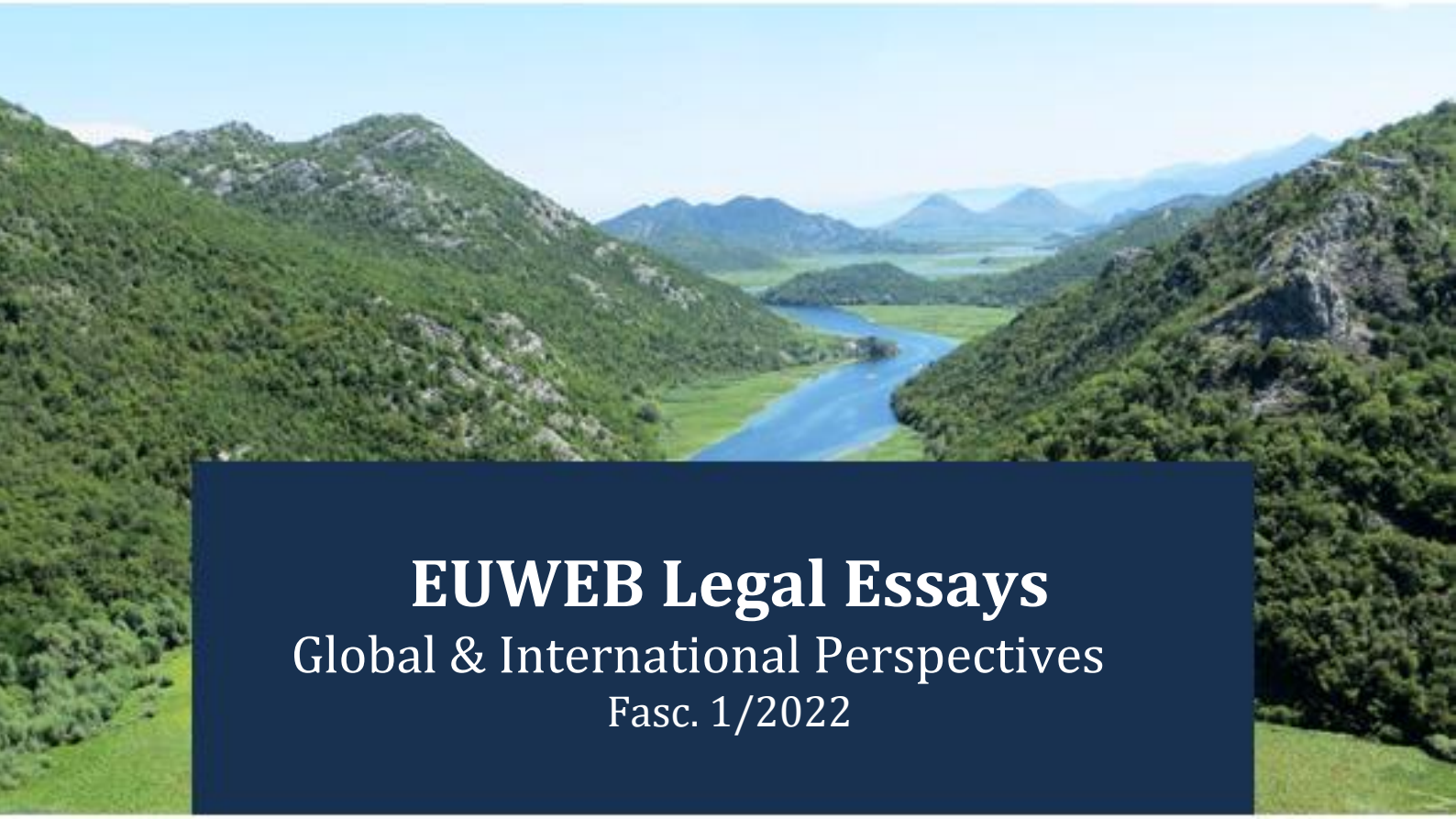
ISSN 2785-5228

EUWEB
EU-WESTERN BALKANS
Cooperation on Justice and Home Affairs



EUWEB Legal Essays

Global & International Perspectives

Fasc. 1/2022

EDITORIALE SCIENTIFICA

Rivista semestrale on line EUWEB Legal Essays. Global & International Perspectives
www.euweb.org
Editoriale Scientifica, Via San Biagio dei Librai, 39 – Napoli
Registrazione presso il Tribunale di Nocera Inferiore n° 5 del 23 marzo 2022
ISSN 2785-5228

Index
2022, n. 1

Databases and Protection of Human Rights

LA PROLIFERAZIONE DELLE BANCHE DATI DI POLIZIA E LA TUTELA EUROPEA DEI DATI PERSONALI: ALCUNE PROSPETTIVE ED ALCUNI LIMITI DELLA DIRETTIVA (EU) 2016/680

di Pietro Milazzo[*]

1. Introduzione

Il settore della cooperazione di polizia è notoriamente considerato un ambito di particolare delicatezza, nel più ampio quadro della integrazione europea, perché attiene al cuore stesso della sovranità in una delle sue forme più tradizionali ed evidenti: l'esercizio dell'attività di polizia, appunto, con tutto ciò che essa comporta in termini di bilanciamento fra diritti e autorità, e – sotto un diverso ma connesso profilo – anche in termini di "identità" (politica e costituzionale) degli Stati.

Non è possibile in questa sede approfondire l'argomento, ma si può dare per acquisito che proprio questi profili hanno reso necessario un percorso particolarmente cauto del legislatore comunitario nell'affermazione del "vecchio" terzo pilastro, ed anche nel successivo contesto dello spazio di libertà sicurezza e giustizia e con i nuovi strumenti attivati dal Trattato di Lisbona[1]. Può sembrare in qualche misura paradossale, ma la cooperazione di polizia si è dimostrata un settore più "difficile" – ovviamente nell'ottica dell'integrazione e del dispiegamento delle potenzialità evolutive insite nei Trattati – rispetto alla stessa cooperazione giudiziaria. In effetti, quest'ultima aveva goduto di forme più strutturate e consolidate di collaborazione interstatuale anche in passato, mentre la cooperazione di polizia, che pure – come fenomeno storico – risale ad epoche tutt'altro che recenti, era stata caratterizzata dal sovrapporsi di iniziative molto diverse per portata, contenuto e finalità, soprattutto con riguardo alla effettiva intensità della cooperazione fra polizie o fra stati in ambito poliziesco e con riguardo allo stesso quadro giuridico in cui tali forme di cooperazione andavano sviluppandosi (o non sviluppandosi affatto)[2]: quello che efficacemente è stato definito un "arcipelago" di forma di cooperazione.[3] Su questo quadro si è poi innestata la cooperazione propriamente euro-unitaria, la quale a sua volta ha avuto un avvio piuttosto controverso e linee di sviluppo non sempre coerenti[4].

---

[*] Professore associato in Istituzioni di diritto pubblico, Dipartimento di Giurisprudenza – Università di Pisa.

[1] Ho cercato di inquadrare il profilo del rapporto fra sovranità nazionale, specialmente alla luce del Trattato di Lisbona, in P. MILAZZO, *Al cuore della sovranità. Cooperazione europea di polizia e legislazioni nazionali*, in E. CATELANI (a cura di), *L'ordinamento giuridico italiano nello "Spazio di libertà, sicurezza e giustizia"*, Napoli, 2014, pp. 33-46.

