'applicazione al caso di specie della giurisprudenza europea rilevante in materia.

Il silenzio dei giudici di Lussemburgo non è comunque passato inosservato allo stesso giudice di rinvio, che ha proposto un altro rinvio pregiudiziale allo scopo di definire alcuni aspetti rimasti poco chiari nella pronuncia[87]. In particolare, il Tribunale regionale di Berlino ha chiesto delucidazioni su se l'art. 6, par. l, lett. a) Direttiva OEI osti ad un ordine qualora «l'intercettazione effettuata dallo Stato di esecuzione riguardi *tutti* gli utenti di un determinato servizio di comunicazione» e quando «venga richiesto, tramite l'OEI, il trasferimento dei dati relativi a *tutti* gli indirizzi utilizzati sul territorio dello Stato di emissione» (enfasi aggiunta). Tuttavia, la causa è stata cancellata dal ruolo lo scorso 3 settembre 2024 in presenza di problematiche circa l'imperativa celerità e la ricusazione del giudice di rinvio, aspetti di cui si è venuto a capo con altra ordinanza della Corte di giustizia richiamata nell'ordine di cancellazione[88].

---

[86] V. anche Corte giust., *Encrochat*, cit., p.to 95. Su tale tema, v. D. Marrani, *Protezione della riservatezza, comunicazioni elettroniche e perseguimento di «reati gravi» nell'UE alla luce della giurisprudenza della Corte di giustizia*, in A. Oriolo, A.R. Castaldo A. Di Stasi, M. Nino (cur.), *Criminalità transnazionale e Unione europea*, Napoli, 2024, 741-758.

[87] Domanda di pronuncia pregiudiziale proposta dal *Landgericht* di Berlino il 14-11-2023 (c-675/23, *Staatsanwaltschaft Berlin II*). In verità, nel momento in cui la Corte di giustizia ha ammesso in *EncroChat* che un OEI finalizzato all'ottenimento di dati cifrati sia ammesso anche contro soggetti ancora «da identificare», ci si deve chiedere se stia anche implicando che l'operazione sia stata una (legittima) sorveglianza di massa.

[88] Corte giust., c-288/24, *Stegmon*, ord. 4-7-2024.

6.1 La centralità dei diritti di difesa ed il ruolo secondario della privacy: la predisposizione di tutele solo incidentali e parziali

Con riguardo alla seconda questione, lett. b), la Corte ha invece rilevato che lo stesso art. 6 Direttiva OEI non osta all'emissione di un OEI «neppure laddove l'integrità dei dati ottenuti tramite la misura di intercettazione non possa essere verificata a causa della riservatezza delle basi tecniche che hanno permesso l'attuazione di tale misura», come accaduto con la secretazione francese. Tuttavia, ribadendo l'importanza della presenza di ricorso effettivo a pena di non legittimità dell'OEI (come già statuito in *Gavanazov II*)[89], ciò è ammesso solo nel caso in cui il diritto ad un processo equo venga garantito nel corso del procedimento penale[90]. Pertanto, l'art. 6, par. 1 Direttiva OEI non esclude *ex ante* l'emissione di un OEI per cui le modalità di formazione della prova non possono essere note alla difesa, ma richiede che sia garantito il ricorso *ex post* di cui all'art. 14 Direttiva OEI allo scopo di verificare l'integrità delle prove fornite. Anche qui il rischio "genetico" della Direttiva, per il quale è dato un diritto di ricorso solo successivo alla potenziale lesione del diritto, sembra purtroppo non superato.

Eppure, al netto di quanto precede, l'aspetto realmente innovativo del giudizio *EncroChat* risiede nella posizione assunta dalla Corte in merito all'ammissibilità delle prove, tema profondamente radicato negli ordinamenti degli Stati sovrani e verso cui gli Stati membri si sono sempre dimostrati altamente protettivi. Mentre l'AG Ćapeta ha sostenuto che la questione ricadrebbe nel diritto nazionale dismettendola del tutto[91], la Corte ha adottato una posizione più audace. In effetti, per la Corte di giustizia anche l'ammissibilità del materiale probatorio rientra nel diritto ad un giusto processo, sancito dall'art. 47 della Carta, il quale deve essere rispettato dagli Stati membri nella valutazione delle prove ottenute mediante un OEI (*ex* art. 14, par. 7 Direttiva OEI). Partendo da questa premessa, la Corte ha deciso di articolare il proprio ragionamento in tre fasi, secondo cui: i) un processo è equo se l'imputato può aver contezza e replicare efficacemente alle prove a suo carico, soprattutto quando è probabile che tali prove influenzino «in modo preponderante» la valutazione dei fatti[92]; ii) se invece l'imputato non è in grado di presentare efficacemente osservazioni su queste prove, allora si verificherà una violazione del diritto ad un giusto processo[93]; iii) come

