Digitalizzazione e giusto processo: la *digital evidence* nella giurisprudenza della Corte Europea dei Diritti dell'Uomo

di Raffaele Prettato

Title: Digitalization and fair trial: digital evidence within the jurisprudence of the European Court of Human Rights

Keywords: European Convention on Human Rights; Right to a fair process; Digital evidence; Turkey

1. – Negli ultimi anni, si è assistito a un profondo mutamento del procedimento penale, sia nella fase delle indagini che in quella del giudizio, dovuto all'utilizzo sempre più significativo in termini quantitativi e qualitativi della c.d. "*digital evidence*" (in italiano, prova digitale). Con tale espressione si indica «any information processed by electronic medium which supports or refutes a hypothesis about the state of digital artefacts or digital events, of potential relevance and probative value for a criminal investigation» (v. R. Stoykova, *Digital evidence: Unaddressed threats to fairness and the presumption of innocence*, in 42 *Computer Law & Security Review* 2 (2021)). La *digital evidence* può quindi essere definita come qualsiasi informazione avente natura digitale, la quale assume una valenza probatoria a fini processuali. Ciò detto, se si considera che oggigiorno la tecnologia riveste un ruolo fondamentale nella vita quotidiana di ogni individuo, è facile comprendere come la *digital evidence* abbia acquisito un ruolo di prim'ordine per l'apertura, lo svolgimento e la conclusione dei procedimenti penali (v. S. Signorato, *Le indagini digitali: profili strutturali di una metamorfosi investigativa*, Torino, 2018). Ogni giorno, infatti, vengono utilizzati un numero considerevole di strumenti digitali tanto per ragioni professionali quanto per questioni personali e ciò comporta la produzione e la conservazione di una quantità enorme di dati che tengono traccia delle attività digitali svolte. Ne consegue che tutto questo materiale assume una notevole importanza per le attività di accertamento e contrasto dei reati, non solo per i c.d. reati informatici (ossia gli illeciti penali che per definizione vengono commessi mediante l'utilizzo di strumenti digitali e informatici), ma anche per reati che possono definirsi "comuni" (si pensi ad es. al caso dei dati di geolocalizzazione, i quali possono essere usati per dimostrare la presenza di un soggetto sulla scena di un omicidio nella finestra temporale all'interno della quale il reato è stato commesso).

Dinnanzi a un tale scenario diviene quindi fondamentale interrogarsi sull'incidenza che questa nuova tipologia di prova ha all'interno della procedura penale: ciò che viene da domandarsi è come le garanzie processuali sancite dal principio del giusto processo debbano essere declinate nel momento in cui la prova

digitale viene impiegata all'interno del procedimento penale. Tale domanda assume una particolare rilevanza soprattutto qualora si prendano in considerazione le caratteristiche della *digital evidence*. Questa, infatti, presenta tre aspetti fondamentali (v. G. Soana, *Catena di Custodia, Prova Digitale e Tecnologia Block-Chain*, in *Diritto di Internet*, 4, 2021, 789-800): i) volatilità, ossia la possibilità che gli ambienti digitali in cui sono contenuti i dati si modifichino rapidamente con conseguente perdita o mutamento dei dati stessi; ii) modificabilità, ossia la suscettibilità dei dati ad alterazioni che da un lato sono solitamente irreversibili e dall'altro sono impercettibili *prima facie*; iii) transnazionalità, ossia il fatto che l'immaterialità e la conseguente facilità di trasferimento dei dati, congiuntamente al sempre più frequente ricorso al *cloud computing*, implicano che i dati siano spesso collocati in *server* posti al di fuori della giurisdizione delle autorità giudiziarie competenti (v. V. Tondi, *L'accesso transfrontaliero all'electronic evidence, tra esigenze di effettività e tutela dei diritti*, in *Diritto Penale Contemporaneo*, 2, 2019, 439-455). Questi caratteri implicano la necessità di prestare una particolare attenzione al rispetto delle garanzie del giusto processo nel momento in cui la prova digitale è utilizzata: si pensi ad esempio al fatto che la volatilità e la modificabilità possono determinare una variazione irreparabile dei dati e conseguentemente delle risultanze probatorie, con l'esito possibile di arrivare a condanne errate (v. S. Signorato, *Le indagini digitali: profili strutturali di una metamorfosi investigativa*, Torino, 2018). Quindi, nonostante tale tipologia di prova possa a prima vista essere considerata infallibile, va al contrario puntualizzato che essa è ben lontana dall'essere una prova perfetta. Come è stato, infatti, notato (v. M. Pittiruti, *Digital evidence e procedimento penale*, Torino, 2017, 14-18), la *digital evidence* può essere considerata come una sottocategoria della prova tecnico-scientifica e in quanto tale vale anche in questo caso l'argomento per cui essa non è una prova perfetta, bensì un elemento che al più permette di approdare a conclusioni ad alta probabilità. Tale argomentazione è d'altronde confermata anche dal fatto che la *digital evidence* è per sua stessa natura suscettibile a errori derivanti dalla stessa tecnologia che produce la prova, come ad esempio errori riguardanti i c.d. *timestamps* o la perdita di dati (v. E. Casey, *Error, Uncertainty, and Loss in Digital Evidence*, in 1(2) *International Journal of Digital Evidence* 1-45 (2002)), oppure a errori dovuti alla mancanza di dati o di rigore scientifico nella gestione delle prove (v. SWGDE, *Establishing Confidence in Digital and Multimedia Evidence Forensic Results by Error Mitigation Analysis*, Version: 2.0, 20 novembre 2018), oppure ancora a errori umani e cognitivi (v. N. Sunde; I. E. Dror, *Cognitive and human factors in digital forensics: Problems, challenges, and the way forward*, in 29 *Digital Investigation* 101-108 (2019)). Tutto ciò comporta due conseguenze: da un lato è necessario che vi sia una gestione attenta e rigorosa della *digital evidence*, finalizzata ad assicurarne l'attendibilità e la veridicità, mentre dall'altro lato è essenziale che all'interno di ogni singolo procedimento venga opportunamente trattato il tema dell'affidabilità, e quindi del valore probatorio, di questa tipologia di prova. Non è un caso, infatti, che in anni recenti si sia affermata una nuova disciplina scientifica denominata *digital forensics*. Quest'ultima è una nuova branca delle scienze forensi che, mettendo insieme competenze tecnologico-informatiche e giuridiche, ha come obiettivo ultimo quello di trasformare i dati digitali in prove fruibili all'interno del procedimento penale, mediante un processo frazionabile in quattro sottofasi (v. G. Horsman, *Digital evidence strategies for digital forensic science examinations*, in 63(1) *Science and Justice* 116-126 (2023)): i) *data acquisition*; ii) *examination/processing*; iii) *analysis and intepretation*; iv) *communication of findings*. Il problema di garantire che il principio del giusto processo continui ad essere rispettato pur in presenza della *digital evidence* rappresenta quindi una questione di primaria importanza, la quale è sentita a livello nazionale (v. con riferimento all'ordinamento italiano C. Parodi, *L'acquisizione della prova digitale*, in *Il diritto vivente*, 3, 2019, 35-76), a livello europeo (v. R. Stoykova, *The right to a fair*