[2] Per una analisi sulle forme di cooperazione di polizia antecedenti l'ingresso della materia nell'ambito del diritto dell'Unione, volendo, P. MILAZZO, *Quadro costituzionale italiano e cooperazione europea di polizia. Elementi istituzionali e ricostruttivi per un bilanciamento complesso*, Napoli, 2012, p. 1-77.

[3] D. BIGO, *Polices en réseaux: l'experience européenne*, Parigi, 1996.

[4] Per una ricostruzione sulle prime fasi della applicazione del "terzo pilastro" dopo il Trattato di Maastricht, cfr., fra gli altri, C. CHEVALLIER-GOVERS, *De la cooperation à l'integration policière dans l'Union européenne*, Bruxelles, 1999, p. 55 e ss.

ISSN 2785-5228
DOI: 10.1400/287611

Un punto però è subito emerso come significativo e qualificante. Quando ci si è interrogati su quali fossero gli aspetti di maggior delicatezza della cooperazione europea (nel senso di euro-unitaria) di polizia, su quali profili le possibili forme di cooperazione incidessero in modo significativo, quale fosse l'ambito in cui l'equilibrio fra sovranità nazionale (declinata specialmente sub specie di livello nazionale di tutela dei diritti) e integrazione e cooperazione fosse messo in maggior crisi, si è sempre rilevato che questo aspetto, questo profilo e quest'ambito riguardasse soprattutto il settore della tutela dei dati personali. Anche se altri contesti di cooperazione possono apparire più "forti" e più invasivi delle tradizionali competenze e funzioni poliziesche nazionali (si pensi, solo ad esempio, al tema del diritto di inseguimento, alle squadre investigative comuni, ecc.), si è constatato che in realtà, le forme di cooperazione operano soprattutto mediante lo scambio di dati: dati personali, dati di *intelligence*, dati relativi ad inchieste, e così via. È quindi la "trincea" della protezione della riservatezza e dei dati personali quella in cui si combatte la battaglia fra cooperazione di polizia e tutela dei diritti, ed amplificando anche il confronto fra sovranità nazionali e integrazioni in questo campo.

In tale contesto generale, con questo contributo ci si ripropone di esaminare sinteticamente le problematiche che si possono considerare insorte a seguito dell'approvazione dell'atto di massima integrazione (finora) proprio nel settore della tutela dei dati personali nell'ambito della cooperazione europea di polizia: la Direttiva 2016/680/EU (nota come *Law Enforcement Directive*, e d'ora in avanti semplicemente la "LED")[5]. Più che descriverne il contenuto[6], ci si propone dunque di verificare se essa in effetti, come appariva chiaro ai suoi fautori ed ai suoi autori, sia stata in grado di costruire un quadro stabile di riferimento per questa delicata materia, o non lasci ancora adito a dubbi interpretativi che, in un contesto in cui "in gioco" ci sono diritti fondamentali ed equilibrio fra sovranità ed integrazione, possono dar luogo a problematiche significative. La selezione – necessariamente parziale – delle problematiche che la LED solleva è effettuata proprio nell'ottica interpretativa complessiva di valutazione del complessivo punto di equilibrio raggiunto dalla LED rispetto alle "forze" che operano contestualmente, e spesso conflittualmente, nella materia.

2. Antecedenti, problemi e (tentativi di) soluzione

La LED non nasce in una situazione di vuoto giuridico. La materia del trattamento dei dati personali in contesti di cooperazione di polizia, infatti, era affidata ad un contesto normativo piuttosto sconnesso e variegato, ma tutt'altro che assente. Si poteva riscontrare una significativa frammentazione delle fonti di disciplina e delle scelte normative, così come una sorta di "settorializzazione" per cui ad aspetti diversi della cooperazione di polizia (od anche a diversi oggetti della cooperazione stessa) corrispondevano strumenti e livelli di tutela dei dati personali anche molto diversificati. Questa diversificazione poteva dipendere dal tipo di dati oggetto del trattamento (vi erano ad esempio discipline

[5] Direttiva 2016/680/UE del Parlamento europeo e del Consiglio, *relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio*, del 27 aprile 2016.

[6] Si è tentata una operazione di lettura complessiva della LED in P. MILAZZO, *La direttiva 2016/680/UE e la protezione dei dati personali nell'ambito della sicurezza pubblica e della giustizia penale*, in L. CALIFANO, P. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017, pp. 709-739, cui volendo si può rinviare per gli aspetti di carattere descrittivo della direttiva.

dedicate alla raccolta delle impronte digitali, o al DNA), dal tipo di soggetto destinato a porre in essere il trattamento stesso (come ad esempio, Eurojust, o Europol), o anche dal tipo di base normativa di volta in volta utilizzata: vi erano (ed in parte, come si dirà, vi sono ancora) trattamenti basati sul "quadro-Schengen" con la sue diverse disposizioni riconducibili alla cooperazione di polizia e con i diversi soggetti abilitati a porre in essere le relative attività, altri basati sul quadro Eurodac, altri sulla Convenzione sulla mutua assistenza in materia penale, altri sugli atti in materia di squadre investigative comuni, ecc. In alcune occasioni, le disposizioni sulla tutela dei dati sono state inserite come un aspetto di una regolamentazione più generale della materia, mentre in altri casi sono stati isolati in un corpus normativo a sé stante, quasi a volere significare la posizione particolarmente rilevante e quasi plasticamente "oppositiva" rispetto alle disposizioni relative specificamente all'esercizio dei poteri di polizia in sede di cooperazione.

Anche in questo caso, quindi, una sorta di *arcipelago regolatorio* di sistemi di protezione rispetto al trattamento dei dati coinvolti in contesti di cooperazione di polizia; con ciò che tale situazione può comportare in punto di certezza del diritto, di possibili antinomie e conflitti, ed in definitiva di livello effettivo di tutela del diritto.

Un arcipelago, però, non privo di alcuni elementi unificanti, peraltro caratterizzati da un "segno" diverso.

Un primo versante di tali caratteri unificanti verte sul piano dei parametri di tutela del diritto. Tutte le diverse fonti di disciplina, infatti, citano espressamente – con riferimento al livello di tutela garantito – due riferimenti normativi che quindi si pongono come parametri significativi di questa evoluzione tumultuosa ed indubbiamente non particolarmente coordinata: la Convenzione n.108 del Consiglio d'Europa e la Raccomandazione n. R(87) 15 elaborata nel medesimo contesto e specificamente per l'attività di polizia. C'è poi da tenere in considerazione la giurisprudenza della Corte europea dei diritti dell'uomo, che è molto copiosa in materia di dati personali, e che in alcune occasioni si è occupata specificamente del trattamento dei dati di polizia. In particolare, la Corte di Strasburgo ha sempre considerato l'archiviazione e la conservazione di dati personali da parte di autorità nazionali di polizia o di sicurezza come una "ingerenza" nella vita privata ai sensi dell'art. 8 par. 1 CEDU, e dunque da fare oggetto di scrutinio sul parametro della necessarietà in una società democratica per garantire la valori previsti nel secondo comma dello stesso art. 8, in quanto "*in linea di principio qualsiasi trattamento dei dati personali effettuato da un terzo è idoneo a costituire pregiudizio a tali diritti*"[7].