[89] V. anche Corte giust., c-33/76, *Rewe-Zentralfinanz e Rewe-Zentral*, sent. 16-12-1976, p.to 5; Corte giust., *La Quadrature du Net*, cit., p.to 223.
[90] Corte giust., *Encrochat*, cit., p.to 90.
[91] Corte giust., concl. AG Ćapeta, cit., p.to 127.
[92] Corte giust., *Encrochat*, cit., p.ti 104-105 e 131. La necessità di tale *discovery* rappresenta il fulcro del diritto di difesa e del contraddittorio al fine di consentire all'interessato di interloquire sulle modalità di acquisizione delle prove digitali.
[93] Ibid., cfr. Corte giust., *Prokuratuur*, cit., p.to 44 nonché Corte EDU, Grande Camera, no. 54810/00, *Jalloh c. Germania*, 11-7-2006, p.to 96: «It must be examined in particular whether the applicant was given the opportunity of challenging the authenticity of the evidence and of opposing its use. In addition, the quality of the evidence must be taken into consideration, including whether the circumstances in which it was obtained cast doubts on its reliability or accuracy». Cfr. pronunce simili quali Corte EDU, no. 2742/12, *Matanović c. Croazia*, 4 aprile 2017, p.ti 151-158; Corte EDU, no. 39757/15,

DPCE online
ISSN: 2037-6677

conseguenza diretta di siffatta circostanza, è previsto che un elemento probatorio di tal genere «debba essere escluso dal procedimento penale» per rimediare a detta violazione del diritto a un equo processo[94]. In sostanza, la terza fase fa riferimento a specifiche conseguenze procedurali, stabilendo una sanzione di inutilizzabilità che interviene in modo chiaro, preciso e lineare.

La risposta della Corte non è certamente un divieto generalizzato all'uso delle prove recuperate grazie all'emissione di un OEI, ma una "condizione univoca" nei confronti dei tribunali nazionali per stabilire quando le prove trasmesse tra gli Stati membri in regime di OEI siano utilizzabili. Per tal motivo, la pronuncia *EncroChat* viene vista come un «potential landmark judgment» che dimostra la maturità della Corte in materia[95]. In effetti, non può negarsi che la decisione sia un importante tentativo di mantenere in equilibrio l'efficienza degli strumenti di cooperazione giudiziaria con il rispetto dei diritti fondamentali dell'indagato/imputato. Inoltre, la Corte colma una delle lacune strutturali dell'OEI, ovvero il preesistente silenzio circa le conseguenze sanzionatorie per una prova che, per via delle modalità d'acquisizione attuate dallo Stato di esecuzione, sia stata considerata indebita nello Stato d'emissione a causa della violazione dei diritti della difesa, espungendo per l'appunto dal procedimento informazioni ed elementi di prova idonei ad influire «in modo preponderante sulla valutazione dei fatti» se l'imputato non sia in grado di svolgere efficacemente le proprie osservazioni. A tal riguardo, la sentenza contribuisce allo sviluppo della mutua fiducia, nel senso che uno Stato membro non temerà più di importare gli effetti di una prova (patologica) trasmessa da altro Stato, superando anche il livello di dettaglio raggiunto dalla Corte EDU in ambito di utilizzabilità della prova straniera[96].

Sennonché, l'intera sentenza, e la risposta all'ultima questione in particolare, sembra porre l'accento sui soli diritti procedurali[97]. La vita privata appare solo "incidentalmente" e "parzialmente" tutelata. Infatti, la sanzione dell'inammissibilità probatoria è congeniata dalla Corte per tutelare esclusivamente i diritti di cui all'art. 47 e 48 Carta di Nizza e non già per gli artt. 7 e 8 di questa. Certamente, nulla esclude che – quale conseguenza della inammissibilità dichiarata per tutelare il diritto al giusto processo – la riservatezza delle comunicazioni potrebbe essere salvaguardata proprio in ambito processuale (incidentalità)[98]. Tuttavia, sempre nel rispetto

Einarsson e altri c. Islanda, 4-6-2019, p.ti 85-86; Corte EDU, no. 1586/15, *Rook c. Germania*, 25-7-2019, p.ti 56-59.

[94] Corte giust., *Encrochat*, cit., p.ti 130-131.

[95] L. Bernardini, *op. cit.*

[96] Corte EDU, ricorso n. 69762/12, *Budak c. Turchia*, 16-2-2021, p.ti 71 e 86-88; Corte EDU, Grande Camera, no. 15669/20, *Yüksel Yalçinkaya c. Turchia*, 26-9-2023.