DPCE online
ISSN: 2037-6677

trial as a conceptual framework for digital evidence rules in criminal investigations, in 49 *Computer Law and Security Review* 1-26 (2023)) e a livello internazionale (v. M. de Arcos Tejerizo, *Digital evidence and fair trial rights at the International Criminal Court*, in 36(3) *Leiden Journal of International Law* 749-769 (2023)).

2. – Di fronte all'importanza della prova digitale all'interno del procedimento penale e alle problematiche che essa pone in relazione al rispetto delle garanzie del giusto processo, era logico aspettarsi che tale questione approdasse dinnanzi alla Corte Europea dei Diritti dell'Uomo. Ciò è infatti quello che è avvenuto, da ultimo con la recente vicenda *Yüksel Yalçinkaya c. Turchia*, decisa dalla Grande Camera con sentenza emessa in data 26 settembre 2023 (Corte Europea dei Diritti dell'Uomo, Grande Camera, *Yüksel Yalçinkaya c. Turchia*, ricorso n. 15669/20, del 26 settembre 2023). Il contesto fattuale all'interno del quale si sviluppa il caso è quello del noto tentativo di colpo di Stato realizzato in Turchia nell'estate del 2016. Nella notte tra il 15 e il 16 luglio 2016, un gruppo di membri delle forze armate turche (il c.d. *Yurtta Sulh Konseyi* o *Peace at Home Council*) tentò di rovesciare il Governo guidato dal Presidente Erdoğan. Il golpe non ebbe però successo e fin dal giorno successivo le autorità nazionali iniziarono ad attribuire la responsabilità dell'accaduto al movimento guidato da Fetullah Gülen, ossia un movimento islamista attivo in vari settori della società, conosciuto dai suoi stessi membri col nome di "*Hizmet*" ("*Servizio*") o di "*Cemaat*" ("*Comunità*") o col nome di FETÖ/PDY dalle autorità turche. Il fatto che la responsabilità del tentato colpo di Stato fosse attribuita fin da subito a questo movimento non fu affatto sorprendente: dopo anni di sospetti in merito alla natura e agli obiettivi reali del FETÖ/PDY e dopo che una serie di procedimenti penali a carico di Gülen furono aperti nel 1999 per sospetta attività terroristica e si conclusero con la sua assoluzione nel 2008 (v. punti 189-193 della sentenza in commento per una ricostruzione della vicenda), il dibattito pubblico e le controversie relative al FETÖ/PDY ripresero a partire dal 2013. Ciò è testimoniato anche dal fatto che il Consiglio di Sicurezza Nazionale turco (*Milli Güvenlik Kurulu* o MGK), un corpo con funzioni consultive e di coordinamento in materia di sicurezza nazionale, iniziò a qualificare il FETÖ/PDY come una "*structure threatening public peace and security*" nel febbraio del 2014, per poi passare a considerarlo come un'organizzazione terroristica dal maggio del 2016 (v. punti 108-113 della sentenza in commento).

In parallelo all'attività della magistratura e del MGK, a partire dai primi mesi del 2016, l'Agenzia di Intelligence nazionale (*Milli İstihbarat Teşkilatı* o MİT) avviò operazioni nei confronti del FETÖ/PDY, tra le quali vi fu l'accesso ai *server* principali dell'applicazione ByLock, ritenuta un'applicazione sviluppata e utilizzata esclusivamente per le esigenze comunicative e organizzative dei membri del movimento di Gülen. A seguito dell'acquisizione di tali dati (in particolare gli indirizzi IP delle persone che si erano connesse al server), migliaia di indagini vennero iniziate nei confronti degli utenti di ByLock, accusati di essere membri dell'organizzazione terroristica FETÖ/PDY e quindi penalmente responsabili a norma dell'art. 314 del Codice penale turco (CPT).

Nel settembre 2016 fu aperta un'indagine nei confronti di 147 insegnanti per sospetta appartenenza al FETÖ/PDY, in quanto erano stati identificati come utenti dell'applicazione ByLock sulla base dei dati raccolti dal MİT. Tra gli indagati, era incluso anche Yüksel Yalçinkaya, ricorrente del caso in commento. Le indagini portarono prima alla sua incriminazione e successivamente alla condanna, confermata in tutti i gradi di giudizio interni. Yüksel Yalçinkaya decise quindi di proporre ricorso dinnanzi alla Corte EDU, lamentando la violazione dell'art. 7 (principio del *nullum crimen sine lege*) e dell'art. 6, par. 1 (principio del giusto processo).