Il secondo versante "unificante" è invece relativo alle modalità generali di trasmissione e trattamento dei dati di polizia. A partire almeno dal Consiglio europeo di Tampere del 1999 ed attraverso il Programma dell'Aia del 2004, infatti, si è affermato in materia il cd. "principio di disponibilità", secondo il quale "*a law enforcement officer in one Member State of the Union who needs information in order to carry out his duties can obtain it from another Member State and that the law enforcement authorities in the Member State that holds this information will make it available for the declared purpose, taking account of the needs of investigations pending in that Member State*"*;* e tale assetto dovrebbe realizzarsi attraverso l'accesso reciproco o l'interoperabilità di basi di dati nazionali. Tale principio ha una portata potenzialmente dirompente, perché tende a prescindere dalle "gelosie" nazionali in punto di informazioni di polizia, avendo lo scopo di garantire in termini più intensi la circolazione dei dati nei quadri di cooperazione, e

[7] Cfr. Corte europea dei diritti dell'uomo, sentenza del 18 aprile 2013, ricorso n. 19522/09, *M. K. c. Francia*; Corte europea dei diritti dell'uomo, sentenza del 4 dicembre 2008, ricorsi nn. 30562/04 e 30566/04, *S. e Marper c. Regno Unito*; Corte europea dei diritti dell'uomo sentenza del 26 marzo 1987, ricorso n. 27798/95, *Laender c. Svezia*.

tende altrettanto ovviamente a rendere più accentuato il problema del rapporto con la protezione dei dati personali specialmente in contesti di evoluzione tumultuosa degli strumenti tecnici a disposizione delle forze di polizia (tali da far presagire, da parte dei più pessimisti, una sorta di controllo generalizzato).

Il principio di disponibilità è senz'altro l'acceleratore perfetto per un approccio considerato innovativo alla cooperazione di polizia (soprattutto all'indomani dei grandi attentati terroristici del 2001 negli Stati Uniti e del 2005 nell'Unione europea) ed è quindi il *leit-motiv* di tutta la normazione euro-unitaria immediatamente antecedente la LED: sono ispirati a questo principio, ad esempio, la Decisione Quadro 2006/960/GAI, così come la cd. "Decisione di Prüm"[8], che hanno costituito probabilmente il grado più avanzato di cooperazione nel citato periodo[9].

Il punto finale di questo complesso e frammentato percorso, traversato peraltro dalle citate nervature unificanti, può essere considerato il "dittico" della Decisione quadro 2008/977/GAI e della Decisione 2008/615/GAI. Qui l'ambizione era effettivamente quella di creare una base unica e comune a diversi trattamenti di polizia, cercando di superare proprio il problema della frammentazione cui si è accennato. Anche questo step della legislazione eurounitaria, però, ha scontato problemi non piccoli di concezione, di struttura e di attuazione. In primo luogo, anche le decisioni del 2008 – come sostanzialmente tutti gli atti europei fino a quel momento – avevano ad oggetto solo gli scambi internazionali di informazioni di polizia, e non invece la legislazione "domestica" (interna) in questa materia. Inoltre, la Decisione Quadro del 2008 dichiarava espressamente la propria applicabilità sostanzialmente in termini residuali rispetto alle normative relativa ai vari "quadri" di cooperazione speciali di cui si è detto: con ciò mostrando di non essere di fatto in grado di sostituirsi – almeno sotto questo profilo – alla natura significativamente frammentata del quadro normativo in materia: rimanevano di fatto vigenti ed operanti dei "microsistemi" di disciplina del trattamento dei dati in singoli contesti di cooperazione, relativamente ai quali le decisioni del 2008 operavano solo in caso di loro inidoneità a regolare il caso di specie (circostanza di fatto piuttosto rara, almeno in quei settori in cui il legislatore europeo si era speso creando "microsistemi" di fatto autosufficienti). Da un punto di vista procedurale, poi, le decisioni del 2008 si collocavano a ridosso del Trattato di Lisbona, ma in una fase antecedente rispetto alla sua entrata in vigore. Trattandosi di atti pre-Lisbona, la materia della cooperazione di polizia implicava l'applicazione delle "vecchie" regole, e dunque essenzialmente il necessario ricorso alla unanimità per eventuali modifiche degli atti stessi.

Infine, *but not least,* sotto un profilo più di merito, le decisioni del 2008 sono state giudicate generalmente impostate in modo da far prevalere – nel bilanciamento fra esigenze securitarie e garanzie di tutela dei diritti – le prime rispetto alle seconde[10].

Ma, come si è accennato, questo bilanciamento – che da un punto di vista politico aveva effettivamente subito una certa lettura securitaria nei primi anni del XXI secolo – doveva fare i conti con una giurisprudenza della Corte europea dei diritti dell'uomo e della Corte di Giustizia assai più equilibrata e garantista rispetto alle esigenze di tutela dei diritti dei titolari dei dati "di polizia". Questa considerazione, assieme alle altre sopra

[8] R. BELLANOVA, *The "Prüm Process", the Way Forward for EU Police Cooperation and data Exchange?*, in E. GUILD, F. GEYER (a cura di), *Security Versus Justice? Police and Judicial Cooperation in the European Union*, Ashgate, 2008, p. 203.

[9] Come è noto, molti dei contenuti del Trattato di Prüm, stipulato inizialmente solo da alcuni dei paesi membri dell'Unione come una sorta di cooperazione rafforzata (non in senso formale), sono poi stati trasposti nelle decisioni 615/2008/GAI e 616/2008/GAI, in cui il punto di riferimento essenziale risulta essere appunto l'affermazione del principio di disponibilità.

[10] D. BIGO, *EU Police Cooperation: National Sovereignity Framed by European Security?*, in E. GUILD, F. GEYER (a cura di), *op. cit.*, p. 91 e ss.

indicate – che avevano fatto nascere "già vecchie" le decisioni del 2008 – ed alla circostanza per cui ci si apprestava a varare una nuova disciplina generale sul trattamento dei dati nell'Unione europea, hanno quindi indotto il legislatore ad elaborare la LED, che dunque è nata in parallelo al Regolamento (EU) 2016/679 (d'ora in avanti, il "GDPR"), e di quella normativa riprende in misura significativa i principi fondamentali, cercando di adattarli ad un settore così particolare e caratterizzato. La prima e forse principale differenza fra il GDPR e la LED è quella per cui mentre nel primo caso viene garantito agli interessati un diritto di informazione e di accesso ai dati personali detenuti e trattati, nel settore criminale questa pienezza informativa non risulta effettivamente realizzabile, perché verosimilmente potrebbe rendere impossibili o eccessivamente difficoltose le indagini ed i procedimenti penali. È stato quindi necessario – in questa materia – ricalibrare il bilanciamento fra diritto alla protezione dei dati personali e le esigenze di corretto ed efficace svolgimento delle attività connesse alla prevenzione e al perseguimento dei reati.

D'altra parte, mentre il GDPR è molto commentato e benissimo conosciuto in tutti i paesi d'Europa, la LED – come è stato icasticamente rilevato – ha una sorta di "*shadowy existence*"[11] che rende sicuramente interessante ed opportuno rilevarne taluni aspetti critici o dubbi.

