ISSN 2384-9169
Fascicolo n. 4 - 2022
rivista.eurojus.it

L'influenza del diritto dell'Unione europea sulla sicurezza nazionale: l'art. 4, par. 2, TUE alla prova della recente giurisprudenza UE tra l'altro in materia di *privacy*

DI SERENA CRESPI*

Sommario: 1. La crescente attenzione della giurisprudenza UE anche in materia di *privacy* per situazioni attinenti alla sicurezza nazionale. – 2. La sicurezza nazionale nel Sistema UE e CEDU: diritto fondamentale od obiettivo d'interesse generale? – 3. L'applicabilità del diritto UE (anche in materia di dati personali) nell'ambito della sicurezza nazionale: l'art. 4, par. 2, TUE. – 4. L'influenza del diritto UE anche in materia di dati personali su misure di diritto interno adottate per motivi di sicurezza nazionale: tra questioni interne al sistema comune …. – 5. *Segue*: … e questioni disciplinate dal diritto interno e CEDU. – 6. L'influenza esercitata dal diritto UE anche in materia di dati personali su questioni attinenti alla sicurezza nazionale tra Stati membri e Paesi terzi. – 7. Il tipo di controllo esercitato dal diritto UE anche in materia di dati personali su misure di diritto interno rientranti nell'ambito d'applicazione dell'art. 4, par. 2, TUE. – 8. Conclusioni.

1. La crescente attenzione della giurisprudenza UE anche in materia di privacy per situazioni attinenti alla sicurezza nazionale.

L'analisi della giurisprudenza della Corte di giustizia dell'Unione europea che dal dicembre 2009 ad oggi – ossia dall'attribuzione di efficacia vincolante alla Carta dei diritti fondamentali dell'Unione europea[1] – è stata chiamata a bilanciare il diritto alla protezione dei dati personali di cui all'art. 8 di quest'ultima con altri diritti o interessi essenziali, nazionali ed europei, alla ricerca di un punto di equilibrio tra gli stessi, evidenzia la progressiva e crescente importanza delle questioni legate all'interferenza tra *privacy* e sicurezza nazionale. Negli ultimi

[1] In dottrina, per tutti, A. TIZZANO, *L'application de la Charte des droits fondamentaux dans les États membres à la lumière de son article 51, paragraphe 1*, in *Diritto dell'Unione europea*, 2014, p. 429 ss.; B. NASCIMBENE, *Carta dei diritti fondamentali, applicabilità e rapporti fra giudici: la necessità di una tutela integrata*, in *europeanpapers.eu*, vol. 6, n. 1, 2021, p. 81 ss.

soli sette anni (2015-2022), il giudice di Lussemburgo è stato, infatti, investito in ben sei occasioni del delicato compito di valutare l'aspetto – invero piuttosto di dettaglio – della compatibilità con il predetto diritto fondamentale di legislazioni nazionali (quelle britannica, francese e belga[2] nelle cause *Privacy International*, *La Quadrature du Net, French Data Network* e *Ordre des barreaux francophones et germanophone* del 2020[3]) o di atti comuni (le decisioni di adeguatezza UE/USA *Safe Harbour* e *Privacy Shield*[4] in *Schrems I* del 2015[5] e

[2] Quanto alla Francia (C-511/18 e C-512/18), *décrets 2015-1185 del 28 settembre 2015 portant désignation des services spécialisés de renseignement* (*JORF* del 29 settembre 2015) ; 2015-1211 del 1 ottobre 2015 *relatif au contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État* (*JORF* del 2 ottobre 2015) ; 2015-1639 del 11 dicembre 2015 *relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure* (*JORF* del 12 dicembre 2015) ; 2016-67 del 29 gennaio 2016 *relatif aux techniques de recueil de renseignement* (*JORF* du 31 gennaio 2016) ; nonché l'art. R. 10-13 *Code des postes et des communications électroniques* e il *décret* 2011-219 del 25 febbraio 2011 *relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne* (*JORF* del 1 marzo 2011). Con riferimento al Belgio (C-520/18), legge del 29 maggio 2016 *relative à la collecte et à la conservation des données dans le secteur des communications électroniques* (*Moniteur belge* del 18 luglio 2016, p. 44717). Quanto al Regno Unito (C-623/17), *Art. 94 del Telecommunications Act* del 1984 e gli artt. 21, par. 4, 6, 65-69 del *Regulation of Investigatory Powers Act* del 2000.

[3] Corte giust., 6 ottobre 2020, causa C-511/18, C-512/18, C-520/18, *La Quadrature du Net, French Data Network e Ordre des barreaux francophones et germanophone*, ECLI:EU:C:2020:791 (di seguito anche nel testo : *La Quadrature du Net*); Corte giust., 6 ottobre 2020, causa C-623/17, *Privacy International*, ECLI:EU:C:2020:790. In dottrina, I. CAMERON, *Metadata retention and national security : Privacy International and La Quadrature du Net : Case C-623/17*, in *Common Market Law Review*, 2021 p. 1433 ss. ; S. J. ESKENS, *The ever-growing complexity of the data retention discussion in the EU : an in-depth review of La Quadrature du Net and others and Privacy International : joined cases C-511/18, C-512/18 and C-520/18 La Quadrature du Net and others [2020], case C-623/17 Privacy International*, in *European Data Protection Law Review*, 2022, vol. 8, nº 1, p. 143 ss.; M. TZANOU, S. KARYDA, *Privacy International and Quadrature du Net : one step forward two steps back in the data retention saga? : case C-623/17 Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others, joined cases C-511/18, C-512/18 and C-520/18 La Quadrature du Net and Others v. Premier Minister and Others*, in *European Public Law*, 2022, n° 1, p. 123 ss.; M. ZALNIERIUTE, *A Struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of European Union*, in *The Modern Law Review*, 2022, n° 1, p. 198 ss.

[4] Sulle decisioni di adeguatezza *Safe Harbour* e *Privacy Shield*, C. KUNER, *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, in *German Law Journal*, 2017, p. 881 ss.; G. VERMEULEN, *Eyes Wide Shut*: *The Privacy Shield's blunt denial of continued bulk, mass or indiscriminate collection or processing and unnecessary or disproportionate access and use by US intelligence and law enforcement authorities*, in G. VERMEULEN, E. LIEVENS (ed.), *Data protection and privacy under pressure. Transatlantic tensions, EU surveillance and Big Data, Antwerp*, 2017, p. 45 ss. A seguito dei negoziati condotti dalla Commissione europea e l'amministrazione USA nel 2021 e dell'accordo di principio raggiunto a marzo 2022 tra queste ultime, la Commissione europea, anche sulla base dell'*Executive Order* USA di ottobre 2022, sta redigendo la proposta di una nuova decisione di adeguatezza (https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045), che sostituirà il *Privacy Shield* dichiarato nullo da Corte giust., 16 luglio 2020, causa C-311/18, *Data Protection Commissioner c. Facebook Ireland Limited e Maximillian Schrems* (c. d. *Schrems II*), ECLI:EU:C:2020:559. Per l'analisi di quest'ultima pronuncia, F. D'ATH, *Arrêt «* Schrems II *» : sur la légalité des transferts de données personnelles fondés sur une décision d'adéquation ou moyennant des garanties appropriées*, in *Journal de droit européen*, 2020, nº 10, p. 442 ss. ; E. FLETT, J. WILSON, J. CLOVER, *Schrems strikes again: EU-US privacy shield suffers same fate as its predecessor*, in *Computer and Telecommunications Law Review*, 2020, p. 161 ss.; M. NINO, *La sentenza Schrems II della Corte di giustizia UE: trasmissione dei dati personali dall'Unione europea agli Stati terzi e tutela dei diritti dell'uomo*, in *Diritti umani e diritto internazionale*, 2020, p. 733 ss.; M. ROTENBERG, Schrems II, *from Snowden to China: toward a new alignment on transatlanticdata protection*, in *European Law Journal*, 2020, p. 141 ss.; C. SELLARS, Schrems II *and Standard Contractual Clauses – the Advocate-General's Opinion*, in *Computer Law Review International*, 2020, p. 29 ss.

[5] Corte giust., 6 ottobre 2015, causa C-362/14, *Maximillian Schrems c. Data Protection Commissioner* (c.d. *Schrems I*), ECLI:EU:C:2015:650. In dottrina, A. DEBET, *L'invalidation du* Safe Harbor *par la CJUE: tempête sur les transferts de données vers les États-Unis*, *La Semaine Juridique – éd. gén.* 2015, nº 46-47, p. 2108 ss.; G.