I due motivi di ricorso collocano il caso all'intersezione di due questioni fondamentali. Con la doglianza relativa all'art.6, si sottopone alla Corte una problematica di carattere generale, ossia la tutela del principio del giusto processo nel momento in cui la *digital evidence* viene utilizzata in sede di giudizio penale. Il motivo di ricorso attinente all'art. 7, invece, pone una questione maggiormente legata al contesto nazionale dal quale il caso in commento ha avuto origine: la Corte EDU si ritrova infatti ad affrontare un problema sistemico dell'ordinamento giuridico turco, quale l'utilizzo di una prova digitale (ossia il *data set* che dimostra l'uso dell'applicazione di messagistica criptata ByLock) per individuare e sanzionare i membri del FETÖ/PDY. Tale tematica si inserisce a sua volta all'interno del fenomeno di erosione dello Stato di diritto e della democrazia che interessa la Turchia da ormai un decennio circa (v. T. Groppi, *L'attacco allo Stato di diritto in Turchia: l'onda lunga del 1989 è definitivamente finita?*, in *DPCE Online*, 1, 2017, 1-7; V.R. Scotti, *Il Presidenzialismo turco: un passo in avanti nel consolidamento dell'autoritarismo competitivo o una ulteriore garanzia per la stabilità delle istituzioni?*, in *DPCE Online*, 1, 2023, 1173-1193; A. Vannucci, *Governo, giudici e militari: come cambia l'equilibrio tra poteri in Turchia alla luce del referendum del 12 settembre 2010*, in *Federalismi.it*, 2, 2011, 1-55).

Le due questioni poste alla Corte riguardano quindi: i) la gestione in sede processuale della *digital evidence* nel rispetto delle garanzie imposte dal principio del giusto processo (questione di carattere generale); ii) il valore probatorio della prova digitale utilizzata dal giudice nazionale per fondare la condanna del ricorrente (questione di carattere specifico). Il presente contributo affronterà entrambi i punti, concentrandosi maggiormente sul primo poiché, dato il suo carattere di generalità, esso appare più rivelante per le problematiche connesse all'utilizzo della *digital evidence*. La questione specifica verrà quindi affrontata per prima in modo da lasciar maggior spazio a quella generale.

3. – Come anticipato, la questione del valore probatorio è rappresentativa di un problema sistemico e diffuso all'interno dell'ordinamento turco: basti pensare che ad oggi vi sono più di 8.000 casi simili a quello in commento pendenti dinnanzi alla Corte EDU e probabilmente più di 100.000 istanze riguardanti lo stesso tema all'interno del sistema giudiziario turco (per questi dati v. A. Yildiz, *Strasburg Weighs In On Political Persecution In Turkey*, in *Verfassungsblog*, 31 ottobre 2023). Il *punctum dolens* si può individuare nel fatto che, come riconosciuto a chiare lettere dalle autorità giudiziarie turche, l'applicazione ByLock sarebbe stata sviluppata e creata solo e soltanto per soddisfare le esigenze comunicative e organizzative di FETÖ/PDY. Sulla base di questa considerazione, i dati che dimostrano il semplice fatto che l'applicazione ByLock è stata scaricata e utilizzata da un determinato soggetto sarebbero una prova sufficiente a dimostrare l'appartenenza all'organizzazione terroristica e conseguentemente a fondare una responsabilità penale a norma dell'art. 314 del CPT. Tale ragionamento è reso ben evidente dalle parole dei giudici turchi «Since the Bylock messaging app is a communication network, exclusively designed and developed to fulfil the communication needs of the FETÖ terrorist organization, the detection, through technical means, of the involvement of any individual within this network beyond any doubt proves the link of the individual to the terrorist organization» (Corte di Cassazione, sentenza E. 2017/16-956, K. 2017/370 del 26 settembre 2017, come citata in A. Yildiz, *Strasburg Weighs In On Political Persecution In Turkey*, in *Verfassungsblog*, 31 ottobre 2023).

Sul punto, il ricorrente contesta che la condotta criminosa che gli è stata imputata e della quale è stato ritenuto responsabile, ossia l'appartenenza a un'organizzazione terroristica, richiederebbe l'accertamento della sussistenza di

DPCE online
ISSN: 2037-6677

alcuni requisiti, di natura tanto materiale quanto mentale, quali: i) l'esistenza al di là di ogni ragionevole dubbio dell'organizzazione terroristica; ii) la conoscenza da parte dell'imputato della natura terroristica dell'organizzazione; iii) l'effettiva appartenenza dell'imputato all'organizzazione; iv) la specifica intenzione dell'imputato di perseguire gli obiettivi dell'organizzazione; v) la struttura gerarchica dell'organizzazione e il collocamento dell'imputato all'interno di tale schema organizzativo. Secondo il ricorrente, i giudici nazionali non avrebbero accertato la presenza di nessuno dei summenzionati elementi, col risultato che la sua condanna a norma dell'art. 314, CPT non sarebbe stata prevedibile e in quanto tale sarebbe avvenuta in violazione dell'art. 7, CEDU. A ciò si aggiungerebbe poi che al tempo dei fatti a lui attribuiti, avvenuti tra il 2014 e il 2015, il movimento di Gülen non poteva essere considerato, al di là di ogni ragionevole dubbio, come un'organizzazione di stampo terroristico.