3. I problemi relativi al "perimetro" della LED

Come anticipato, la LED nasce insieme al GDPR, e ne condivide l'ambizione potremmo dire generalizzante, cioè di porsi come strumento orizzontale applicabile a tutti i trattamenti di dati di polizia (per la prima volta – e questa è una novità di grande portata – anche quelli puramente "domestici"). Non ne condivide lo strumento: è una direttiva, appunto, e non un regolamento. Si tratta dell'ennesima conferma che: (i) per quanto anche la cooperazione di polizia si sia "lisbonizzata" quanto al regime degli atti europei, (ii) per quanto oltre trenta anni di cooperazione *in action* abbiano senz'altro esercitato una forte pressione in favore dell'integrazione (si pensi solo ai progressi di non poco momento riconducibili alla cooperazione via Europol[12]), (iii) per quanto l'Unione abbia acquisito un *framework* in materia di diritti sempre più significativo e tale da garantire una tutela molto forte[13] proprio in punto di protezione dei dati personali[14], eppure la materia è sempre particolarmente sensibile in quanto attiene ad un aspetto percepito dagli stati come quanto di più vicino alla essenza stessa della sovranità, come anche espressamente indicato ad esempio nella ben nota giurisprudenza costituzionale tedesca sui Trattati[15].

---

[11] T. RADTKE, *The Concept Of Joint Control Under The Data Protection Law Enforcement Directive 2016/680 in Contrast to the GDPR*, in *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 2020, n. 11, pp. 242-252.

[12] Sulla quale, volendo, P. MILAZZO, *Article 88 [Europol]*, in H.J. BLANKE, S. MANGIAMELI (a cura di), *Treaty on the Functioning of the European Union – a Commentary*, Berlin-Heidelberg, 2021, pp. 1671-1698.

[13] La stessa LED indica proprio in alcuni elementi di questo *framework* il proprio fondamento: l'art. 8 comma 1 della Carta dei diritti fondamentali, dedicato proprio alla protezione dei dati personali (laddove non tutte le Costituzioni nazionali, elaborate spesso in periodi più risalenti, prevedono un diretto riferimento a tale principio); l'art. 16 TFUE che colloca tale principio nel quadro del Trattati; la già citata Dichiarazione n.21 allegata al Trattato di Lisbona.

[14] Si veda la ampia ricostruzione di G. GONZÁLEZ FUSTER, *The Emergence of Personal Data as a Fundamental Right of the EU*, New York, 2014.

[15] Ci si riferisce soprattutto alla nota sentenza del 30 giugno 2009 del *Bundesverfassungsericht* sul Trattato di Lisbona, nella quale il *BVerfG* ha indicato come il processo di integrazione nell'Unione europea non possa estendersi fino a comprimere eccessivamente una "*sfera effettiva di azione*" da riconoscersi alla

Ciò implica che lo strumento del regolamento, con la sua portata uniformizzante e la sua efficacia diretta, non si presti (ancora?) a costituire il mezzo ottimo per disciplinare il settore, e gli Stati si sentano ancora nella necessità di disporre di un margine di apprezzamento (invero significativo[16]) sulle scelte da operare nella materia: come peraltro reso evidente dalla stessa Dichiarazione n. 21 allegata al Trattato di Lisbona[17], che fa riferimento proprio alla necessità di "*norme specifiche*" (cioè differenti da quelle generali) sulla protezione dei dati in virtù della "*specificità dei settori in questione*".

Un primo aspetto problematico che merita di essere trattato riguarda la effettiva capacità della LED di porsi come strumento generale. È in grado la LED di superare la situazione che abbiamo descritto come un arcipelago di microcosmi normativi in materia di trattamento dei dati "di polizia"? L'art. 60 della LED stabilisce che "*rimangono impregiudicate le disposizioni specifiche per la protezione dei dati personali contenute in atti giuridici dell'Unione che sono entrati in vigore il o anteriormente al 6 maggio 2016 nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia, che disciplinano il trattamento tra Stati membri e l'accesso delle autorità nazionali designate ai sistemi d'informazione istituiti ai sensi dei trattati, nell'ambito di applicazione della presente direttiva*". Una disposizione di questo tipo sembra confermare la incapacità della LED di sostituirsi ai vari "microcosmi" normativi, e dunque la persistenza di una situazione di convivenza fra uno schema sostanzialmente uniformante, e varie ulteriori sedi in cui invece continua ad applicarsi – su soggetti sostanzialmente convergenti nella medesima materia – una disciplina speciale[18]. E tale conferma di una certa frammentazione della materia, con le connesse possibili contraddizioni o incertezze applicative, sembra anche ribadito da taluni interventi normativi successivi alla LED nei quali viene riproposto un modello "speciale" di trattamento dei dati personali in abiti riconducibili alla cooperazione di polizia[19].

Va però detto che l'art. 62 comma 6 della LED chiama la Commissione europea ad una attività di riesame gli altri atti giuridici adottati dall'Unione che disciplinano il trattamento da parte delle autorità di polizia, "*in particolare quelli di cui all'articolo 60*", al fine di valutare la necessità di allinearli alla LED e formulare, ove opportuno, le proposte necessarie per modificarli in modo da garantire un approccio coerente alla protezione dei dati personali nell'ambito della LED stessa. Al momento in cui si scrive,

---

repubblica federale, specialmente in ambiti sensibili per la sovranità nazionale, fra i quali figurano il diritto e la procedura penale, e l'uso legittimo della forza. Su tale sentenza, fra i moltissimi, cfr., L. VIOLINI, *Tra il vecchio e il nuovo. La sentenza* Lissabon *del* Bundesverfassungsgericht *alla luce dei suoi più significativi precedenti*: Solange, Maastricht, Bananen, in *www.astrid.eu*, 2009; M. LUCIANI, *Il* Bundesverfassungsgericht *e le prospettive dell'integrazione europea*, in *www.astrid.eu*, 2009.

[16] T. MARQUENIE, *The Police and Criminal Justice Authorities Directive: Data Protection Standards and Impact on the Legal Framework*, in *Computer Law & Security Review*, Vol. 33, Issue 3, 2017, pp. 324-340.

[17] Secondo la quale "*la conferenza riconosce che potrebbero rivelarsi necessarie, in considerazione della specificità dei settori in questione, norme specifiche sulla protezione dei dati personali e sulla libera circolazione di tali dati nei settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia, in base all'articolo 16 del trattato sul funzionamento dell'Unione europea*".

[18] Tale prospettiva è assunta ad esempio da G. RUGANI, *La protezione dei dati nel settore della cooperazione giudiziaria e di polizia in materia penale alla luce della direttiva (UE) 2016/680: frammentazione e incertezze applicative*, in *Freedom, Security & Justice: European Legal Studies*, n. 1, 2019, pp. 75-93.