Schrems II del 2020[6]) che autorizzavano, in vario modo e misura, le autorità di *intelligence* rispettivamente di Stati membri o di paesi terzi all'accesso e al successivo trattamento, per motivi di sicurezza nazionale, di dati raccolti inizialmente in Internet da operatori commerciali (fornitori di servizi di comunicazione anche elettronica). Tale dato è ancora più rilevante considerato che in ulteriori sette casi risolti negli ultimi otto anni – *Digital Rights Ireland* del 2014[7], *Tele2 Severige* del 2016[8], *Accordo PNR tra Canada e Unione europea* del 2017[9], *Ministerio Fiscal* del 2018[10], *G.D.*, *SpaceNet*, *VD e SR* del 2022[11] – la Corte di giustizia ha affrontato la questione, diversa ma invero contigua, di un simile accesso e uso dei dati da parte di autorità pubbliche nell'ambito questa volta di mansioni di contrasto alla criminalità. Pur se questi ultimi casi si riferiscono ad attività differenti da quella di protezione della sicurezza nazionale e relativamente ad autorità pubbliche diverse dai servizi di *intelligence*, essi hanno richiesto parimenti di bilanciare il diritto di cui all'art. 8 della Carta con esigenze securitarie, sollevando così analoghe questioni attinenti ai limiti e alle condizioni dell'accesso da parte di autorità pubbliche ai dati raccolti in Internet per ragioni commerciali. E ciò ancora una volta al

---

FINOCCHIARO, *La giurisprudenza della Corte di Giustizia in materia di dati personali da* Google Spain *a* Schrems, in *Il diritto dell'informazione e dell'informatica*, 2015, p. 779 ss. L. COLONNA, Schrems vs. Commissioner*: A Precedent for the CJEU to Intervene in the National Intelligence Surveillance Activities of Member States?*, in *Europarättslig tidskrift*, 2016, nº 2, p. 208 ss.; R. A. EPSTEIN, *The ECJ's Fanal Imbalance: Its cavalier treatment of national security issues poses serious risk to public safety and sound commercial practices*, in *European Constitutional Law Review*, 2016, Vol. 12, p. 330 ss.

[6] Corte giust., *Schrems II* cit.

[7] Corte giust., 8 aprile 2014, causa C-293/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238. In dottrina, M. COLE, F. BOEHM, *EU Data Retention – Finally abolished? Eight years in light of Article 8*, in *Critical Quarterly for Legislation and Law*, 2014, p. 58 ss.; D. LYNSKEY, *The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety:* Digital Rights Ireland, in *Common Market Law Review*, 2014, p. 1789 ss.; O. POLLICINO, *Diritto all'oblio e conservazione di dati. La Corte di giustizia a piedi uniti: verso un digital right to privacy*, in *Giurisprudenza costituzionale*, 2014, p. 2949 ss.; S. CRESPI, *Il trasferimento dei dati personali UE in Stati terzi: dall'Approdo sicuro allo Scudo UE/USA per la privacy*, in *Diritto Pubblico Comparato ed Europeo*, 2017, p. 687 ss.

[8] Corte giust., 21 dicembre 2016, causa C-203/15, *Tele2 Sverige*, ECLI:EU:C:2016:970. Per un commento, I. CAMERON, *Balancing data protection and law enforcement needs: Tele2 Sverige and Watson*, in *Common Market Law Review*, 2017, p. 1467 ss.; O. POLLICINO, M. BASSINI, *La Corte di Giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in *Diritto Penale Contemporaneo*, 9 gennaio 2017, https://archiviodpc.dirittopenaleuomo.org/upload/POLLICINOBASSINI_2017a.pdf; X. TRACOL, *The judgement of the Grand Chamber dated 21 December 2016 in the two joint Tele2Sverige and Watson cases: the need for a harmonised legal framework on the retention of data at EU level*, in *Computer Law & Security Review*, 2017, p. 1 ss.

[9] Corte giust., parere 1/15 *Canada/UE* del 27 luglio 2017, pubblicato nella Raccolta digitale della Corte di giustizia dell'Unione europea. In dottrina, N. LE BONNIEC, *L'avis 1/15 de la CJUE relatif à l'accord PNR entre le Canada et l'Union européenne : une délicate conciliation entre sécurité nationale et sécurité numérique*, in *Revue trimestrielle de droit européen*, 2018, n. 3, p. 617 ss. ; C. KUNER, *International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR*, in *Common Market Law Review*, 2018, p. 857 ss.; E. A. ROSSI, *Gli accordi PNR (Passenger Name Record) nella lotta al terrorismo internazionale. Conseguenze del parere n. 1/15 della Corte di giustizia del 26 luglio 2017 per la legittimità della direttiva n. 2016/681/UE*, in *Diritto comunitario e degli scambi internazionali*, 2018, p. 395 ss.

[10] Corte giust., 2 dicembre 2018, causa C-207/16, *Ministerio Fiscal*, ECLI:EU:C:2018:788. Per un'analisi della pronuncia, C. DOCKSEY, *Ministerio Fiscal: holding the line on ePrivacy*, in *Maastricht Journal of European and Comparative Law*, 2019, p. 585 ss.; X. TRACOL, *Ministerio Fiscal: access of public authorities to personal data retained by providers of electronic communications services*, in *European Data protection Law Review*, 2019, p. 127 ss.

[11] Corte giust., 20 settembre 2022, cause riunite C-793/ e 794/19, *SpaceNet*, ECLI:EU:C:2022:702; 20 settembre 2022, cause riunite C-339 e 397/20, *VD e SR*, ECLI:EU:C:2022:703; 5 aprile 2022, causa C-140/20, *G.D.*, ECLI:EU:C:2022:258.

fine di trovare un punto di equilibrio tra diritti fondamentali (*privacy*) ed esigenze securitarie (lotta alla criminalità) tra loro in conflitto.

La crescente importanza attribuita, soprattutto nell'ultimo decennio, al tema in esame invero non sorprende. L'efficacia dell'attività di mantenimento della sicurezza interna – ma invero anche il contrasto del terrorismo e della criminalità – dipende, infatti, ormai in larga misura dall'uso da parte delle autorità di *intelligence* delle moderne tecniche d'indagine, che implicano proprio l'accesso ai dati personali raccolti tramite l'impiego di Internet o di altri strumenti della società di comunicazione per lo più per ragioni commerciali. Tuttavia, l'accesso a tali dati, soprattutto se effettuato con metodi di raccolta di massa, da parte di tali autorità può quantomeno comprimere il diritto fondamentale di cui all'art. 8 della Carta. Peraltro, mentre in passato i servizi di *intelligence* acquisivano per lo più informazioni con autonomi mezzi di intercettazione, la ormai consueta raccolta di dati per ragioni commerciali permette a questi ultimi di attingere a una quantità di informazioni superiore rispetto al passato rivolgendosi ai fornitori di servizi di comunicazione anche elettronica che hanno raccolto dati nell'ambito delle loro operazioni economiche. In tale occasione, l'accesso ai dati da parte delle autorità di sorveglianza può inoltre avvenire sia in forma mediata, ossia richiedendone l'acquisizione alle imprese o alle autorità pubbliche che li abbiano raccolti per ragioni estranee alla sicurezza dello Stato, i quali sono poi spesso obbligati a mettere tali dati nella disponibilità dei predetti servizi, sia invece in forma diretta, ossia impiegando autonomi mezzi di intercettazione per acquisire le informazioni conservate nelle banche dati dei predetti operatori. In quest'ultimo caso, l'acquisizione di dati da parte delle autorità di *intelligence* avviene dunque senza il coinvolgimento di questi ultimi e spesso senza che loro ne siano neppure informati. Gli sviluppi tecnologici dell'era digitale e i moderni strumenti di comunicazione e intercettazione che ne sono derivati hanno, in altri termini, accresciuto la capacità di raccolta di dati su larga scala, ai quali i servizi di sorveglianza possono accedere, rendendo così più alta la potenziale interferenza tra attività volte a tutelare la sicurezza nazionale e quelle invece inerenti alla salvaguardia di diritti fondamentali, quale per l'appunto quello della *privacy*.

In tale contesto, l'esigenza, ormai sempre più marcata, di circoscrivere il perimetro entro cui i servizi di *intelligence* possono avere accesso ai dati personali – e quindi di autorizzarlo ma entro confini prestabiliti – che è sottesa alla copiosa giurisprudenza UE degli ultimi dieci anni – ma invero anche di quella nazionale[12] e CEDU[13] – è allora la risposta di ogni sistema

[12] Quanto agli aspetti nazionali, in aggiunta alle controversie interne alla base dei rinvii pregiudiziali *La Quadrature du Net* e *Privacy International* già cit., v. la recente sentenza del *Bundesverfassungsgericht* del 26 aprile 2022, *BvR* 1619/17 ove la Corte Costituzionale Federale ha dichiarato alcune norme della legge bavarese sull'*intelligence* (*Bayerisches Verfassungschutzgesetz* - *BayVSG*) incompatibile con la Costituzione tedesca (*Grundgesetz – GC*) in quanto taluni poteri conferiti dalla prima ai servizi di sicurezza bavarese (*Landesamt fur Verfassungsschutz*) violavano i diritti fondamentali tedeschi della segretezza e dell'integrità delle comunicazioni elettroniche, della *privacy* delle telecomunicazioni e dell'inviolabilità dell'abitazione (artt. 1(1) e 2(1) GG; 10(1) GG; 13(1) GG).