La Corte EDU analizza la questione premurandosi innanzitutto di sottolineare che l'art. 7, «which is an essential element of the rule of law» (punto 237), non si limita solamente a proibire l'applicazione retroattiva della legge penale *in malam partem*, bensì esso implica anche da un lato il principio per cui solamente la legge può individuare le condotte criminose e imporre una sanzione in caso di loro commissione e dall'altro il principio per cui è fatto divieto di interpretazione estensiva ed analogica della legge penale *in malam partem*. Affinché tali requisiti possano essere soddisfatti è imprescindibile che la legge penale, letta anche alla luce della giurisprudenza nazionale, sia chiara e precisa nel definire e individuare le condotte commissive o omissive che integrano fattispecie di reato. La prevedibilità è quindi un corollario del principio di legalità ex art. 7, CEDU. A detta dei giudici di Strasburgo, quest'ultimo principio dev'essere applicato non solamente nei confronti della legge, ma anche dalla giurisprudenza stessa: i giudici nazionali devono applicare la legge in maniera compatibile, e quindi prevedibile, rispetto alla *ratio* della previsione normativa. Infine, i giudici di Strasburgo sottolineano che, per potersi avere una condanna penale, è imprescindibile che esista un *"mental link"* tra la condotta integrante reato e il soggetto imputato del reato stesso. Ciò detto, però, si specifica che alcune forme di responsabilità oggettiva basate su presunzioni di responsabilità sono compatibili con la Convenzione e in quanto tali ammissibili, a condizione che tali presunzioni non abbiano l'effetto ultimo di rendere impossibile per l'imputato la contestazione dell'accusa a lui rivolta. È proprio su quest'ultimo punto che si innesta l'aspetto cruciale del caso in commento.

In merito, la Corte EDU arriva alla conclusione che, avendo riguardo alle normative già in vigore al momento del compimento dei fatti oggetto di causa (in particolare l'art. 314, CPT e la legge n. 4928 del 15 luglio 2003 sulla prevenzione del terrorismo) il reato per il quale il ricorrente è stato condannato era già codificato. A ciò si aggiunga che prima della condanna del ricorrente i giudici turchi avevano già avuto modo di specificare l'interpretazione della legge (in particolare il riferimento è alla giurisprudenza della Corte di Cassazione, come ad esempio le sentenze E. 2015/3, K. 2017/3 e E. 2017/16-956, K. 2017/370, rispettivamente del 24 aprile e del 26 settembre 2017). Il principio di legalità propriamente detto è quindi rispettato. Inoltre, non appare neanche rilevante che, al momento del compimento dei fatti di causa, il movimento di Gülen non fosse ancora stato qualificato dalle autorità giudiziarie come organizzazione terroristica: anche se la legge turca richiede che la natura terroristica di un'organizzazione sia accertata mediante decisione giurisdizionale, la mancanza di una tale designazione non preclude la responsabilità penale dei suoi fondatori e dei suoi membri per gli atti commessi, purché tali atti siano consapevoli e volontari.

Per la Corte quindi il punto centrale della questione non è tanto se il FETÖ/PDY fosse qualificato come organizzazione terroristica al momento dei fatti, bensì se la condanna dei suoi membri fosse sufficientemente prevedibile alla

luce della normativa. Tale valutazione deve essere condotta, inoltre, tenendo in considerazione il fatto che l'art. 7, CEDU non richiede solamente che una condotta sia chiaramente qualificata come reato dalla legge, ma anche che i giudici nazionali rispettino la legge, interpretandola e applicandola in maniera ragionevole e quindi prevedibile. Al contrario, un'interpretazione e un'applicazione irragionevoli della normativa rilevante implicherebbero una mancanza di prevedibilità della condanna penale e conseguentemente una violazione dell'art. 7. A questo punto, i giudici di Strasburgo rilevano che la condanna del ricorrente è stata fondata solo e unicamente sulla base dell'utilizzo dell'applicazione ByLock. Secondo i giudici di Strasburgo, infatti: «It was, however, also made clear that the mere fact of having used the ByLock application would serve, on its own, as conclusive proof of the presence of all of the constituent elements of the crime of membership of an armed terrorist organisation as defined in domestic law, irrespective of the content of the messages exchanged or the identity of the persons with whom the exchanges were made» (punto 258). La condanna del ricorrente sarebbe quindi avvenuta senza considerare l'uso effettivo che è stato fatto dall'applicazione (ad es. senza verificare il contenuto dei messaggi inviati e ricevuti). Il mero utilizzo di ByLock sarebbe stato ritenuto sufficiente dai giudici turchi per accertare l'esistenza di tutti gli elementi costitutivi della fattispecie di reato e quindi arrivare alla condanna: la Corte infatti nota che «over and above its evidential value, the finding regarding the use of ByLock here effectively replaced an individualised finding as to the presence of the constituent material and mental elements of the offence, thereby bypassing the requirements of Article 314 § 2 of the Criminal Code – as interpreted by the Court of Cassation itself – in contravention of the principle of legality and bringing the matter within the realm of Article 7» (punto 262). La conseguenza di una tale interpretazione e applicazione della normativa nazionale sarebbe quella di creare «an almost automatic presumption of guilt based on ByLock use alone, making it nearly impossible for the applicant to exonerate himself from the accusations» (punto 268). Anche perché, come i giudici europei hanno avuto modo di sottolineare nella parte della sentenza dedicata all'art.6, l'argomento dell'esclusività utilizzato dai giudici turchi (ossia la massima secondo la quale l'applicazione sarebbe stata utilizzata solamente dai membri di FETÖ/PDY) presenta notevoli lacune, ossia il fatto che i giudici nazionali: i) sarebbero arrivati all'argomento dell'esclusività sulla base delle caratteristiche tecniche dell'applicazione stessa (ad es. il criptaggio dei messaggi e degli utenti, le particolari procedure per entrare in contatto con gli altri utenti, la necessità di utilizzo della VPN, l'automatica cancellazione dei contenuti dei messaggi), senza considerare che a partire dai primi mesi del 2016 l'applicazione poteva essere scaricata da siti o store aperti al pubblico, senza che vi fosse alcun meccanismo di controllo (ad es. ci sono stati un milione di *download* da siti APK, a cui se ne aggiungo altri 500.000 dal Google Play *store*); ii) non hanno considerato che le caratteristiche dell'applicazione sopra richiamate sono spesso presenti anche in altre applicazioni accessibili al grande pubblico; iii) non hanno considerato se il ricorrente si è unito al *network* ByLock dietro indicazione e istruzione dell'organizzazione terroristica come richiesto dalla Cassazione nei precedenti che avevano stabilito che l'utilizzo dell'applicazione ByLock costitutiva una prova di connessione con FETÖ/PDY; iv) hanno accettato le conclusioni a cui il MİT è arrivato in un contesto extragiudiziario riguardo all'argomento di esclusività, senza renderle oggetto di un vaglio all'interno del processo. Un tale ragionamento rappresenta quindi una chiara violazione del principio di legalità e del principio di prevedibilità ex art. 7, CEDU. La decisione dei giudici nazionali va quindi censurata per contrarietà alla disposizione convenzionale.