[19] Il riferimento è soprattutto al Regolamento (UE) 2016/794 – quindi successivo alla LED – nel quale sono state ridisciplinate l'attività e l'organizzazione di Europol. In quella sede si sono previste regole specifiche per il trattamento dei dati nel quadro appunto di Europol (non completamente sovrapponibili alle disposizioni della LED), e si è indicato come "*le norme di protezione dei dati applicabili presso Europol dovrebbero essere autonome e nel contempo coerenti con quelle di altri strumenti pertinenti di protezione dei dati applicabili nel settore della cooperazione di polizia nell'Unione*" (Considerando n. 40: cfr. G. RUGANI, *op. cit.*, p. 86.

la Commissione ha rilasciato una Comunicazione[20] nella quale ha dato atto di avere effettuato la ricognizione richiesta dall'art. 62 della LED, e di avere rilevato che taluni atti non richiedono affatto allineamento (perché, ad esempio, non contengono disposizioni sul trattamento dei dati "di polizia" e quindi troverà applicazione la LED non appena attuata dagli Stati), mentre diversi altri richiedono effettivamente un allineamento, il cui meccanismo e la cui tempistica è di volta in volta indicata dalla Commissione stessa[21]. In altre parole, è certamente vero che la LED, di per sé, non ha saputo porsi come un quadro unico di riferimento nella materia della protezione/trattamento dei dati "di polizia" (come invece, ad esempio, fa il GDPR per i dati in generale), tale da superare del tutto il quadro frammentario esistente. Ma certamente la LED ha imposto una attività di convergenza verso i suoi contenuti ed i principi da essa espressi anche da parte degli altri "microcosmi" normativi esistenti: i quali dunque sono fatti salvi, ma devono tendere verso l'allineamento alla LED. Sotto questo profilo *de iure condendo* la LED sembra avere una efficacia – perlomeno potenziale – che nessun altro atto dell'ex "terzo pilastro" ha mai avuto nella materia della protezione dei dati (dietro la quale, lo si ricorda, si cela il punto più generale e delicato del rapporto fra attività di polizia e tutela del principale diritto ad oggi potenzialmente leso da tale attività). Ovviamente, molta della effettività di questa prospettiva armonizzante dipende da come gli Stati decidono di dare attuazione dalla LED esercitando il loro margine di manovra e di apprezzamento, e della capacità/volontà della Commissione di farsi in concreto interprete ed attore principale dei processi di modifica degli atti che richiedono l'allineamento stesso.

Sotto un secondo profilo, il "perimetro" della LED appare non completamente chiaro anche in relazione al fondamentale profilo del novero di trattamenti di dati che possono essere considerati ricompresi nel suo oggetto. L'art. 2 comma 3 della LED, infatti, stabilisce che la direttiva non si applica ai trattamenti di dati personali: "*a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione; b) effettuati da istituzioni, organi, uffici e agenzie dell'Unione*". Già di per sé questa formula si presta ad una certa ambiguità di fondo, che peraltro appare accentuata dalla lettura del considerando n. 14, secondo il quale l'esclusione del trattamento di dati personali nell'ambito di un'attività che non rientra nell'ambito di applicazione del diritto dell'Unione, comporterebbe l'esclusione dei trattamenti "*concernenti la sicurezza nazionale, le attività delle agenzie o unità che si occupano di questioni connesse alla sicurezza nazionale*", così come il trattamento dei dati personali effettuato dagli Stati membri nell'esercizio di attività rientranti nell'ambito della politica estera e sicurezza comune.

Questa limitazione si presta a qualche osservazione. La "sicurezza nazionale" (i cui trattamenti di dati non sarebbero interessati dalla LED), infatti, non appare un concetto così ben definito da poter essere chiaramente distinta dalla "pubblica sicurezza" (i cui trattamenti invece ricadrebbero senz'altro nella LED[22]). Da un punto di vista schiettamente giuridico, infatti, non sembra sussistere una netta separazione fra le due

[20] Comunicazione della Commissione al Parlamento Europeo e al Consiglio, *Via da seguire per allineare l'acquis dell'ex terzo pilastro alle norme sulla protezione dei dati*, del 24 giugno 2020, COM(2020) 262 final.

[21] Si tratta, ad esempio, del sistema attivato dalla Decisione quadro 2002/465/GAI sulle squadre investigative comuni, dell'applicazione della Decisione quadro 2006/960/GAI sulla semplificazione dello scambio dei dati nella attività di intelligence, della Decisione 2008/615/GAI, già citata, sul potenziamento della cooperazione transfrontaliera soprattutto in materia di lotta al terrorismo ed alla criminalità transfrontaliera.

[22] L'art. 1 della LED, infatti, prevede che essa si applichi al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica.

attività, tale da rendere chiaro ed evidente il rispettivo ambito di applicazione[23]. Più in particolare, non sembra si possa escludere che possa sussistere una zona d'ombra in cui ad attività che astrattamente potrebbero essere considerate di pubblica sicurezza (volte alla prevenzione e repressione dei reati) potrebbe essere impressa una lettura diversa, che possa farle assurgere a problemi di sicurezza nazionale: ad esempio, a seguito di una evoluzione della sensibilità politica su certe tipologie di comportamento, che non vengono più lette come reati tout court ma come contegni che comportino lesioni gravi – attuali o potenziali – all'ordine politico complessivo nazionale. È evidente che, in casi come questo, la scelta sulla qualificazione dei contegni in una o nell'atra categoria – per quello che qui ci interessa – importa l'applicabilità o meno delle norme della LED; se si riflette sul fatto che tale qualificazione spesso potrà avere riguardo a contegni *lato sensu* politici, in relazione ai quali la protezione dei dati è sempre stata considerata delicata e fondamentale, si vede bene come lo "scivolamento" di senso e di lettura può comportare conseguenze di notevolissima portata proprio nell'ambito del complesso bilanciamento fra sicurezza e garanzia dei diritti. Verosimilmente, questa linea di ambiguità che si può leggere nelle disposizioni appena citate (*rectius*: nella relativa interpretazione) potrebbe non essere estranea al problema di fondo di cui si è detto: cioè la necessità di lasciare agli Stati un certo margine di apprezzamento nella materia; margine di apprezzamento che potrebbe anche coinvolgere la qualificazione di un trattamento come rientrante nell'ambito della sicurezza nazionale piuttosto che nella pubblica sicurezza[24]. Vi sarebbe senz'altro una possibilità di controllo giudiziario su tale qualificazione, ma la colorazione anche politica che esse potrebbero avere, oltre alla *better position* che spesso la Corte europea dei diritti dell'uomo riconosce agli Stati nella valutazione delle proprie esigenze di sicurezza nazionale[25], potrebbero rendere tale controllo se non del tutto inefficace, probabilmente non così forte.

Sotto un profilo diverso, il perimetro della LED appare non del tutto chiaro già con riferimento alla nozione di "autorità competenti" (a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica). L'art. 3 ci fornisce una definizione molto ampia, ma che non appaga del tutto. In particolare, essa allude al fatto che dovrebbero rientrare fra le "autorità competenti" non solo le autorità propriamente pubbliche, ma anche soggetti privati cui siano attribuiti nell'ordinamento interno di alcuni Stati funzioni riconducibili a quelle oggetto della LED. Si tratta di una nozione difficile; è stato infatti osservato che, ad esempio, negli Stati membri non vi è una perfetta omogeneità organizzativa per lo svolgimento di talune attività astrattamente riconducibili

[23] Cfr. sul punto, J. SAJFERT, T. QUINTEL, *Data Protectin Directive (EU) 2016/680 for Police and Criminal Justice cooperation*, in M. COLE, F. BOEHM (eds.), *Commentary on the General Data Protection Regulation*, Chelthenam, 2019.