[13] Come si avrà modo di vedere oltre nel testo del presente contributo, la Corte di Strasburgo ha avuto ripetutamente occasione di valutare la compatibilità di legislazioni dei paesi aderenti inerenti i poteri delle autorità di *intelligence* con il diritto alla tutela della vita privata (art. 8), il quale è interpretato dalla stessa, in modo estensivo, come comprensivo anche del diritto alla protezione dei dati personali. Al riguardo, v. in particolare le pronunce 25 maggio 2021, *Big Brother Watch and Others c. Regno Unito*, nn° 58170/13, 62322/14 e 24960/15; 25 maggio 2021, *Centrum för Rättvisa c. Svezia*, n° 35252/08; 12 gennaio 2016, *Szabó et Vissy c. Ungheria*, n° 37138/14; 4 dicembre 2015, *Roman Zakharov c. Russia*, n° 47143/06; 25 settembre 2013, *Serbia c. Youth Initiative for Human Rights*, n° 48135/06; 8 aprile 2013, *Romania c. Bucur and Toma*, n° 40238/02; 30 gennaio 2008, *Bulgaria c.*

giuridico, nazionale, comune ed internazionale, alla nuove sfide poste dall'uso sempre più diffuso della tecnologia per esigenze securitarie. In effetti, l'impiego per tali motivi di dati raccolti per ragioni commerciali, pur essendo ormai un pilastro ineludibile della lotta al terrorismo, alla criminalità e della protezione della sicurezza dello Stato, espone per sua stessa natura la vita privata di ogni individuo a nuovi e maggiori rischi.

2. La sicurezza nazionale nel sistema UE e CEDU: diritto fondamentale od obiettivo d'interesse generale?

L'elevato numero di controversie attinenti all'equilibrio giuridico tra tutela dei dati personali e salvaguardia della sicurezza dello Stato sollevate dinnanzi ai giudici dell'Unione europea nell'ultimo decennio è ancora più evidente se paragonato alle sole quattro sentenze, emesse dal medesimo organo giurisdizionale nello stesso lasso di tempo, riguardanti il bilanciamento del diritto alla tutela dei dati con altri diritti dell'Unione europea come, ad esempio, la libertà d'espressione[14]. E ciò sebbene le predette esigenze securitarie (lotta alla criminalità e salvaguardia della sicurezza nazionale) non siano neppure qualificabili, diversamente dalla libertà d'espressione, come un diritto fondamentale anche UE[15]. In effetti, pur sempre ribadendo la Corte di giustizia l'importanza di garantire la sicurezza all'interno dell'Unione europea, da oltre un decennio la giurisprudenza comune ha ripetutamente affermato che la lotta al terrorismo internazionale[16] e alla criminalità per garantire la sicurezza pubblica[17] o quella nazionale[18] sono «obiettivi legittimi di interesse generale», senza cioè mai spingersi fino a qualificarli come dei veri e propri diritti fondamentali. L'unica norma che, all'interno della Carta, menziona la sicurezza – ossia l'art. 6 – si limita, infatti, a stabilire che «ogni

Association for European Integration and Human Rights and Ekimdzhiev group, n° 62540/00; 2 giugno 2006, *Weber e Saravia c. Germania*, n° 54934/00; 16 febbraio 2000, *Amann c. Svizzera*, n° 27798/95; 24 aprile 1990, *Huvig c. Francia*, n° 11105/84. Una sistematizzazione della giurisprudenza CEDU in materia di protezione dei dati personali è stata pubblicata a settembre 2022 dalla Corte di Strasburgo in *www.coe.int/en/web/execution*. Sull'equilibrio tra sicurezza nazionale e diritto alla vita privata in dottrina, F. DUBUISSSON, *The European Court of Human Rights and the mass* surveillance, in *Revue trimestrielle des droits de l'homme*, 2016, p.855 ss.; ID, *La Cour européenne des droits de l'homme face à la surveillance de masse: obs. sous Cour eur. dr. h., Gde Ch., arrêt Big Brother Watch et autres c. Royaume-Uni*, *ibidem*, 2022, p.123 ss.; B. VAN DER SLOOT, *Big Brother Watch and others v. the United Kingdom & Centrum för Rättvisa v. Sweden: Does the Grand Chamber Set Back the Clock in Mass Surveillance Cases?*, in *European data protection law review (Internet)*, 2021, p. 319 ss.; M. ZALNIERIUTE, *Big Brother Watch and Others v. the United Kingdom*, in *The American journal of international law*, 2022, p. 585 ss.

[14] In tal senso, Corte giust., 24 settembre 2019, causa C-507/17, *Google LLC*, ECLI:EU:C:2019:772; 24 settembre 2019, causa C-136/17, *GC, AF, BH, ED c. Commission nationale de l'informatique et des libertés (CNIL)*, ECLI:EU:C:2019:773; 14 febbraio 2019, causa C-40/17, *Buividis*, ECLI:EU:C:2019:122; *Tele2 Sverige* cit.

[15] Quanto dibattito accademico sulla qualifica della sicurezza nazionale come un diritto o, ancora più in particolare, come un diritto fondamentale, X. DUPRE DE BOULOIS, *Existe-t-il un droit fondamental à la sécurité* ?, in *Revue des droits et libertés fondamentaux*, 2018, chron. 13 ; M.-A. GRANGER, *Existe-t-il un « droit fondamental à la sécurité ?*, in *Revue de science criminelle*, 2009, n° 2, p. 273 ss.

[16] Così, Corte giust., 3 settembre 2008, cause riunite C-402 e 415/05, *Kadi c. Consiglio e Commissione*, ECLI:EU:C:2008:461, punto 363, nonché 15 novembre 2012, cause riunite C-539 e 550/10, *Al-Aqsa c. Consiglio*, ECLI:EU:C:2012:711, punto 130.

[17] Al riguardo, Corte giust., 23 novembre 2010, causa C-145/09, *Tsakouridis*, ECLI:EU:C:2010:708, punti 46-47.

[18] In tal senso, Corte giust., *Schrems I* cit., punto 87; *Privacy International* cit., punti 74 e ss.

individuo ha diritto alla libertà e alla sicurezza»[19]. Tale disposizione, affiancando quest'ultima alla «libertà», non sembra così preordinata ad attribuire alla «sicurezza», peraltro definita in modo generico, il rango di diritto fondamentale comune, ma pare piuttosto volta ad evidenziare la complementarità tra questi due elementi al fine di costruire un equilibrato «spazio di libertà, sicurezza e giustizia» di cui all'art. 4 TFUE.

Né invero a una diversa conclusione pare condurre il fatto che, al punto 85 della sentenza *La Quadrature du Net*, il giudice di Lussemburgo, impiegando un linguaggio invero già in uso nella pronuncia *Digital Rights Ireland* con riguardo al contrasto della criminalità e nel parere *PNR tra Canada e Unione europea* quanto alla lotta contro reati di terrorismo[20], menzioni « il diritto alla sicurezza di cui all'art. 6 della Carta» per valutare la compatibilità con la direttiva *e-privacy* del 2002, che disciplina le condizioni di trattamento dei dati da parte dei fornitori di servizi di comunicazione,[21] delle legislazioni francese e belga che autorizzavano i propri servizi di *intelligence* a derogare alla predetta disciplina per salvaguardare la sicurezza nazionale,[22] così lasciando aperta la porta alla comprensione di quest'ultima nella più ampia nozione di «sicurezza» di cui alla norma di diritto primario in esame. Da un lato, ai punti 123-125 della pronuncia *La Quadrature du Net*, i giudici dell'Unione europea hanno precisato che l'art. 6 della Carta garantisce dei diritti analoghi a quelli tutelati dall'art. 5 CEDU, il quale, anche in virtù di una costante giurisprudenza di Strasburgo,[23] è volto a proteggere gli individui da ogni privazione di libertà arbitraria e ingiustificata da parte di un'autorità pubblica[24]. L'art. 5 CEDU e l'art. 6 della Carta hanno allora un contenuto tra loro omogeneo, nonché parimenti volto alla tutela di valori attinenti alla dignità umana in quanto tali estranei alla sfera pubblicistica invece sottesa alla nozione di «sicurezza nazionale». Secondo la giurisprudenza UE, quest'ultima corrisponde, infatti, al diverso interesse pubblico di tutelare le funzioni essenziali dello Stato e comprende così la prevenzione di attività in grado di destabilizzare le strutture costituzionali,

---

[19] Per un commento alla disposizione di diritto primario in esame, F. ROSSI DAL POZZO, *Art. 6 della Carta dei diritti fondamentali*, in R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Milano, 2017, p. 104 ss.

[20] Corte giust., *Digital Rights Ireland*, cit., punto 42; parere 1/15 *Canada/UE*, cit., punto 149. Sull'ambiguità dell'uso dell'art. 6 della Carta nella giurisprudenza UE, v. anche il Comitato LIBE in *Working Document (C) on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (2018/0108 (COD)) – Safeguards and remedies*, *PE637.469v01-00* del 1 aprile 2019, https://www.europarl.europa.eu/doceo/document/LIBE-DT-637469_EN.pdf?redirect, spec. p. 8, nota 20. In dottrina, X. TRACOL, *The two judgments of the European Court of Justice in the four cases of* Privacy International, La Quadrature du Net and Others, French Data Network and Others and Ordre des Barreaux francophones et germanophone and Others*: The Grand Chamber is trying hard to square the circle of data retention*, in *Computer Law & Security Review*, 2021, p. 11 ss.