DPCE online
ISSN: 2037-6677

4. – Per quanto attiene invece alla questione generale della gestione della *digital evidence* all'interno del procedimento penale e della presunta violazione dell'art. 6, CEDU, due sono le doglianze del ricorrente. Innanzitutto, i dati relativi all'utilizzo di ByLock sarebbero stati acquisiti illegalmente dai servizi di intelligence turca e quindi non potrebbero essere impiegati come prova, dato che l'utilizzo di prove raccolte illegalmente sarebbe proibito dalla stessa legislazione turca. In particolare, l'illegittimità deriverebbe dal fatto che la raccolta e la successiva analisi ed elaborazione dei dati sarebbero avvenute in totale segretezza e senza una preventiva autorizzazione giudiziaria. Tale mancanza avrebbe avuto la conseguenza di rendere impossibile l'accertamento dell'integrità e dell'autenticità dei dati. La situazione sarebbe poi stata ulteriormente aggravata dal fatto che il MİT non ha fornito alcuna indicazione in merito alle misure adottate per assicurarne l'integrità. A fronte di tali circostanze sarebbe quindi impossibile considerare i dati come prova affidabile e decisiva. In secondo luogo, il ricorrente lamenta una violazione del suo diritto a un giusto processo derivante dall'impossibilità di contestare compiutamente le prove a suo carico. La difesa infatti lamenta che, nonostante essi siano stati utilizzati come prova decisiva per la sua condanna, essa non ha avuto la possibilità né di accedere a una copia dei dati di ByLock né tantomeno di sottoporli alla perizia di un esperto indipendente. Il ricorrente non avrebbe quindi potuto utilizzare i dati per contestare le conclusioni del MİT né cercare di individuare informazioni a suo favore all'interno del *data set*. I report messi a disposizione della difesa, infatti, avrebbero contenuto solamente informazioni molto generiche, indirette e non verificabili e soprattutto non avrebbero fornito alcuna indicazione in merito alle modalità tecnico-operazionali seguite dal MİT per estrapolare le informazioni rilevanti dal *data set* rendendo quindi di fatto impossibile la contestazione della prova.

La Corte sottolinea, innanzitutto, che essa non ha alcuna competenza in merito all'individuazione e alla fissazione di principi generali in materia di ammissibilità e valutazione delle prove: tale competenza rimane infatti ai singoli Stati. Ciò che la Corte deve accertare non è quindi se una prova sia ammissibile o se il ricorrente sia colpevole o meno. Essa deve solo limitarsi a verificare che il procedimento nel suo complesso sia giusto: i giudici di Strasburgo potranno quindi considerare come la prova sia stata ottenuta al fine di verificare se vi possano essere dubbi in merito alla sua affidabilità, se alla difesa sia stata data l'opportunità di contestare la prova, se l'accertamento condotto dai giudici nazionali sia stato arbitrario o manifestamente irragionevole, se sia stato rispettato il principio del contraddittorio e il principio della parità delle armi. A seguito di tale premessa, la Corte ritiene che nel caso di specie non sia necessario né accertare se i dati relativi a ByLock siano stati ottenuti nel rispetto della normativa nazionale e siano ammissibili né verificare se i giudici nazionali abbiano commesso errori nella valutazione della rilevanza di questa prova. Il compito della Corte è invece quello di accertare l'equità del procedimento nel suo complesso e quindi è sufficiente limitarsi a verificare se le modalità di acquisizione e di utilizzo della prova abbiano inciso negativamente sull'equità del procedimento e come siano state trattate dai giudici nazionali le obiezioni della difesa in relazione alla prova digitale. Le questioni che i giudici di Strasburgo devono affrontare sono quindi due: i) la qualità della prova; ii) la possibilità del ricorrente di contestarla.

In merito alla prima delle due problematiche, la Corte si dichiara immediatamente consapevole del fatto che la mancanza di un'autorizzazione preventiva o di una convalida successiva della raccolta e dell'elaborazione dei dati da parte dell'autorità giudiziaria, così come la mancanza di altre garanzie procedurali, può far sorgere dei dubbi in merito all'affidabilità e alla qualità della prova. I dubbi del ricorrente non possono quindi essere bollati come astratti e infondati come sostenuto dal Governo. In ogni caso, si rileva che l'accuratezza dei dati di ByLock ottenuti dal MİT è corroborata anche da altri metadati (in

particolare i dati CGNAT e i registri HTS), i quali sono stati utilizzati per verificare che il ricorrente, il cui *user ID* era stato individuato all'interno dei dati grezzi raccolti dal MİT, si era effettivamente connesso all'indirizzo IP di ByLock dal suo telefono. Secondo la Corte quindi non vi sarebbero sufficienti elementi per contestare l'accuratezza dei dati, almeno fintanto che essi dimostrano l'utilizzo dell'applicazione ByLock da parte del ricorrente. Le lamentele in relazione alla questione della qualità della prova vengono quindi rigettate.