[97] Sui quali, con riguardo al diritto primario dell'Unione, si v. A. Di Stasi, A. Lang, A. Iermano, A. Oriolo, R. Palladino, *Spazio europeo di giustizia e applicazione giurisprudenziale del Titolo VI della Carta dei diritti fondamentali dell'Unione europea*, Napoli, 2024. Per quanto concerne il diritto derivato, si v. in part. T. Russo, *Alcuni spunti riflessivi sull'evoluzione della competenza penale dell'Unione europea e sulle criticità "procedurali" della cooperazione giudiziaria in materia*, in *Riv. coop. giur. internaz.*, 2024, 76, 88 ss.

[98] Si noti che non varrebbe il contrario dato che la Corte EDU ha ripetutamente affermato che le prove ottenute attraverso una violazione del diritto alla vita privata non costituiscono necessariamente una violazione del diritto a un processo equo.

delle esigenze di persecuzione penale e di efficienza della giustizia, la sensazione è che nella sentenza non è stato dato alcuno spazio a soluzioni che anticipino e neghino l'ingerenza da parte dell'autorità di esecuzione, piuttosto che limitarsi a considerarne *ex post* la non impiegabilità a livello processuale (parzialità). Maggiore decisione nella delimitazione dei parametri di cui all'art. 6, par. 1 Direttiva OEI avrebbe invece consentito di addivenire anche a questo risultato.

E, vieppiù, tali aspetti problematici del potenziamento del solo controllo successivo sono avvalorati dal fatto che nel giudizio riservato all'autorità di esecuzione sia «unclear what are the requirements for an intrusiveness assessment»[99]. Più nel dettaglio, sembra assai inopportuno che la valutazione *ex post* venga limitata esclusivamente ad un dato momento temporale specifico, visto che plurime e diverse ingerenze per la *privacy* possono presentarsi in più passaggi nella formazione della prova digitale. Eppure, non tenendo conto della pluralità di questi "momenti" peculiari della captazione e conservazione del dato crittografato, la Direttiva non impone in tal senso nessun tipo di valutazione sugli "effetti" sortiti dalle misure intrusive. Inoltre, specialmente in relazione alle comunicazioni cifrate, la portata dell'art. 14 Direttiva OEI potrebbe rivelarsi ancor più limitata di quanto non si pensi data una sua applicazione solo "eventuale". Infatti, la disposizione stabilisce in maniera piuttosto chiara che l'autorità di emissione e di esecuzione provvederanno ad adottare «le misure adeguate […] ove applicabili» per far sì che l'interessato venga a conoscenza dell'OEI e della possibilità di impugnazione dello stesso solo «laddove non comprometta la riservatezza di un'indagine» (art. 14, par. 3)[100]. Ne consegue che un indagato o imputato potrebbe alternativamente o non essere affatto informato della possibilità di ricorso o non riuscire ad evitare l'esecuzione della misura intrusiva in tempo utile ad impedire un'interferenza nella propria riservatezza. In entrambi i casi prospettati tale forma di controllo *ex post* non impedisce che la lesione del diritto sia prodotta ed, anzi, le disposizioni appaiono invero di difficile applicazione quando le indagini afferiscano ad intercettazione di comunicazioni cifrate, ove la compromissione della «riservatezza di un'indagine» ancora in corso sarebbe scontata nel momento dell'avvenuta notifica all'interessato.

Pertanto, alla luce di quanto finora esposto, la sentenza *EncroChat*, tutto sommato, è una vittoria per i diritti processuali e di difesa, ma non riesce a "spostare" più di tanto gli equilibri già definiti dalle corti nazionali in tema di bilanciamento tra sicurezza e *privacy*.

Pertanto, le violazioni della riservatezza non dovrebbero portare all'esclusione di elementi probatori, con un impatto minimo o nullo sui possibili procedimenti penali in corso e futuri. Corte EDU, no. 22767/08, *Dragos c. Romania*, sent. 31-10-2017, p.to 50; Corte EDU, no. 40233/07, *Klaneniene c. Belgio*, 31-1-2017, p.to 50; Corte EDU, no. 35394/97, *Khan c. Regno Unito*, 12-5-2000, p.to 40.

[99] R. Stoykova, *op. cit.*, 10.

[100] E, ancora, è assai rilevante che l'impugnazione «non sospende l'esecuzione dell'atto di indagine, a meno che ciò non abbia tale effetto in casi interni analoghi» (art. 14, par. 7).