[24] Ci si potrebbe peraltro chiedere se, in tali casi (attività concernenti la sicurezza nazionale) non troverebbe comunque applicazione il GDPR, come sembra potersi desumere dal *considerando* n. 12 della LED, secondo cui "*gli Stati membri possono conferire alle autorità competenti altri compiti che non siano necessariamente svolti a fini di prevenzione, indagine, accertamento o perseguimento di reati, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, cosicché il trattamento di dati personali per tali altre finalità, nella misura in cui ricada nell'ambito di applicazione del diritto dell'Unione, rientra nell'ambito di applicazione del regolamento (UE) 2016/679*". Sarebbe però abbastanza curioso, se non del tutto inverosimile, che i trattamenti concernenti la "sicurezza nazionale" – sottratti anche alla più soft disciplina della LED – si trovassero nell'ambito di applicazione complessivamente più rigido del GDPR.

[25] Su tali aspetti, volendo, F. DONATI, P. MILAZZO, *La dottrina del margine di apprezzamento nella giurisprudenza della Corte europea dei diritti dell'uomo*, in P. FALZEA, A. SPADARO, L. VENTURA (a cura di), *La Corte costituzionale e le Corti d'Europa. Atti del Seminario svoltosi a Copanello (CZ) il 31 maggio-1° giugno 2002*, Torino, 2003, pp. 65-117.

a quelle oggetto della LED: è il caso, ad esempio, dei soggetti che sono incaricati di accertare violazioni di carattere finanziario, che a seconda dei diversi ordinamenti possono essere soggetti pubblici o non pubblici. Evidentemente questa ambiguità di risolve anche in una correlativa incertezza sui rispettivi confini fra applicazione della LED ed applicazione (residuale) del GPDR, nonché in un potenziale *vulnus* sulla effettiva portata armonizzante della LED. D'altra parte, se si può convenire che la nozione di "autorità competenti" sia stata espansa in maniera notevole (erodendo quindi spazio all'applicazione del GDPR rispetto alla LED), appare più difficilmente sostenibile che in tale nozione possano certamente entrare anche le compagnie private di sorveglianza – come è stato sostenuto[26] – a meno che esse non siano destinatarie di poteri tipicamente pubblici. Questo ultimo aspetto – quella della possibile "disarmonia" delle legislazioni nazionali nella applicazione della LED – appare anche potenzialmente rafforzato da quanto disposto dall'art. 1 par. 3 della stessa LED, laddove prevede che la direttiva non pregiudica la facoltà degli Stati membri di prevedere garanzie più elevate di quelle in essa stabilite per la tutela dei diritti e delle libertà dell'interessato con riguardo al trattamento dei dati personali da parte delle autorità competenti. Si tratta di una sorta di clausola di "maggior tutela" che senz'altro è compatibile con lo schema della direttiva che si è scelto di adottare e merita di essere valutato positivamente nella prospettiva del rafforzamento (o quantomeno della conservazione) del livello di tutela del diritti degli interessati, ma che si presta al tempo stesso a costituire una sorta di incognita – potenzialmente anche molto "ingombrante" – se ci si rivolge all'angolo visuale del potenziamento della circolazione dei dati "di polizia" che, come abbiamo accennato, è sempre stato e continua ad essere l'aspetto centrale della cooperazione europea in questo settore. Anche in questo caso, quindi, l'individuazione esatta del perimetro di applicazione della LED non potrà che essere tracciata solo nella misura in cui gli Stati in sede di attuazione non riterranno di preservare le proprie specificità nazionali eventualmente più garantiste.

4. I complessi rapporti fra LED e GDPR

La LED è stata elaborata nel medesimo torno di tempo in cui è stato elaborato il GDPR, ed effettivamente una lettura parallela dei due testi lascia intendere come essi siano animati da una medesima – o comunque tutt'altro che dissimile – impostazione culturale e giuridica di fondo. Ovviamente, la LED presenta alcune significative differenze rispetto al GDPR, a conferma della citata "specificità" del settore, evocata anche dalla Dichiarazione n. 21 allegata al Trattato di Lisbona.

Sintetizzando molto, credo sia interessante sottolineare i seguenti aspetti, seguendo il *fil rouge* che ci siamo riproposti fin dall'inizio, cioè quello di valutare se ed in che misura la LED risponda alle esigenze di equilibrio e di bilanciamento fra la spinta alla circolazione dei dati "di polizia" e la protezione dei dati personali, o se invece la LED comporti un indebolimento della tutela dei diritti degli interessati in favore del versante "securitario" del dilemma:

(i) *il principio del consenso al trattamento*. La LED rimuove dai principi della materia – diversamente da GDPR che invece ne fa un caposaldo del suo sistema di tutela – il principio del consenso al trattamento. Secondo il considerando n. 35 della LED, infatti, l'adempimento dei compiti di prevenzione, indagine, accertamento e perseguimento di reati, affidato istituzionalmente per legge alle autorità competenti,

[26] M.M. CARUANA, *The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement*, in *International Review of Law, Computers & Technology*, n. 3, 2019, pp. 249-270.

consente a queste ultime di richiedere od ordinare alle persone fisiche di dare seguito alle richieste formulate (dalle stesse autorità); in tali casi il consenso dell'interessato non dovrebbe costituire la base giuridica per il trattamento di dati personali da parte delle autorità competenti in quanto – essendo tenuto ad adempiere un obbligo legale – l'interessato non è in grado di operare una scelta autenticamente libera, pertanto la sua reazione non potrebbe essere considerata una manifestazione di volontà libera. D'altra parte, però, lo stesso considerando consente ai singoli Stati di prevedere forme di consenso dell'interessato quando il trattamento abbia ad oggetto, ad esempio, il "*test del DNA nell'ambito di indagini penali o per il monitoraggio della sua ubicazione mediante dispositivo elettronico per l'esecuzione di sanzioni penali*". In altre parole, la LED indica una situazione tipo, nella quale normalmente il consenso dell'interessato non è necessario per il trattamento (altrimenti si presume che l'interessato non darebbe mai il consenso, dato che il trattamento è finalizzato ad attività potenzialmente negative per la sua sfera personale

(ii) *la limitazione dei diritti dell'interessato*. La LED consente la limitazione dei diritti di informazione, accesso, rettifica e cancellazione dei dati personali per motivi specifici relativi al settore dell'attività "di polizia": non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari; non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali; proteggere la sicurezza pubblica; proteggere la sicurezza nazionale; proteggere i diritti e le libertà altrui. La LED peraltro sottolinea come una così potenzialmente massiccia limitabilità dei più tipici diritto dell'interessato ad un trattamento debba essere sottoposta al test – ben noto nella giurisprudenza della Corte europea dei diritti dell'uomo – della "*necessarietà in una società democratica*". Sotto questo profilo, quindi, avranno necessariamente ingresso nella valutazione delle misure statali di limitazione dei diritti della LED le linee interpretative elaborate dalla Corte europea dei diritti dell'uomo e dalla Corte di Giustizia in ordine alla compatibilità con una società democratica. Come è noto, sono innumerevoli i casi in cui le due Corti hanno dovuto utilizzare questo parametro, e spesso ciò è avvenuto anche proprio in materia di trattamento dei dati e diritti degli interessati. In più occasioni le Corti – pur cercando di riconoscere un certo margine di apprezzamento agli Stati – hanno saputo segnare un confine fra ciò che è consentito agli Stati e ciò che viola di volta in volta la Convezione, la Carta dei Diritti, o che in questo caso violerebbe la stessa LED[27].