La questione più problematica diviene a questo punto quella relativa all'accesso ai dati da parte della difesa. Sul punto, la Corte reitera che, in virtù del principio del contraddittorio e della parità delle armi, tutto il materiale probatorio raccolto dall'accusa deve essere condiviso con la difesa, sia esso a favore o contrario all'imputato. Questo principio vale indipendentemente dal fatto che l'accusa consideri il materiale probatorio rilevante o meno: per questo motivo anche se il ricorrente ha avuto accesso a tutti i report sui quali hanno fatto affidamento i giudici nazionali per la loro decisione, non si esclude che il ricorrente potesse avere diritto o interesse ad accedere anche ai dati grezzi, utilizzati per la preparazione dei report. A maggior ragione, se si considera che questi dati hanno giocato un ruolo decisivo per la condanna. Al tempo stesso però, i giudici europei chiariscono che il diritto alla c.d. *disclosure* della prova non è assoluto, essendovi diverse ragioni che possono giustificare il rifiuto all'accesso: la riservatezza della prova può essere necessaria per tutelare la sicurezza nazionale o per tutelare i diritti fondamentali di altri soggetti coinvolti nella vicenda. Oppure ancora, la quantità delle prove può rendere materialmente impossibile per l'accusa garantire un accesso completo alla difesa (ipotesi questa che è particolarmente centrata quando si tratta di *digital evidence*). Anche qualora il mancato accesso alla prova sia giustificato da interessi che finiscono per entrare in bilanciamento con i diritti della difesa, la Corte è comunque chiamata a esaminare se il pregiudizio derivante a questi ultimi sia stato sufficientemente controbilanciato da adeguate garanzie processuali e se sia stata effettivamente riconosciuta al ricorrente l'opportunità di preparare in maniera esaustiva la propria difesa.

Nel caso di specie, si ritiene che il mancato accesso ai dati sia giustificato e di conseguenza la legittimità del rifiuto dell'accesso ai dati grezzi debba essere valutata alla luce dell'adeguatezza delle misure procedimentali di bilanciamento rispetto a tale rifiuto. Sul punto la Corte conclude che vi sono almeno cinque ragioni per ritenere che tali misure non siano mai state adottate. In primo luogo, la richiesta del ricorrente di avere accesso ai dati grezzi è stata semplicemente ignorata dai giudici nazionali: all'interno delle decisioni della magistratura turca, infatti, non vi è alcun passaggio in cui ci si soffermi a spiegare quali siano le ragioni che giustificano il rifiuto all'accesso. Di conseguenza, il ricorrente è stato privato dell'opportunità di presentare una qualsiasi contro-argomentazione per contestare il rifiuto all'accesso. Analogamente, si indica come secondo elemento da prendere in considerazione il fatto che i giudici nazionali non abbiano fornito nessuna risposta, né in senso positivo né negativo, alla richiesta del ricorrente di sottoporre i dati grezzi alla perizia di un esperto indipendente al fine di verificarne il contenuto e l'integrità. Nonostante la Corte si dica consapevole del fatto che non esiste un obbligo delle Corti nazionali di accordare una perizia (o qualsiasi altra misura probatoria) per il solo fatto che vi sia una richiesta della difesa, al tempo stesso afferma che i giudici nazionali hanno quanto meno l'obbligo di dare una risposta appropriata a tale domanda. Ciò significa che i giudici nazionali hanno la facoltà di rigettare la richiesta della difesa, dato che comunque spetta ad essi il compito di decidere se le misure richieste siano rilevanti ed essenziali per la decisione del caso, ma saranno in ogni caso gravati dall'obbligo di motivare il rifiuto. Il terzo elemento problematico continua ad avere a che fare con la mancata risposta da parte dei giudici nazionali a questioni sollevate dalla difesa. Il ricorrente ha infatti indicato

DPCE online
ISSN: 2037-6677

ulteriori aspetti che, a suo dire, avrebbero messo in discussione l'attendibilità e l'affidabilità dei dati. Ad esempio, il ricorrente richiama il fatto che se si confrontano le diverse liste di utenti ByLock stilate dal MİT, si possono notare delle discrepanze proprio in merito all'individuazione degli stessi utenti oppure il fatto che non vi sia corrispondenza tra il numero di utenti identificati ed eventualmente perseguiti e il numero di *download* dell'applicazione. Anche in tal caso i giudici nazionali sono rimasti silenti e non hanno motivato in alcun modo il rigetto di tali questioni. Come quarto elemento viene invece citato il fatto che, anche qualora non fosse stato possibile condividere i dati grezzi con la difesa, il principio della parità delle armi avrebbe comunque imposto di condurre i procedimenti penali in una maniera tale da rendere possibile per il ricorrente commentare a pieno i dati che lo riguardavano, soprattutto per i profili relativi alla natura e al contenuto dell'attività da lui svolta sull'applicazione. I giudici nazionali hanno invece totalmente ignorato tale necessità, tanto che le loro decisioni sono state prese prima ancora che potessero essere loro consegnati i dati relativi al contenuto dei messaggi scambiati dal ricorrente su ByLock. Inoltre, la doglianza presentata dal ricorrente sul punto dinnanzi alla Corte di Cassazione è stata dalla stessa rigettata, sostenendo che tali dati non avrebbero inciso in alcun modo sull'esito del procedimento. Al contrario, per i giudici di Strasburgo è innegabile che questi elementi avrebbero potuto potenzialmente servire per rinforzare gli argomenti della difesa. Infine, il quinto e ultimo aspetto da considerare sono le lacune che caratterizzano l'argomento dell'esclusività alla base della condanna del ricorrente (v. *supra* par. 3).