[21] La direttiva 2002/58 del 12 luglio 2008, che disciplina il trattamento dei dati personali nel settore delle comunicazioni elettroniche anche al fine di tutela la vita privata degli individui, in *GUUE* L 201 del 31 luglio 2002, è stata modificata in ultimo dalla direttiva 2009/136 del 25 novembre 2009 in *GUUE* L 337 del 18 dicembre 2009, nonché rettificata nel 2017 in *GUUE* L 162 del 23 giugno 2017. Come si dirà oltre alla nota 50, sotto presidenza francese (2021) è stato avviato un procedimento di revisione dell'atto in esame.

[22] Sulla diversità in francese tra « *sûreté* » et « *securité* », L. ROBERT, *La jurisprudence de la CJUE relative au droit à la liberté et à la sûreté*, https://www.conseil-constitutionnel.fr/publications/titre-vii/la-jurisprudence-de-la-cjue-relative-au-droit-a-la-liberte-et-a-la-surete.

[23] Così, ad esempio, Corte Strasburgo 18 marzo 2008, *Ladent c. Polonia*, 11036/03, §§ 45-46; 29 marzo 2010, *Medvedyev c. Francia*, 3394/03, §§ 76-77; 13 dicembre 2012, *El-Masri c. Macedonia*, 39630/09, § 239.

[24] In questo senso, già M. GIALUZ, S. SPAGNUOLO, *Art. 5 CEDU*, in S. BARTOLE, P. DE SENA, V. ZAGREBELSKY (a cura di), *Commentario breve alla Convenzione europea dei diritti dell'uomo*, Padova, 2012, p. 107 ss. Sulla norma in esame, v. anche la Guida relativa all'art. 5 CEDU, https://www.echr.coe.int/Documents/Guide_Art_5_ITA.pdf

politiche, economiche e sociali fondamentali di un certo paese[25]. Dall'altro lato, ai punti 134-136 della sentenza *La Quadrature du Net*, i giudici di Lussemburgo, pur assegnando alla sicurezza nazionale un'importanza maggiore rispetto ad altre necessità securitarie (ad esempio, la sicurezza pubblica e la lotta alla criminalità) in quanto essa è tesa per l'appunto a salvaguardare le funzioni essenziali dello Stato da minacce di eccezionale gravità,[26] hanno confermato la qualificazione della «sicurezza nazionale» come un obiettivo d'interesse generale» anche dell'Unione europea[27], in tal modo allineandosi alla propria precedente giurisprudenza sul punto.

Questa interpretazione è stata peraltro confermata più di recente nella sentenza *G.D.* dell'aprile 2022. Pur se tale causa riguardava la ricevibilità nell'ambito di un procedimento penale di elementi di prova fondati su dati raccolti in base alla legislazione irlandese di trasposizione di una direttiva (la 2006/24/CE[28] inerente la conservazione dei dati generati nell'ambito dei servizi di comunicazione elettronica per il contrasto alla criminalità grave) dichiarata invalida nella già menzionata pronuncia *Digital Rights Ireland*, i giudici dell'Unione europea, sollecitati dagli Stati membri a prendere in considerazioni anche la diversa esigenza della sicurezza nazionale, hanno confermato una volta di più la qualificazione di quest'ultima come un «obiettivo d'interesse generale» del sistema comune[29]. Analogamente, nella pronuncia *SpaceNet* di settembre 2022, la Corte di giustizia, nel valutare la compatibilità con il diritto alla tutela dei dati dell'obbligo imposto dalla legislazione tedesca agli operatori di comunicazione nazionali di conservare in modo generalizzato i dati degli utenti per ragioni inerenti il contrasto della criminalità, ha precisato che «i diritti sanciti [tra l'altro all'art.] 8 della Carta non [sono] prerogative assolute, [l'art.] 52, par. 1, della [stessa], ammette[ndo] limitazioni all'esercizio di tale diritto, purché tali limitazioni rispondano [tra l'altro] a finalità di interesse generale riconosciute dall'Unione europea o all'esigenza di proteggere i diritti e le libertà altrui [… quali, ad esempio, i] diritti sanciti [tra l'altro all'art.] 6 della Carta e […] gli obiettivi di salvaguardia della sicurezza nazionale e di lotta alle forme gravi di criminalità»[30]. La «sicurezza» menzionata all'art. 6 della Carta è, in altri termini, un diritto fondamentale UE distinto dalla «sicurezza nazionale», la quale è viceversa ivi qualificata come un obiettivo d'interesse comune.

Se allora la sicurezza nazionale non è un diritto fondamentale UE, il riferimento alla «sicurezza di cui all'art. 6 della Carta» contenuto tra l'altro nella sentenza *La Quadrature du Net* deve allora essere più correttamente inteso – come forse già desumibile dal tenore dello stesso punto 85 secondo cui «i giudici del rinvio si interrogano, in particolare, in merito alle eventuali incidenze del diritto alla sicurezza sancito dall'art. 6 della Carta sull'interpretazione dell'art. 15, par. 1, della direttiva [*e-privacy*]» – come la mera riproduzione in sentenza di una (errata) qualificazione della norma in esame da parte degli organi giurisdizionali di rinvio, forse alimentata anche dall'ambiguo uso della stessa nella pronuncia *Digital Rights Ireland* e nel

[25] Tale definizione è contenuta in Corte giust., *La Quadrature du Net* cit., punto 135; *Privacy International* cit., punto 74. In tal senso anche Corte giust., *SpaceNet* cit., punto 92.
[26] Così, Corte giust., *La Quadrature du Net* cit., punto 135 e anche *Privacy International* cit., punto 74
[27] In tal senso, Corte giust., *La Quadrature du Net* cit., punti 134-136.
[28] Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE, in *GUUE*, 13.4.2005, L 105/54.
[29] Al riguardo, Corte giust., *G.D.* cit., punti 56-57.
[30] Corte giust., *SpaceNet* cit., pt. 63.

parere *PNR tra Canada e Unione europea*. La comprensione, nelle sentenze *La Quadrature du Net*, *G.D.* e *SpaceNet* della nozione di «sicurezza» di cui all'art. 6 della Carta nell'ambito della tutela dell'individuo, come peraltro appariva già chiaro dalle spiegazioni allegate alla stessa Carta[31], dovrebbe quindi escludere la riproposizione in futuro di tesi che viceversa associno quest'ultima ad esigenze pubblicistiche inerenti la protezione dello Stato e della società civile, nonché qualifichino la sicurezza nazionale come un diritto fondamentale europeo[32].

3. L'applicabilità del diritto UE anche in materia di dati personali nell'ambito della sicurezza nazionale: l'art. 4, par. 2, TUE.

La possibilità che il diritto dell'Unione europea inerente alla tutela dati personali – legislativo, giurisprudenziale e la Carta dei diritti fondamentali, che è applicabile «esclusivamente nell'attuazione» del diritto UE (art. 51, par. 1, Carta) – potesse influire su misure anche legislative degli Stati membri volte a salvaguardare la sicurezza nazionale non è però così scontata, quantomeno relativamente alle attività dei servizi di *intelligence* dei paesi membri. A ciò s'opponevano alcuni ostacoli di base inerenti i principi di ripartizione di competenza tra l'Unione europea e gli Stati membri, non a caso sollevati anche di recente da Regno Unito, Irlanda, Francia Svezia, Cipro, Repubblica ceca, Ungheria, Estonia e Polonia nei procedimenti pregiudiziali *La Quadrature du Net, French Data Network, Ordre des barreaux francophones et germanophone* e *Privacy International*[33], nonché dai governi francese, svedese, polacco e olandese nella successiva causa *SpaceNet*[34]. Se, da un lato, l'art. 16, par. 2, TFUE attribuisce all'Unione la competenza a stabilire «le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte degli Stati membri», in tal modo positivizzando il diritto fondamentale di cui all'art. 8 della Carta, dall'altro lato, l'art. 4, par. 2, TUE, introdotto con il trattato di Lisbona, prevede che «la sicurezza nazionale rest[i] di esclusiva competenza di ciascuno Stato membro»[35].

---

[31] Le spiegazioni alla Carta sono pubblicate in *GUUE* del 14 dicembre 2007, C 303/17.

[32] Un po' sorprendentemente tale teoria è stata proposta dal giudice del rinvio (il *Bundesverwaltungsgericht*, ossia la Corte amministrativa federale tedesca) anche nella causa *SpaceNet* cit., punto 36, risolta poi con la già citata sentenza Corte giust., del 20 settembre 2022. Alla luce della precedente della giurisprudenza UE – segnatamente le sent. *La Quadrature du Net* e *G.D.*, entrambe già cit. – e della qualificazione ivi contenuta della sicurezza nazionale come un obiettivo d'interesse generale anche UE – e non come diritto fondamentale di cui all'art. 6 della Carta – comprensibilmente la Corte di giustizia, in *SpaceNet* al punto 63, si è limitata ad affermare « l'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58 alla luce della Carta richiede che si tenga conto allo stesso modo dell'importanza dei diritti [fondamentali] sanciti agli articoli 3, 4, 6 e 7 della Carta e di quella che rivestono *gli obiettivi di salvaguardia della sicurezza nazionale* [corsivo aggiunto] e di lotta alle forme gravi di criminalità nel contribuire alla protezione dei diritti e delle libertà altrui».