(iii) disciplina dei dati sensibili. La disciplina dei dati sensibili[28] costituisce uno dei passaggi più importanti di qualsiasi normativa ti protezione dei dati, proprio perché si tratta di attribuire un livello particolarmente alto di tutela in relazione a dati a loro volta particolarmente qualificati e degni della massima garanzia rispetto al trattamento ed all'uso. Sul punto, la LED non prevede uno schema analogo a quello dell'art. 9 del GDPR

[27] A. BONFANTI, *Big data e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali*, in *Media Laws - Rivista di diritto dei media*, n. 3, 2018, pp. 1-13 cita ad esempio la sentenza della Corte di Giustizia dell'8 aprile 2014, causa C-293/12, *Digital Rights Ireland Ltd. c. Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a.*, nella quale la Corte ha individuato una ingerenza di vasta portata e particolarmente grave nei diritti consacrati dalla Carta dei diritti fondamentali dell'Unione europea (art. 7 e art. 8) derivante dal regime di conservazione dei dati degli utenti imposto ai *service providers*, con possibilità di accesso da parte della autorità nazionali (ancorché nell'ambito del perseguimento di un obiettivo astrattamente legittimo come quello di contribuire alla lotta contro la criminalità grave).

[28] Secondo la definizione dell'art. 10 della LED, si tratta dei dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica o i dati relativi alla salute o di dati relativi alla vita sessuale della persona fisica o all'orientamento sessuale.

(divieto generale; individuazione di una serie di ipotesi derogatorie), ma prevede direttamente le ipotesi di praticabilità del trattamento dei dati sensibili. Tali ipotesi sono ovviamente assai meno numerose rispetto a quelle indicate dal GDPR. Tale tipo di trattamento, infatti, è autorizzato solo se strettamente necessario, soggetto a garanzie adeguate per i diritti e le libertà dell'interessato e soltanto: a) se autorizzato dal diritto dell'Unione o dello Stato membro; b) per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica; o c) se il suddetto trattamento riguarda dati resi manifestamente pubblici dall'interessato.

(iv) il trasferimento dei dati. Altro momento molto significativo è quello della disciplina della trasmissione dei dati "di polizia" a soggetti terzi rispetto allo Stato che li ha raccolti. Sul punto, ed in estrema sintesi, la LED prevede un sistema a "cascata a tre livelli". Esso dovrebbe essere articolato in prima battuta su "decisioni di adeguatezza"[29], in assenza delle quali subentrerebbe la possibilità di operare sulla base di "garanzie adeguate" contenute in uno strumento giuridicamente vincolante, o sulla base di un *self-assessment*; infine, in carenza anche di queste condizioni, la LED contempla anche alcune ipotesi di deroga (non sempre di facile interpretazione). Prescindendo dai complessi profili di questa regolamentazione, credo sia opportuno notare come essa si basi in primo luogo sulle decisioni di adeguatezza, cui le altre ipotesi sono poste a mo' di corollari. Ma di fatto le decisioni di adeguatezza sostanzialmente non sono state adottate, e quindi si è costretti ad operare secondo le altre alternative. Le quali – come è stato condivisibilmente osservato[30] – non forniscono il medesimo livello di tutela dei diritti che invece potrebbe essere raggiunto sulla base di una decisione di adeguatezza. Il blocco dell'adozione delle decisioni di adeguatezza – forse anche indotto dalla reazione alla severa giurisprudenza *Schrems* I e II della Corte di Giustizia – di fatto ha incanalato il meccanismo di circolazione esterna dei dati personali "di polizia" in strade meno garantiste e senz'altro più opache di quella prevista come normale dalla LED.

5. Strumenti digitali e dati "di polizia": la decisione puramente automatica

La LED – meritevolmente – prende atto dell'esistenza di strumenti tecnologici a contenuto digitale che impongono un serio ripensamento complessivo e generale dello stesso trattamento dei dati. Essi, infatti, consentono attività articolate e complesse come il *data mining*, il *data matching*, la *prediction analyis*, le quali pongono il tema del trattamento dei dati in una prospettiva completamente nuova, del tutto estranea rispetto ai profili classici della tutela e della protezione. In questo contesto la LED si pone soprattutto il problema della decisione basata esclusivamente su trattamenti automatici (compresa la profilazione), prevedendo un generale divieto qualora tale decisione

[29] Sulle decisioni di adeguatezza è intervenuta la giurisprudenza della Corte di Giustizia, sentenza 6 ottobre 2015, Causa C-362/14, *Schrems c. Data Protection Commissioner*, per la quale "*è vero che il termine «adeguato» […] implica che non possa esigersi che un paese terzo assicuri un livello di protezione identico a quello garantito nell'ordinamento giuridico dell'Unione. Tuttavia, […] l'espressione «livello di protezione adeguato» deve essere intesa nel senso che esige che tale paese assicuri effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione delle libertà e dei diritti fondamentali sostanzialmente equivalente a quello garantito all'interno dell'Unione*".

[30] L. DRECHSLER, *Wanted: LED Adequacy Decisions. How the Absencce of Any Adequacy Decision is Hurting the Protection of Fundamental Rights in a Law Enforcement Context*, in *International Data Privacy Law*, 2021, pp. 1-14.

produca effetti giuridici negativi (*adverse legal effect*)[31] o incida significativamente sull'interessato. Il divieto può essere derogato se la decisione automatizzata sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che preveda garanzie adeguate (*appropriate safeguards*) per i diritti e le libertà dell'interessato, fra cui "*almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento*". La disposizione ha il merito indubbio di porre il problema della risposta ai mezzi di profilazione e di trattamento dei dati completamente automatizzati e che incidono negativamente sulla situazione soggettiva dell'interessato. Un limite significativo può essere forse però rilevato nella circostanza per cui la LED (così come il GDPR) fanno riferimento ad effetti giuridici negativi di carattere individuale, mentre non si fa cenno ai possibili interessi "di gruppo" alla protezione di dati relativi al gruppo stesso. Le tecnologie di gestione dei cd. *big data* si prestano in modo notevole ad una gestione aggregata dei dati tale da generare decisioni che possono avere effetti negativi non tanto nei confronti di individui singoli, ma proprio nei confronti di insiemi di individui appositamente profilati. In questo contesto, e vista la portata analogamente discriminatoria, ci si potrebbe chiedere se non sarebbe necessario o quantomeno opportuno strutturare la protezione garantita dalla LED anche in favore dei gruppi, e non solo degli individui.