Alla luce di tutti gli elementi sopra richiamati, la Corte ritiene quindi che il mancato accesso alle prove da parte della difesa non sia stato sufficientemente bilanciato da adeguate garanzie procedurali. Si riconosce quindi che la difesa non ha avuto «a genuine opportunity to challenge the evidence against him and conduct his defence in an effective manner and on an equal footing with the prosecution. Moreover, the domestic courts' failure to respond to the applicant's specific and pertinent requests and objections raised a legitimate doubt that they were impervious to the defence arguments and that the applicant was not truly heard» (punto 341). Di conseguenza, il principio del giusto processo deve intendersi violato.

5. – A seguito dell'analisi svolta, appare possibile affermare che, dal punto di vista della questione generale dell'utilizzo della *digital evidence* all'interno del procedimento penale, vi sono delle ragioni per guardare con ottimismo alla decisione, alle quali però fanno da contraltare altrettanti motivi che possono indurre a un maggiore pessimismo. Tra gli elementi che rappresentano sicuramente una nota positiva, si può citare il fatto che la Corte EDU sembra in parte aver compreso alcune delle problematicità proprie della prova digitale. In particolare, i giudici di Strasburgo riconoscono esplicitamente come «electronic evidence differs in many respects from traditional forms of evidence, including as regards its nature and the special technologies required for its collection, securing, processing and analysis. Most significantly, it raises distinct reliability issues as it is inherently more prone to destruction, damage, alteration or manipulation» (punto 312). I giudici europei si dimostrano di conseguenza consapevoli della necessità di modulare i classici standard procedurali al fine di garantire il rispetto del principio del giusto processo anche in presenza della *digital evidence*. Ad esempio, essi riconoscono, se non il diritto del ricorrente a richiedere la perizia di un esperto indipendente, quanto meno il suo interesse a presentare tale richiesta e a ricevere una risposta sul punto, alla luce della «absence of any concrete information in the case file to suggest that the data in question had at any point been subjected to examination for verification of their integrity, whether at the time of their submission to the judicial authorities in December 2016 or subsequently» (punto 333). In altre parole, data la volatilità e la

modificabilità della prova digitale, per la Corte è imprescindibile che in sede processuale venga trattata la questione della sua integrità e affidabilità, pena l'impossibilità di assicurare la corretta amministrazione della giustizia e la violazione della parità delle armi tra accusa e difesa.

Ciò detto, al riconoscimento delle specificità della *digital evidence* e delle problematiche che essa determina all'interno del procedimento penale, non sembra seguire un sufficiente coraggio da parte dei giudici di Strasburgo nello stabilire regole chiare e precise per tutti gli aspetti dell'utilizzo della prova digitale. Guardando al dibattito, sulla *digital evidence* si può infatti notare che da più parti è stata invocata l'esigenza di rileggere e ripensare le regole della procedura penale alla luce del dirompente ruolo assunto oggigiorno dalla prova digitale, tanto da arrivare ad auspicare la nascita di una procedura penale nuova (v. O.S. Kerr, *Digital Evidence and the New Criminal Procedure*, in 105(1) *Columbia Law Review* 279-318 (2005)). Al tempo stesso è stata spesso sottolineata la necessità di fornire uniformità alle regole relative alla prova digitale: la *digital evidence* è infatti oggetto di legislazioni nazionali profondamente differenti, così come diversi continuano ad essere gli attori coinvolti a livello internazionale, sovranazionale e nazionale. È chiaro come da questa frammentazione possano facilmente nascere disaccordi o contrasti in merito a come "maneggiare" questa tipologia di prova (sulla questione della frammentazione v. M.A. Biasiotti, J.A. Cannataci, M. Bonnici, J. Pia, F. Turchi, *Introduction: Opportunities and Challenges for Electronic Evidence*, in Id. (Eds), *Handling and Exchanging Electronic Evidence Across Europe*, in 39 *Law, Governance and Technology Series* 3-12 (2018)). La Corte EDU potrebbe contribuire al superamento della frammentazione e delle problematiche connesse all'utilizzo della *digital evidence*, potendo assumere il ruolo di pioniere nell'elaborazione un vero e proprio "statuto della prova digitale" (L. Bartoli, *Parità delle armi e discovery digitale: qualche indicazione da Strasburgo*, in *La legislazione penale*, 1, 2022, 3-13). Le occasioni che si sono presentate però non sono mai state sfruttate a pieno dai giudici di Strasburgo e il caso in commento conferma questo andamento. Si pensi all'esempio citato sopra: sul tema della veridicità, dell'attendibilità e dell'autenticità della prova digitale, la Corte si limita a prendere atto che le autorità nazionali turche non hanno condotto verifiche in merito e a riconoscere l'interesse del ricorrente a richiedere la perizia di un esperto indipendente. Si sarebbe invece potuto, almeno a livello di *obiter dicta*, affermare la necessità che all'interno della *discovery* digitale venga tenuta traccia della *chain of custody*. Anche perché, come è stato fatto notare, «it is questionable if the defence (and in some cases the judge) have a sufficient possibility to contest the authenticity and quality of the digital evidence by the prosecution. This safeguard cannot be realized if data processing is not sufficiently documented to establish the evidence origin, acquisition, examination, and analysis» (R. Stoykova, *The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations*, in 49 *Computer Law & Security Review* 9 (2023)).