DPCE online
ISSN: 2037-6677

7. Conclusioni

In conclusione, l'analisi condotta ha evidenziato che l'Unione ha dimostrato di avere adottato un atteggiamento di iniziale neutralità ed ambivalenza verso la cifratura, evolutosi tramite la legislazione più recente in una evidente prevalenza della prospettiva securitaria volta a limitare il dato criptato. Attestando una certa indifferenza verso la tipologia di dato da intercettare, si registra una tendenza normativa favorevole al cd. *lawful access* delle autorità nei confronti di questo tipo di comunicazioni, che in verità potrebbe celare un rischio di sorveglianza di massa. Tale approccio sembra essere stato accompagnato da uno sviluppo pratico analogo nella cooperazione giudiziaria in ambito penale.

Non a caso, le prove acquisite nell'ambito delle operazioni volte a captare dati criptati sollevano molte questioni circa potenziali imprecisioni procedurali e anticipano il panorama delle sfide future al diritto del giusto processo e della *privacy*. Da un lato, la presenza di difetti genetici nella Direttiva OEI, con riguardo all'art. 6, par. 1 in particolar modo, rende l'applicazione di quest'ultimo più incerto. Dall'altro, si osserva nella Direttiva la mancanza di sufficienti garanzie per la riservatezza, nonché di vere e proprie norme in materia che differenzino le diverse fasi della formazione della prova digitale. In altre parole, la Direttiva non risolve una possibile tensione in partenza tra l'art. 72 TFUE, sulla responsabilità incombente agli Stati membri per il mantenimento dell'ordine pubblico e la salvaguardia della sicurezza interna, e l'artt. 16 TFUE, nonché 7 e 8 Carta di Nizza, sulla tutela della riservatezza delle comunicazioni.

Come verificato nella vicenda riguardante la piattaforma *EncroChat*, in effetti, tali problematiche sembrano essersi acuite guardando al fatto che l'impiego di nuove tecnologie stimola diffidenza e, addirittura, una presunzione di colpevolezza verso l'indagato da parte dell'organo giudicante. Tant'è che «il dogma secondo cui il crimine è un passo avanti sembra non aver funzionato del tutto» nel caso delle comunicazioni criptate[101]. Su tale aspetto la Corte EDU in *Podchasov* ha fornito delle linee guida sul bilanciamento in questione, chiarendo che la criptazione delle chat non è illegale di per sé e che, anzi, essa è un pieno diritto degli individui, capace di venire in supporto di altri diritti quali la libertà d'espressione. Di converso, nella vicenda *EncroChat* è stata fatta poca chiarezza sulle modalità di acquisizione della prova, rendendo opachi elementi fondamentali per il giudice al momento del giudizio di necessità e proporzionalità in sede di ricorso *ex post*, come pure sarebbe richiesto nella Direttiva OEI. E, infatti, in tali circostanze, le corti nazionali hanno sempre proteso verso uno sbilanciamento favorevole alla sicurezza piuttosto che verso la tutela della *privacy*, praticamente "fidandosi" dell'azione di repressione criminale intentata dalle autorità competenti.

Avvalorando tale sensazione, in questo contesto si è inserita la sentenza da parte della Corte di giustizia. Quest'ultima non si è ripetuta, come invece fatto nella *caselaw* sulla sorveglianza di massa, nel fornire una definizione di "giusta ingerenza" per quanto attiene le comunicazioni

[101] A. Halimi, *Encrochat, le verità della decisione della Corte di giustizia nei dilemmi di un processo che segue. 5 domande e 5 risposte*, in *BotaSot*, 26-12-2024.

criptate. È possibile, dunque, che la Corte ritenga di intervenire in tal senso nei casi in cui si presenti per lo più un'ingerenza "quantitativa" (sorveglianza di massa) piuttosto che un'ingerenza "qualitativa" (comunicazioni criptate), ovvero quando una violazione della riservatezza coinvolga un ragguardevole numero di soggetti rispetto a quando colpisca un numero inferiore di questi, ma più "in profondità".