[33] Così, Corte giust., *La Quadrature du Net* cit., punto 89; *Privacy International* cit., punto 32. Analogamente, il governo italiano nelle cause C-300/11, *ZZ c. Regno Unito*, ECLI:EU:C:2013:363, punto 38, risolta con sent. del 4 giugno 2013, nonché in causa C-387/05, *Commissione c. Italia*, ECLI:EU:C:2009:781, punto 44, conclusa con sent. del 15 dicembre 2009.

[34] In tal senso, Corte giust., *SpaceNet* cit., punto 48.

[35] Su tale norma dei trattati, v., *ex multiis*, G. MARTINICO, *What lies behind article 4(2) TEU?*, in A.S. ARNAIZ, C.A. LLIVINA (eds.), *National Constitutional Identity and European Integration*, 2013, p. 93 ss; ID., *Taming National Identity: A Systematic Understanding of Article 4.2 TEU*, in *European Public Law*, no. 3, 2021, p. 447 ss.; T. TRIDIMAS, *The General Principles of EU Law*, 3rd ed., Oxford, 2013; G. DI FEDERICO, *L'identità nazionale degli Stati membri nel diritto dell'Unione europea. Natura e portata dell'art. 4, par. 2, TUE*, Napoli, 2017; ID., *Il ruolo dell'art. 4, par. 2, TUE nella soluzione dei conflitti interordinamentali*, in *Quaderni costituzionali*, fasc. 2, 2019, p. 333 ss.; F. FERRARO, *Brevi note sulla competenza esclusiva degli Stati membri in materia di sicurezza nazionale*, Post AISDUE, Sezione "Convegni annuali e interinali", 2019, p. 95 ss.; A. KACZOROWSKA-IRELAND, *What Is the European Union required to Respect under Article 4(2) TEU?: The Uniqueness Approach*, in *European*

Tale tensione tra diritto comune in materia di protezione dei dati personali e diritto interno quanto alla salvaguardia della sicurezza nazionale si riproduce comprensibilmente anche a livello derivato. Probabilmente per dar conto a livello normativo dell'art. 4, par. 2, TUE, infatti, il Regolamento (UE) 2016/679 (di seguito, "GDPR"), che disciplina qualsiasi forma di uso dei dati (dalla raccolta alla cancellazione, passando per l'accesso, la conservazione o la trasmissione degli stessi a terzi) da parte di ogni persona fisica o giuridica, ivi incluse le autorità pubbliche, a prescindere dalla finalità sottesa al trattamento, esclude dal proprio ambito di applicazione – in un modo che, visto quando già sancito dalla norma dei trattati in esame, potrebbe sembrare in una certa misura superfluo e ridondante – i trattamenti «effettuati per attività che non rientrano nell'ambito di applicazione del diritto» UE (art. 2, par. 2, let. a))[36]. Come si evince dal combinato disposto di quest'ultima norma con il considerando 16 GDPR – «il presente regolamento non si applica a questioni […] quali le attività riguardanti la sicurezza nazionale» – l'art. 2, par. 2, let. a) richiama allora l'ambito della sicurezza nazionale e fa così eco all'art. 4, par. 2, TUE. Seppur impiegando la diversa dicitura di sicurezza «dello Stato» – la quale è in ogni caso intesa come sinonimo di «nazionale» (in tal senso, l'art. 15 direttiva *e-privacy*) – anche la direttiva *e-privacy*, che completa la disciplina generale del GDPR, esclude parimenti dal proprio ambito di applicazione le attività securitarie (art. 1, par. 3).

Ora, a fronte di tale quadro normativo ambivalente, se si propendesse, come sostenuto dai governi intervenuti nelle cause *La Quadrature du Net, French Data Network, Ordre des barreaux francophones et germanophone, Privacy International* e *SpaceNet*, per un'interpretazione letterale dell'art. 4, par. 2, TUE e delle corrispondenti norme di esclusione del GDPR (art. 2, par. 2, let. a)) e della direttiva *e-privacy* (art. 1, par. 3), della sicurezza nazionale sarebbero allora competenti esclusivamente gli ordinamenti giuridici interni[37]. Il diritto UE – primario, secondario e giurisprudenziale – non potrebbe così incidere in alcun modo sulle misure adottate dai paesi membri in materia di sorveglianza, e ciò anche quando queste ultime comprimano il godimento di diritti anche fondamentali comuni come, ad esempio, quello alla protezione dei dati personali, la cui disciplina positiva è contenuta nella direttiva *e-privacy* e nel GDPR.

Public Law, Vol. 25, 2019, p. 57 ss.; S. SULE, *National security and EU law restraints on intelligence activities* IN J-H DIETRICH, F. ALLUM, I. CAMERON, S. SULE, M.K. DAVIS CROSS, F. LE DIVELEC, J. GAJDOSOVÁ, S. GILMOUR, M. S. GOODMAN (eds), *Intelligence Law and Policies in Europe: A Handbook*, Munchen – Oxford, 2019, p. 335 ss.; B. DE WITTE, *Article 4(2) TEU as a Protection of the Institutional Diversity of the Member States*, in *European Public Law*, no. 3, 2021, p. 559 ss.; M. CLAES, *National Identity and the Protection of Fundamental Rights*, in *European Public Law*, Vol. 27, 2021, p. 517 ss. Più in generale sull'equilibrio tra diritto UE e diritto interno, E. BARTOLONI, *Ambito di applicazione del Diritto dell'Unione europea e ordinamenti nazionali. Una questione aperta*, Napoli, 2018, spec. p. 224 ss.

[36] Il regolamento 2016/679 del 27 aprile 2016 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in *GUUE* L 199, del 4 maggio 2016, p. 1. La disciplina UE sulla protezione dei dati è completata dalla direttiva 2016/680 che riguarda la tutela dei dati in materia penale (*GUUE* L 119 del 4 maggio 2016). Per un'analisi delle singole disposizioni del GDPR e, in termini comparativi, di quelle della direttiva *e-privacy* già cit., C. KUNER (eds), *The EU General Data Protection Regulation: A Commentary*, Oxford, 2020. Anche al fine di tener contro delle pronunce *Privacy Internationa*l e *La Quadrature du Net* cit., un aggiornamento – del 2021 a cura di C. KUNER, L.A. BYGRAVE E C. DOCKSEY – è reperibile https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3839645.

[37] Come si dirà oltre nel teso, il "diritto interno" comprende anche gli obblighi derivanti dal diritto CEDU, il quale, a differenza del sistema UE, non contiene alcun limite *ratione materiae* paragonabile all'art. 4, par. 2, TUE.

Tale interpretazione, che esclude ogni forma di influenza (anche reciproca) tra il sistema comune e quello nazionale allorché essi si sovrappongano, è stata tuttavia respinta dalla Corte di giustizia nelle pronunce *La Quadrature du Net* e *Privacy International*. Applicando alla tutela dei dati un principio invero già contenuto nella propria precedente giurisprudenza interpretativa dell'art. 4, par. 2, TUE[38], quest'ultima ha in effetti precisato che «sebbene spetti agli Stati membri decidere le misure idonee a garantire la loro sicurezza interna ed esterna, la mera circostanza che una decisione riguardi la sicurezza dello Stato non può comportare l'inapplicabilità del diritto dell'Unione europea»[39]. Tale norma dei trattati non costituisce allora una riserva di competenza esclusiva nelle mani dei sistemi giuridici nazionali che esclude dall'ambito d'applicazione del diritto UE qualsiasi provvedimento interno adottato per motivi securitari, in quanto ciò potrebbe compromettere la forza cogente, l'applicazione uniforme e l'effettività del diritto dell'Unione europea – e nelle fattispecie di quello della tutela dei dati di cui alla direttiva *e-privacy* oggetto di analisi nelle cause *La Quadrature du Net* e *Privacy International* – ogni volta in cui quest'ultimo entri in contatto e in conflitto con misure adottate dai paesi membri in materia di sicurezza nazionale[40].

Queste conclusioni, basate sul classico metodo comune dell'interpretazione funzionale se non teleologica[41], sono condivisibili anche considerato che la disposizione in esame – e la sicurezza ivi richiamata – non è una norma estranea ai trattati, ma ne è invece parte integrante[42]. Il fatto che, in modo inusuale rispetto al principio di attribuzione (art. 5 TUE), questa competenza non sia indirettamente desumibile dal difetto di competenza comune, ma sia invece espressamente riconosciuta agli Stati membri dallo stesso trattato, è un dato rilevante nell'interpretazione dell'art. 4, par. 2, TUE, dal quale sembra possibile desumere il mantenimento di un certo potere di controllo del diritto UE sulle misure interne, anche legislative, adottate per ragioni di sicurezza nazionale ogni volta in cui quest'ultima apporti limiti o deroghe a diritti contigui disciplinati dal diritto dell'Unione europea[43]. Ciò pare a maggior ragione vero considerato che, secondo una giurisprudenza UE costante, neppure ambiti di competenza esclusiva dei paesi membri – non menzionati cioè nei trattati diversamente da

[38] Tale principio è stato usato anche nelle già citate sent. *ZZ c. Regno Unito* e *Commissione c. Italia*, nonché nelle sent. 20 marzo 2018, causa C-187/16, *Commissione c. Austria (Tipografia di Stato)*, ECLI:EU:C:2018:194, punti 75-76; 2 aprile 2020, cause riunite C-715, 718 e 719/17, *Commissione c. Polonia, Ungheria e Repubblica ceca (Meccanismo temporaneo di ricollocazione di richiedenti protezione internazionale)*, ECLI:EU:C:2020:257, punti 143 e 170.