Nel quadro delle decisioni completamente automatizzate con effetti negativi, la LED ne consente l'adozione quando vi sia il contrappeso di *appropriate safeguards*, fra le quali il considerando n. 38 include "*il rilascio di specifiche informazioni all'interessato e il diritto di ottenere l'intervento umano, in particolare di esprimere la propria opinione, di ottenere una spiegazione della decisione raggiunta dopo tale valutazione e di impugnare la decisione*". Come si vede, l'elemento assai valorizzato dalla LED in questo contesto è il diritto all'intervento umano: nel ciclo automatizzato della decisione si pretende l'inserimento di un elemento umano, del quale peraltro non viene chiaramente precisata la natura né la portata. Come evidenziato in dottrina, un intervento umano purchessia, collocato in una qualsiasi fase del processo automatizzato, senza una particolare considerazione per la sua funzione, le sue modalità e le sue conseguenze, può avere una efficacia davvero modesta nell'ottica della tutela dei diritti dei soggetti sottoposti al trattamento.

Ancora una volta, la LED ha dunque lasciato un margine di apprezzamento invero assai significativo agli Stati pure in questo ambito così evolutivo e così importante per gli orizzonti di sviluppo delle tecniche di indagine e di polizia. Il limite che la LED ha comunque posto è quello relativo ai dati sensibili: la decisione completamente automatizzata non può infatti essere basata su dati sensibili "*a meno che non siano in vigore misure adeguate a salvaguardia dei diritti, delle libertà e dei legittimi interessi dell'interessato*"[32], e la profilazione che porta alla discriminazione di persone fisiche sulla base di tali dati è vietata.

[31] Sul punto emerge una differenza fra l'art. 11 della LED e l'art. 22 del GDPR. Nel primo caso, infatti, la direttiva richiede la sussistenza "*adverse legal effects*" per confermare il generalizzato divieto di decisioni automatizzate, mentre per il GDPR è sufficiente che tale misura dia luogo ad un effetto (non necessariamente negativo).

[32] Il considerando n. 37 della LED inserisce fra le possibili misure "*la possibilità di raccogliere tali dati unicamente in connessione con altri dati relativi alla persona fisica interessata, la possibilità di provvedere adeguatamente alla sicurezza dei dati raccolti, norme più severe riguardo all'accesso ai dati da parte del personale dell'autorità competente e il divieto di trasmissione di tali dati*".

6. Conclusioni

Alla luce di questo breve excursus su alcuni profili problematici della LED, può trarsi qualche conclusione nell'ottica interpretativa proposta. Innanzitutto, può dirsi che la LED costituisce senza dubbio una novità di portata molto significativa, un benchmark per l'allineamento delle regole europee di protezione dei dati nelle attività di polizia: essa ha innescato infatti – oltre che i processi di adeguamento statali necessari – anche un processo di ripensamento dei "microcosmi" di sistemi di tutela dei dati personali esistenti, in una prospettiva effettivamente uniformante (non solo in senso verticale, quindi, ma anche orizzontale, all'interno cioè dello stesso diritto dell'Unione). Si tratta poi di una normativa che risente sicuramente di una esigenza di garanzia di una forte protezione dei diritti e di un livello di tutela dei dati personali molto alto.

Un altro aspetto significativo della LED è la presa d'atto che la protezione della riservatezza e dei dati personali nell'ambito delle attività di polizia non si gioca più soltanto su strumenti classici e tradizionali (schedari, archivi, ecc.) ma si giocherà sempre di più mediante strumenti digitali sui quali possono essere svolte attività ampiamente (o anche completamente) automatizzate, che costituiscono una vera sfida contemporanea al contenuto stesso ed alle modalità di espressione dei diritti connessi alla riservatezza.

In questo quadro complessivamente positivo, si è cercato di indicare come esistano comunque taluni aspetti di perplessità, che concernono ad esempio (i) la stessa scelta dello strumento della direttiva, (ii) la rinuncia a fare della LED immediatamente l'unico strumento di protezione dei dati personali in attività di polizia (consentendo la sopravvivenza, almeno in questa fase, di molti altri sottosistemi), (iii) i complessi confini fra GDPR e LED, la cui difficile determinazione è data anche da alcune scelte normative forse insufficientemente definite della LED e che costringerà senz'altro a una qualche delicata *actio finium regundorum* fra i due sistemi di protezione, (iv) il sistema di trasmissione dei dati a terzi imperniato su un modello centrale – la decisione di adeguatezza – la cui adozione sembra però attualmente assai difficile.

Sembra di poter dire che tutte queste problematiche di carattere interpretativo derivino sempre dalla medesima duplice origine: da un lato la necessità - attinente alla materia – di effettuare un bilanciamento fra valori degni che selezioni un punto di equilibrio diverso rispetto a quello valevole generalmente, e che sia ovviamente meno squilibrato in favore del soggetto del trattamento, riconoscendo strumenti limiti meno rigidi per l'attività di polizia; dall'altro lato, la percepibile e persistente esigenza degli Stati di non spogliarsi completamente del proprio margine decisionale in un contesto che viene ancora ricostruito come strettamente legato alla sovranità nazionale ed ai poteri più intimi e connessi alla natura stessa dello Stato.

Da qui derivano, credo, molte delle tematiche che si sono rapidamente passate in rassegna: dall'operare congiunto di forze uniformanti ed esigenze di garanzia di scelte autonome degli Stati. In questo contesto, l'attuazione che gli Stati hanno dato e stanno dando della LED è decisiva, perché – stante il margine di manovra non piccolo che la LED riconosce loro – solo in quella sede sarà finalmente possibile valutare in concreto quanto avanzato sia il punto di bilanciamento e di equilibrio fra attività di polizia e protezione dei dati nel contesto europeo.

ABSTRACT

La Direttiva (EU) 2016/680 ha l'obiettivo di costituire una base normativa stabile per la protezione dei dati personali nell'ambito delle attività di polizia, in un contesto un cui si

è invece assistito in passato alla proliferazione delle banche dati, dei modelli e degli strumenti di tutela. La Direttiva – elaborata congiuntamente al Regolamento (EU) 2016/679 – garantisce certamente un alto livello di protezione ed ha molti aspetti positivi ed anche innovativi: in particolare il rilievo dato alle forme nuove di trattamento digitale ed informatizzato dei dati. Ciò non di meno, essa presenta taluni aspetti strutturali e contenutistici che pongono significativi interrogativi sulla effettiva capacità della stessa Direttiva di porsi come strumento principale nel contesto di riferimento, e sull'effettivo punto di equilibrio che essa determina nel bilanciamento fra protezione del diritto ed attività di polizia.

KEYWORDS
Banche Dati, Bilanciamento, Cooperazione di Polizia, Lotta alla Criminalità, Polizia, Profilazione, Protezione Dei Dati Personali, Riservatezza.

PROLIFERATION OF POLICE DATABASES AND PROTECTION OF PERSONAL DATA: SOME PERSPECTIVES AND LIMITS OF DIRECTIVE (EU) 2016/680

ABSTRACT
Directive (EU) 2016/680 aims to establish a steady legal basis for the protection of personal data in the context of police activities where, conversely, in the past we have witnessed a proliferation of databases, models and protection tools. This Directive – drafted jointly with Regulation (EU) 2016/679 – certainly guarantees a high level of protection, featuring many positive, just as innovative, aspects: in particular, the emphasis given to new forms of digital and electronic data processing. Nonetheless, it presents some structural and content aspects that raise significant questions on the effective capacity of the Directive itself to act as the main instrument in the reference context, and on and on its effective capacity to determine a point of balance between protection of the law and police activities

KEYWORDS
Balance, Confidentiality, Data Protection, Databases, Fight Against Crime, Police, Police Cooperation, Profiling.