Tornando alle note positive, è incoraggiante che, nonostante la Corte EDU si sia mostrata consapevole delle difficoltà e delle sfide tecniche e pratiche che le autorità giudiziarie si trovano ad affrontare di fronte alla *digital evidence*, essa abbia comunque ritenuto essenziale sottolineare che «these factors do not in the abstract call for the safeguards under Article 6 § 1 to be applied differently, be it more strictly or more leniently» (punto 313). La Corte cioè afferma a chiare lettere che il principio del giusto processo dev'essere applicato e osservato con la stessa intensità di sempre. La presa di posizione appare poi ancora più forte, se ci si sofferma sul fatto che nonostante l'importanza che la prova digitale riveste per il contrasto al fenomeno terroristico, i giudici europei dichiarano che «while the fight against terrorism may necessitate resorting to such evidence, the right to a fair trial, from which the requirement of the proper administration of justice is to be inferred, applies to all types of criminal offence, from the most straightforward to the most

DPCE online
ISSN: 2037-6677

complex. The right to the fair administration of justice holds so prominent a place in a democratic society that it cannot be sacrificed for the sake of expediency and the evidence obtained, whether electronic or not, may not be used by the domestic courts in a manner that undermines the basic tenets of a fair trial» (punto 344). Il principio del giusto processo appare quindi un limite invalicabile: sarà possibile deviare da alcuni standard procedurali per assicurare il soddisfacimento di altri rilevanti interessi, come ad esempio la tutela della sicurezza nazionale, ma in ogni caso sarà sempre necessario che l'essenza del principio del giusto processo venga salvaguardata. La Corte sembra non considerare ammissibile alcuna tendenza illiberale.

La portata di quest'ultima affermazione sembra essere però ridimensionata dal fatto che anche nel caso in commento pare possibile scorgere le tracce del ricorso a quell'approccio compensativo che dalla sentenza *Al-Khawaja e Tahery c. Regno Unito* (Corte Europea dei Diritti dell'Uomo, Grande Camera, *Al-Khawaja e Tahery c. Regno Unito*, ricorso n. 26766/05 e 22228/06, del 15 dicembre 2011) caratterizza la giurisprudenza di Strasburgo in tema di art. 6, CEDU (v. A. Boldrin, *Approccio compensativo e overall fairness nella giurisprudenza della Corte EDU, tra relativismo delle garanzie e altre derive*, in *La legislazione penale*, 4, 2021, 28-58; M. Caianiello, *You can't always counterbalance what you want*, in 25(4) *European Journal of Crime, Criminal Law and Criminal Justice* 283-298 (2017)). In passato la Corte si era sempre dimostrata particolarmente attenta alle questioni riguardanti tale articolo, assumendo un'attitudine di forte protezione del principio del giusto processo, pur sanzionando le violazioni delle garanzie ex art. 6 non singolarmente, ma solamente qualora esse incidessero sull'equità del procedimento "*as a whole*" (c.d. approccio olistico, fra le numerose sentenze si vedano ad esempio le decisioni *Kostovski c. Paesi Bassi, Edwards c. Regno Unito, Saidi c. Francia, Bracci c. Italia*). A partire dal sopracitato caso *Al-Khawaja e Tahery c. Regno Unito*, invece, pare si stia assistendo all'estremizzazione di questo atteggiamento (c.d. approccio compensativo): il giudice europeo sembra non limitarsi più al solo accertamento della lesione delle garanzie del giusto processo e alla valutazione dell'equità del processo "*as a whole*", bensì esso si spinge a valutare se l'effetto negativo derivante da una di queste violazioni sia stato o meno controbilanciato da altri elementi del procedimento, indicando spesso come misure compensative elementi che in realtà sono garanzie che già di per sé dovrebbero essere assicurate all'imputato. Tale logica sembra essere stata applicata anche nel caso in commento, in particolare in relazione al mancato accesso ai *raw data*: dopo che la Corte ha riconosciuto che il diritto all'accesso del ricorrente non è assoluto, ma può subire delle limitazioni dovute al necessario bilanciamento di questo diritto con ulteriori interessi meritevoli di tutela, essa non si concentra tanto sulla questione della legittimità del rifiuto di concedere l'accesso alla prova, bensì si focalizza soprattutto sulla presenza di garanzie procedurali che avrebbero potuto compensare tale mancanza. Nell'individuare tali elementi però indica anche garanzie spettanti all'imputato già *ab origine*. Ad esempio, dalle parole della Corte emerge che se i giudici nazionali avessero sufficientemente valutato le questioni sollevate dal ricorrente e motivato le loro decisioni, ciò avrebbe potuto compensare il rifiuto della *disclosure*. Ma l'obbligo del giudice di valutare compiutamente e di dare risposta (anche se non esplicita) a tutte le questioni rilevanti in sede processuale non è forse una garanzia che persiste in ogni frangente? È possibile giustificare il mancato rispetto di una garanzia processuale facendo riferimento al fatto che è invece ne è stata rispettata un'altra, nonostante l'osservanza di quest'ultima sia imposta in partenza dalle norme convenzionali? Se è vero che l'esito finale della vicenda, ossia il riconoscimento della violazione delle disposizioni convenzionali e la conseguente condanna della Turchia, appare soddisfacente, meno tranquillizzante risulta la ricostruzione avanzata dalla Corte per arrivare a tale conclusione. L'esito

apparentemente positivo della vicenda potrebbe in realtà mascherare una preoccupante tendenza della Corte ad attenuare la tutela ex art. 6. In un'epoca in cui le garanzie del giusto processo vengono messe a dura prova anche dall'irrompere sulla scena della *digital evidence*, la risoluzione del presente caso non pare quindi pienamente convincente. Il rischio è che le parole spese dai giudici di Strasburgo sull'inviolabilità del principio del giusto processo vengano depotenziate da tale approccio e rimangano appunto solamente parole.

Raffaele Prettato
Dipartimento di Scienze Giuridiche
Università degli Studi di Udine
prettato.raffaele@spes.uniud.it