[39] Corte giust., *La Quadrature du Net* cit., punto 99; *Privacy International* cit., punto 44.

[40] Pare allora superata la teoria dottrinale (A. RUGGERI, *Trattato costituzionale, europeizzazione dei controlimiti e tecniche di risoluzione delle antinomie tra diritto comunitario e diritto interno*, in *Forum di Quaderni Costituzionali*, 2006; M. CARTABRIA, *Art. 4 TUE*, in A. TIZZANO (a cura di), *Trattati dell'Unione europea*, Milano, 2014, p. 26 ss.) che leggeva nell'art. 4, par. 2, TUE una mera codificazione europea dei c.d. controlimiti italiani.

[41] Sull'uso del classico metodo UE dell'interpretazione teleologica, seppur in termini critici, G. CONWAY, *The Legal Limits of Legal Reasoning and the European Court of Justice*, Cambridge, 2012, spec. p. 205 ss.

[42] *Contra*, I. CAMERON, *Metadata retention and national security: Privacy International and La Quadrature du Net*, in *Common Market Law Reviuw*, 2021, spec. pp. 1457-1460, la cui analisi a supporto della competenza nazionale non pare tuttavia convincente.

[43] In tal senso, già A. TIZZANO, *Il nuovo ruolo delle Corte supreme nell'ordine politico istituzionale: la Corte di giustizia dell'UE,* in *Diritto dell'Unione europea*, 2012, p. 811 ss., spec. p. 830; M. CONDINANZI, *I controlimiti come sintesi ideale tra primato da affermare e identità nazionale da rispettare*, in B. NASCIMBENE (a cura di), *Costa/Enel: Corte Costituzionale e Corte di giustizia a confronto, cinquant'anni dopo*, Milano, 2015, p. 119 ss., spec. p. 129 ss.; G. DI FEDERICO, *L'identità nazionale* cit., spec. Cap. III.

quanto accade in materia di sicurezza nazionale – sfuggono del tutto al rispetto del diritto comune in situazioni ricadenti nell'ambito di applicazione di quest'ultimo[44].

Dalle considerazioni appena svolte anche alla luce dell'interpretazione UE dell'art. 4, par. 2, TUE discendono allora alcune considerazioni. Da un lato, è lo stesso sistema comune a riconoscere, attraverso l'art. 4, par. 2, TUE, la competenza degli Stati membri (e non dell'Unione europea) ad adottare misure anche legislative inerenti alla sicurezza nazionale. Dall'altro lato, questi ultimi, nell'avvalersi di questa competenza, non possono però solo semplicemente invocare esigenze securitarie per giustificare qualsiasi provvedimento interno che escluda, limiti o deroghi a una disciplina UE contigua, dovendo l'esercizio di questo potere nazionale tener conto del diritto dell'Unione europea. Il fatto tuttavia che, anche nelle recenti sentenze *La Quadrature du Net, Privacy International* e *SpaceNet*, la Corte di giustizia dedichi a tale norma dei trattati solo il predetto inciso – il che, come si avrà modo di vedere nel prosieguo, deriva dall'inapplicabilità dell'art. 4, par. 2, TUE ai casi di specie – lascia irrisolta la questione, invero piuttosto delicata in quanto di confine tra diritto UE e diritto nazionale, dell'intensità dell'influenza che il primo può esercitare sul secondo allorché le misure interne adottate in materia di sicurezza nazionale deroghino, anche in modo rilevante, a una certa disciplina comune. Almeno allo stadio attuale dell'evoluzione giurisprudenziale UE, non è, in altri termini, chiaro quale tipo di controllo possano esercitare in tale ambito le istituzioni europee – e, tra queste, gli stessi giudici comuni – al fine di salvaguardare la forza cogente, l'effetto utile e la coerenza del diritto UE ogni volti in cui quest'ultimo entri in contatto con quello interno in materia di sicurezza nazionale. Seppur in un quadro giuridico ancora *in itinere* e di non facile interpretazione anche per effetto di una giurisprudenza dell'Unione non sempre lineare, l'analisi delle pronunce *La Quadrature du Net* e *Privacy International* alla luce di quelle relative all'art. 4, par. 2, TUE (*Commissione europea c. Italia* del 2009, *ZZ c. Regno Unito* del 2013, *B. c. Lettonia* e *B.K. c. Slovenia* del 2021[45]) pare offrire alcune prime risposte in merito.

4. L'influenza del diritto UE (anche in materia di dati personali) su misure di diritto interno adottate per motivi di sicurezza nazionale: tra questioni interne al sistema comune...

Il controllo che, al di là della sua intensità, il diritto dell'Unione europea spiega, per effetto della giurisprudenza interpretativa relativa all'art. 4, par. 2, TUE, sulle misure interne in

[44] Così, Corte giust., 24 novembre 1998, causa C-274/96, *Bickel e Franz*, ECLI:EU:C:1998:563, punto 17 in materia penale; 2 ottobre 2003, causa C-148/02, *Garcia Avello*, ECLI:EU:C:2003:539, punto 25 sul nome delle persone; 12 luglio 2005, causa C-403/03, *Schempp*, ECLI:EU:C:2005:446, punto 19 in materia di fiscalità diretta; 12 settembre 2006, causa C-145/04, *Spagna c. Regno Unito*, ECLI:EU:C:2006:543, punto 78 con riguardo al diritto di elettorato alle elezioni del Parlamento europeo; 2 marzo 2010, causa C-135/08, *Rottmann*, ECLI:EU:C:2010:104, punto 41 quanto alla cittadinanza di uno Stato membro.

[45] In aggiunta alle già menzionate pronunce *Commissione c. Italia* e *ZZ c. Regno Unito*, v. Corte giust., 22 giugno 2021, causa C-439/19, *B. c. Lettonia*, ECLI:EU:C:2021:504; 15 luglio 2021, causa C-742/19, *B.K. c. Slovenia*, ECLI:EU:C:2021:597. Quanto a *B. c. Lettonia*, v. in dottrina per un primo comment B. VAN DER SLOOT, *Is this the end for the re-use of PSI? :* Latvijas Republikas Saeima (HvJ EU, C-439/19), in *European Data Protection Law Review*, 2021, p. 473 ss.; S. WRIGLEY, B v Latvijas Republikas Saeima *: GDPR limits publishing of information about drivers who receive penalty points : case C-439/19 B v Latvijas Republikas Saeima*, *ibidem*, p. 609 ss. Con riguardo a *B.K. c. Slovenia*, M. Orlandi, *In tema di organizzazione dell'orario di lavoro del personale delle forze armate e di applicazione dei precetti sanciti nella direttiva 2003/88/CE*, in *Diritto dell'Unione Europea*, 2021, p. 647 ss.

materia di sicurezza nazionale è invero circoscritta a quei provvedimenti interni che, pur entrando in contatto con il diritto comune, rientrino nell'ambito di applicazione della predetta disposizione dei trattati. Quest'ultima è una (atipica) norma UE di riconoscimento della competenza degli Stati membri nell'ambito della sicurezza dello Stato, cosicché le misure interne ricomprese nella sfera attuativa dell'art. 4, par. 2, TUE sono escluse da quella del diritto dell'Unione europea, la quale inizia laddove finisce quella nazionale prevista dalla norma dei trattati in esame.