Della sentenza della Corte di giustizia si evidenzia in senso positivo la progressione del grado di tutela offerto rispetto ai diritti processuali in seno all'OEI, disponendo una conseguenza sanzionatoria – l'inutilizzabilità – quando non è stato possibile fare un corretto esercizio dei diritti di difesa dell'indagato/imputato, come tra l'altro confermato dalla giurisprudenza nazionale occorsa dopo la pronuncia dei giudici di Lussemburgo[102]. Se non altro, l'enfasi rivolta al diritto al giusto processo sembra far slittare la *privacy* in un ruolo secondario, ove questa sia solo incidentalmente tutelata. Ulteriormente, si consideri che l'introduzione della sanzione-inammissibilità è un'innovazione strettamente processuale, che non risolve il problema nel *vulnus* del diritto (sostanziale) alla *privacy*. Quest'ultimo è precedente alla dichiarazione di inutilizzabilità e si consuma nel momento in cui l'autorità competente per l'emissione dell'OEI effettuerà un giudizio di proporzionalità e necessità aggravato di un ampio margine di apprezzamento[103]. Ne consegue che la "retrocessione" della riservatezza a diritto secondario rispetto ai diritti processuali è suffragata dal "rifiuto" della Corte di giustizia di pronunciarsi sulla proporzionalità delle misure disposte in forza della Direttiva OEI in caso di dati crittografati. Rinviando la Corte ad una valutazione sulla proporzionalità operata a livello nazionale, allora il bilanciamento in ipotesi di comunicazioni criptate rimarrà nelle mani delle corti nazionali che, come si è detto, hanno fatto propria una posizione preminentemente securitaria.

Da ultimo, rispondendo alla domanda alla base dell'indagine condotta, si può affermare che esiste una nuova sfida alla tutela riservatezza, la quale appare sia "a rischio" che "limitata" 1) da problematiche applicative genetiche legate al mutuo riconoscimento ed al rispetto sovranità statale altrui; 2) dalla propensione verso la sicurezza in assenza di adeguate competenze conoscitive da parte dei giudici, specie nel caso di comunicazioni criptate, e; 3) dalla preminenza di altri diritti, maggiormente protetti, fermo restando che la *privacy* potrebbe comunque essere tutelata in via derivata. In ottica di sviluppi futuri – al netto del secondo rinvio pregiudiziale su *EncroChat*

[102] Cass., Sez. VI, n. 45843, sent. 5-12-2024. Tuttavia, si intende sottolineare la non limpidissima vittoria dei diritti processuali di difesa nella decisione (p.to 3) siccome, analogamente a Corte EDU, Grande Camera, no. 15669/20, *Yüksel Yalçinkaya c. Turchia*, 26-9-2023, p.to 336: «neppure determina, almeno in linea di principio, una violazione di «diritti fondamentali» l'impossibilità, per la difesa, di accedere all'algoritmo utilizzato nell'ambito di un sistema di comunicazioni per "criptare" il contenuto delle stesse». Così, da ultimo, anche Cass., Sez. III, n. 44047, 3-12-2024. Pertanto, si verrebbe a creare una doppia preclusione – tra il segreto di Stato francese e l'occultamento dell'algoritmo di decrittazione – opposta al difensore nel poter compiutamente accedere agli atti originari a presupposto dell'OEI.

[103] Margine di apprezzamento da parte dei giudici nazionali che, in generale, è visto da B. Cortese, *op. cit.*, come non compatibile con il nuovo contesto venutosi a formare dopo l'introduzione dell'art. 16 TFUE in materia di circolazione dei dati.

DPCE online
ISSN: 2037-6677

cancellato dal registro della Corte di giustizia e della dichiarata inammissibilità dei due ricorsi presentati contro la Francia dinanzi la Corte EDU – difficilmente si ritiene che le corti europee opteranno per una modifica dei propri orientamenti nel brevissimo termine[104]. Tuttavia, è stato notato da uno dei suoi stessi giudici che «the Strasbourg Court lags behind the Luxembourg Court, which remains the lighthouse for privacy rights in Europe»[105]. Dunque, più che altro, ci si può attendere che un'eventuale inversione di rotta, con un approccio maggiormente protettivo della *privacy*, sarà avviata più facilmente nella giurisprudenza dell'Unione Europea che in quella legata al Consiglio d'Europa.

Stefano Busillo
Dip.to di Scienze Giuridiche
Università degli Studi di Salerno
sbusillo@unisa.it

[104] Si pensi ad altre operazioni appena concluse come risulta dal Comunicato stampa di Europol, *International operation takes down another encrypted messaging service used by criminals*, 3-12-2024., da cui emerge che una SIC tra autorità francesi e olandesi (di nuovo), con l'ausilio di una *task force* inclusiva di autorità italiane, lituane, spagnole e tedesche, ha eseguito un'operazione contro la piattaforma MATRIX, ritenuta anche più complessa rispetto alle note *EncroChat* e SkyECC. Interessante è la velata sponsorizzazione dell'OEI attraverso la frase «[t]hrough legal requests, authorities will now be able to access the messages for their investigations».
[105] Corte EDU, no. 70078/12, *Ekimdzhiev e altri c. Bulgaria*, *diss. op.* del giudice Pinto De Albuquerque 11-1-2022, p.to 60.