La situazione è tuttavia diversa – e l'influenza del diritto UE su quelli interni è allora maggiore – qualora, come accade in materia di tutela dei dati, sia lo stesso diritto comune a prevedere, con un'apposita norma, eccezioni alla propria disciplina generale – e ai diritti fondamentali ivi sottesi – al fine di garantire le esigenze di sicurezza nazionale. Probabilmente sul presupposto che le moderne tecniche di indagine dei servizi di *intelligence* si fondano ormai sull'uso di dati raccolti per ragioni estranee alla sicurezza dello Stato e che ciò comporta per natura rilevanti deroghe alle regole di accesso e trattamento dei dati previste del diritto derivato comune, gli artt. 15 della direttiva *e-privacy* e 23 GDPR – nonostante la generale esclusione di competenza di cui agli artt. 1, par. 3, della direttiva *e-privacy* e 2, par. 2, let. a) GDPR – autorizzano i paesi membri ad adottare, per esigenze di sicurezza nazionale, legislazioni che limitino la portata (solo) di taluni obblighi e diritti ivi stabiliti, ancorché esclusivamente nel rispetto di talune condizioni. In particolare, l'art. 15 della direttiva *e-privacy* impone agli ordinamenti giuridici interni l'uso dello strumento legislativo per adottare ogni misura derogatoria, nonché prevede la possibilità di apportare eccezioni solo agli obblighi e diritti di cui agli artt. 5, 6, 8 e 9 della direttiva. L'intervento di deroga devo poi rispettare i valori (art. 2 TUE) e i diritti fondamentali dell'Unione europea (art. 6 TUE), nonché i principi di necessità e di proporzionalità. Riproducendo per ampi trattati quest'ultima disposizione temporalmente antecedente, l'art. 23 GDPR stabilisce che gli Stati membri possono, per motivi di sicurezza dello Stato, limitare, anche in tal caso solo mediante misure legislative, la portata esclusivamente di taluni obblighi e diritti del GDPR (quelli di cui agli artt. 5, 12-22 e 34) qualora tale limitazione, oltre ad essere necessaria e proporzionata, rispetti l'essenza dei diritti e delle libertà fondamentali comuni. Al fine poi di dare concretezza alle condizioni generali di cui al par. 1, il par. 2 della medesima norma GDPR precisa che le legislazioni derogatorie degli Stati membri debbano contenere regole specifiche riguardanti almeno le finalità del trattamento, le categorie di dati impiegati, la portata delle limitazioni introdotte, talune garanzie per prevenire abusi (accessi o trasferimenti illeciti a terzi), l'indicazione precisa del titolare del trattamento, i periodi di conservazione dei dati, i rischi per i diritti e le libertà degli interessati, nonché il diritto di questi ultimi di essere informati delle predette limitazioni.

In casi del genere, secondo la Corte di giustizia[46], le normative degli Stati membri che derogano, per ragioni di sicurezza nazionale, alla disciplina UE prevista dalla direttiva *e-privacy* – perché, come accade nelle predette cause, esse obblighino gli operatori economici a mettere

[46] In tal senso, Corte giust., *La Quadrature du Net* cit., punto 94; *Privacy International* cit., punto 38. In generale sull'equilibrio tra sicurezza nazionale e tutela UE dei dati personali, C. DOCKSEY, *The European Court of Justice and the Decade of Surveillance*, in H. HIJMANS, H. KRANENBORG (eds.), *Data Protection 2014: How to Restore Trust?*, Bruxelles, 2014, p. 97 ss.; C. TIMMERMANS, *The Competence Divide of the Lisbon Treaty Six Years After*, in S. GARBEN, I. GOVAERE (eds.), *The Division of Competences between the EU and the Member States: Reflections on the Past, the Present and the Future*, Oxford-Portland, 2017, p. 19 ss.

nella disponibilità dei servizi di *intelligence* i dati da loro raccolti per ragioni commerciali, andando in tal modo oltre i limiti al trattamento degli stessi stabiliti dal predetto atto comune al fine di tutelare la riservatezza delle comunicazioni degli utenti – rientrano nell'ambito di applicazione dell'atto UE derogato per effetto dell'art. 15 della direttiva *e-privacy*. Disposizioni che, come quest'ultima e anche l'analogo art. 23 GDPR, stabiliscono le condizioni di compatibilità delle legislazioni interne derogatorie a una certa disciplina comune, presuppongo, infatti, la comprensione di queste ultime nella sfera attuativa dell'atto UE derogato. Questi provvedimenti sono di conseguenza compatibili con il diritto dell'Unione europea solo laddove essi rispettino le condizioni derogatorie previste dall'art. 15 dalla direttiva *e-privacy* e anche dall'analogo art. 23 GDPR, le quali applicano condizioni e principi classici di bilanciamento tra diritti/esigenze propri del sistema UE. Considerato poi che, come già ricordato, lo spazio attuativo dell'art. 4, par. 2, TUE inizia ove finisce quello comune, misure interne di questo tipo sono allora viceversa escluse dall'ambito attuativo della predetta norma dei trattati.

Né invero a una diversa conclusione – ossia l'inclusione di queste ultime nella sfera di controllo del diritto interno per effetto dell'art. 4, par. 2, TUE – avrebbe condotto il già citato art. 1, par. 3, della direttiva *e-privacy* (e invero anche l'analogo art. 2, par. 2, let. a) GDPR) secondo cui quest'ultima «non si applica alle attività riguardanti la sicurezza dello Stato». Da un lato, e seppur con riferimento all'analogo art. 2, par. 2, let. a) GDPR, i giudici dell'Unione europea, nella pronuncia *B. c. Lettonia*, hanno rilevato che tale norma «dal momento che configura un'eccezione alla definizione molto ampia dell'ambito di applicazione [del GDPR] deve essere interpretata restrittivamente»[47]. L'esistenza di norme analoghe all'art. 2, par. 2, let. a) GDPR – e dunque anche l'art. 1, par. 3, della direttiva *e-privacy* – non determina allora l'esclusione totale di ogni misura interna adottata in materia di sicurezza dello Stato dall'ambito attuativo del diritto comune derogato (GDPR e direttiva *e-privacy*). Ciò è invero comprensibile dato che ciò è stato già affermato dai giudici dell'Unione europea con riguardo all'art. 4, par. 2, TUE, ossia a una disposizione che riproduce il contento degli artt. 2, par. 2, let. a) GDPR e 1, par. 3, della direttiva *e-privacy*. Dall'altro lato, l'art. 1, par. 3, della direttiva *e-privacy* contempla legislazioni nazionali diverse da quelle sottese all'art. 15 della direttiva *e-privacy* e le due norme, pur riferendosi sempre alla sicurezza nazionale, hanno così ambiti attuativi distinti, presupponendo così un grado di interferenza e sovrapposizione tra diritto UE e diritto interno differente. Una diversa conclusione avrebbe in effetti privato di senso l'art. 15 della direttiva *e-privacy* (e anche l'art. 23 GDPR). In effetti, se si fosse ritenuto, come sostenuto dagli Stati membri intervenuti nei procedimenti pregiudiziali *La Quadrature du Net* e *Privacy International*, che la sicurezza nazionale fosse esclusa, in virtù dell'art. 1, par. 3, dall'ambito di applicazione della direttiva *e-privacy*, l'art. 15 della stessa, che invece subordina l'esercizio di almeno parte della potestà legislativa dei paesi membri in materia di sicurezza nazionale al rispetto delle condizioni ivi stabilite, avrebbe perso il proprio effetto utile. Anche considerato che le legislazioni francese, belga e inglese oggetto dei rinvii pregiudiziali in esame derogavano in modo sostanziale alla disciplina UE prevista nella direttiva *e-privacy*, per i giudici di

[47] Così, Corte giust., *B. c. Lettonia* cit., punto 68; nonché in precedenza già 9 luglio 2020, causa C-272/19, *Land Hessen*, ECLI:EU:C:2020:535, punto 68. In termini analoghi, quanto però agli Stari terzi, Corte giust., *Schrems II* cit., punto 84. L'interpretazione restrittiva di norme derogatorie alla disciplina generale UE sempre in materia di protezione dei dati personali è peraltro ribadita nella sentenza *SpaceNet* cit., punto 57 quanto all'art. 15 della direttiva *e-privacy* cit.

Lussemburgo sono state sufficienti queste considerazioni per concludere ritenendo che queste ultime rientrassero nell'ambito di applicazione del diritto comune (e non invece del diritto interno e CEDU per effetto dell'art. 1, par. 3, della direttiva *e-privacy*). E in effetti, tali sentenze si concentrano sulla valutazione della compatibilità – in ultimo accertata – delle predette misure con l'insieme delle condizioni derogatorie stabilite all'art. 15 della direttiva *e-privacy*, così confermando la comprensione delle prime nell'ambito attuativo di quest'ultima e dunque del diritto UE[48].

Da tali considerazioni si possono trarre alcune conseguenze. Innanzitutto, sul presupposto che l'art. 1, par. 3, della direttiva in esame riproduce a livello derivato il contenuto dell'art. 4, par. 2, TUE, la distinzione operata dai giudici dell'Unione europea tra gli ambiti di applicazione degli artt. 1, par. 3, e 15 della direttiva *e-privacy* equivale a riconoscere un'analoga diversità attuativa tra quest'ultimo e l'art. 4, par. 2, TUE. Le legislazioni degli Stati membri adottate per ragioni di sicurezza nazionale che rientrano nell'ambito di applicazione di quest'ultima norma non sono dunque le stesse di quelle che sono considerate parte dell'art. 15 della direttiva *e-privacy*. A tale conclusione non si potrebbe neppure obiettare che in realtà la Corte di giustizia e l'avvocato generale Campos Sánchez Bordona nelle cause *La Quadrature du Net* e *Privacy International* non abbiano stabilito, quantomeno espressamente, un legame giuridico tra l'art. 1, par. 3, della direttiva *e-privacy* e l'art. 4, par. 2, TUE, concentrando la propria analisi sul primo e limitandosi a ricordare, quanto al secondo, che la competenza ivi attribuita agli Stati membri non comporta l'inapplicabilità del diritto comune. Da un lato, l'analisi dell'art. 4, par. 2, TUE (punti 99 *La Quadrature du Net* e 44 *Privacy International*) segue immediatamente quella dell'art. 1, par. 3, della direttiva *e-privacy* (punti 96-98 *La Quadrature du Net* e 42-43 *Privacy International*), in tal modo attestando la continuità logico-giuridica tra le due disposizioni in esame nel ragionamento dei giudici dell'Unione europea. Dall'altro lato, questi ultimi hanno affermato che «le disposizioni dell'art. 4, par. 2, TUE non valgono a inficiare le conclusion[i] raggiunte», ossia per l'appunto la distinzione tra gli ambiti applicativi degli artt. 1, par. 3, e 15 della direttiva *e-privacy*. Anzi, proprio il fatto che la Corte di giustizia abbia dedicato all'art. 4, par. 2, TUE, solo brevi cenni, limitandosi a ribadire che questa norma non costituisce una riserva di competenza assoluta a favore dei paesi membri nel settore della sicurezza dello Stato, pare proprio supportare la tesi interpretativa ivi proposta. Le legislazioni francese, belga e inglese oggetto dei rinvii pregiudiziali *La Quadrature du Net* e *Privacy International*, nella misura in cui contemplavano un regime pienamente derogatorio alla disciplina della direttiva *e-privacy*, rientravano nell'ambito di attuazione di quest'ultima per effetto del suo art. 15, cosicché, proprio a fronte della distinzione tra gli ambiti attuativi di quest'ultima norma e dell'art. 1, par. 3, era allora superfluo dilungarsi nella disamina di una disposizione – l'art. 4, par. 2, TUE – quantomeno non totalmente pertinente per la soluzione delle cause, seppur (erroneamente) invocata dagli organi giurisdizionali di rinvio.

La linea interpretativa seguita nelle pronunce *La Quadrature du Net* e *Privacy International* pare inoltre essere stata confermata dalla Corte di giustizia nelle successive pronunce *G.D.* del 5 aprile 2022 e *SpaceNet* del 20 settembre 2022, emesse anch'esse nella composizione della Grande Sezione. Quanto alla prima, e seppur relativamente alla compatibilità con l'art. 15 direttiva *e-privacy* di una normativa irlandese che permetteva alle

[48] In merito, Corte giust,. *La Quadrature du Net* cit., punti 105 ss.; *Privacy International* cit., punti 50 ss.

autorità pubbliche un accesso generale ai dati generati o trattati nell'ambito della fornitura di servizi di comunicazione anche elettronica per il contrasto della lotta alla criminalità, i giudici dell'Unione europea, sollecitati dai governi intervenuti nella procedura a pronunciarsi anche in merito alla diversa esigenza della salvaguardia della sicurezza nazionale, hanno precisato che quest'ultima «letta alla luce dell'art. 4, par. 2, TUE, supera quella degli altri obiettivi di cui all'art. 15 della direttiva *e-privacy* e in particolare di quelli della lotta alla criminalità anche grave [cosicché], fatto salvo il rispetto degli altri requisiti previsti all'art. 52, par. 1, della Carta, [essa] è quindi idone[a] a giustificare misure [degli Stati membri] che comportino ingerenze nei diritti fondamentali più gravi di quelle che potrebbero giustificare tali altri obiettivi»[49]. L'art. 4, par. 2, TUE – questa volta espressamente menzionato accanto all'art. 15 della direttiva *e-privacy* – non comporta parimenti l'esclusione dei provvedimenti interni inerenti la sicurezza nazionale dall'ambito di attuazione dell'atto comune in esame, la loro ammissibilità essendo anche in questo caso subordinata al rispetto delle condizioni stabilite dall'art. 15 della direttiva *e-privacy*. Sulla base della predetta norma dei trattati, i giudici di Lussemburgo, nella sentenza *G.D*, sono giunti così alle medesime conclusioni raggiunte nelle pronunce *La Quadrature du Net* e *Privacy International* sulla base dell'art. 1, par. 3, della direttiva *e-privacy*, in tal modo confermando il parallelismo tra quest'ultima disposizione e la predetta norma dei trattati. Analogamente, nella sentenza *SpaceNet*, la Corte di giustizia, rispondendo alle argomentazioni dei governi irlandese, francese, olandese, polacco e svedese secondo cui le normative intere adottate ai fini della salvaguardia della sicurezza nazionale non rientrano nell'ambito di applicazione della direttiva *e-privacy* in virtù dell'art. 4, par. 2, TUE, ha affermato che queste ultime rientrano viceversa nell'ambito di applicazione del predetto atto di diritto derivato UE in virtù dell'art. 15 della direttiva *e-privacy* [50].

Il fatto peraltro che in tutte le sentenze esaminate i giudici di Lussemburgo, nell'interpretare quest'ultima norma, abbiano sempre preso in considerazione l'art. 4, par. 2, TUE esclude la possibilità di proporre in futuro teorie interpretative che, al fine di negare valore alla distinzione tra gli ambiti di applicazione degli artt. 1, par. 3, della direttiva *e-privacy* e 4, par. 2, TUE, da un alto, e dell'art. 15 della direttiva in esame, dall'altro lato, sostengano l'incompatibilità di quest'ultimo (e anche dell'art. 23 GDPR) con la predetta norma di diritto primario[51]. Una tesi del genere non terrebbe conto del fatto che l'art. 15 della direttiva *e-privacy*, come anche l'art. 23 GDPR, si limitano a ribadire a livello derivato condizioni di compatibilità – ovvero l'uso di uno strumento legislativo, il rispetto del contenuto essenziale dei diritti e libertà fondamentali UE, nonché i principi di necessità e proporzionalità – già stabilite all'art. 52, par. 1, della Carta secondo cui «eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto

[49] Così, Corte giust., *G.D*. cit., punti 56- 57.
[50] In tal senso, Corte giust., *SpaceNet* cit, punto 48.
[51] Sull'eliminazione, in sede di revisione della direttiva *e-privacy* effettuata sotto presidenza francese, dell'attuale art. 15 della direttiva *e-privacy* e l'introduzione di un nuovo articolo che escludesse espressamente ogni attività di trattamento di dati inerenti la sicurezza nazionale indipendentemente dal soggetto che effettuerà tale operazione (operatore privato o autorità pubblica), v. il considerando 7° e l'art. 2, par. 2, let. a) della proposta di regolamento del Parlamento europeo e del Consiglio del 10 febbraio 2021 sul rispetto della vita privata e sulla protezione dei dati nelle comunicazioni elettroniche in sostituzione della predetta direttiva (https://www.lawfareblog.com/how-europes-intelligence-services-aim-avoid-eus-highest-court-and-what-it-means-united-states), nonché https://www.lawfareblog.com/how-europes-intelligence-services-aim-avoid-eus-highest-court-and-what-it-means-united-states.

essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione europea o all'esigenza di proteggere i diritti e le libertà altrui»[52]. Analoghe condizioni sono state inoltre applicate dalla giurisprudenza UE per contemperare il diritto alla tutela dei dati di cui all'art. 8 della Carta con le esigenze di lotta alla criminalità (*Digital Rights Ireland*, *Tele2 Sevige* e *G.D.*), nonché di salvaguardia della sicurezza nazionale (*Schrems I, PNR tra Canada e Unione europea, Schrems II*). Seppur con riferimento alla tutela dei dati in Stati terzi, la Corte di giustizia, nella sentenza *Schrems I*, ha, infatti, concluso per l'invalidità della decisione di adeguatezza *Safe Harbour* in quanto essa, non prevedendo limiti e condizioni al trattamento dei dati UE da parte dei servizi di *intelligenc*e USA per ragioni di sicurezza nazionale, autorizzava queste ultime ad un accesso generalizzato alle comunicazioni degli utenti europei, il che era inammissibile in quanto avrebbe comportato una compressione non proporzionata a un diritto fondamentale tutelato nella Carta (art. 8), in tal modo pregiudicatone il contenuto essenziale (art. 52)[53]. Inoltre, nel parere *PNR tra Canada e Unione europea* e nella pronuncia *Schrems II*, i giudici di Lussemburgo hanno precisato che eventuali limitazioni all'esercizio del diritto fondamentale alla protezione dei dati devono essere previste dalla legge[54]. Al fine poi di soddisfare i requisiti di necessità e proporzionalità, la normativa interna che comporta una tale ingerenza deve indicare in modo chiaro e preciso la portata e l'applicazione della misura *de qua*, nonché prevedere garanzie sufficienti a favore degli individui che permettano di proteggere efficacemente i propri dati contro il rischio di abusi[55].

Anche considerato che tali condizioni di compatibilità, applicate nei casi *Schrems I, PNR tra Canada e Unione europea* e *Schrems II* relativamente a Stati extra-UE, sono state impiegate in ugual modo dalla Corte nelle pronunce *La Quadrature du Net* e *Privacy International* con riguardo agli Stati membri, l'eventuale abrogazione – in sede di riversione della direttiva *e-privacy* o del GDPR – dell'art. 15 della direttiva *e-privacy* o dell'art. 23 GDPR non escluderebbe allora automaticamente dall'ambito di applicazione di tali atti UE provvedimenti nazionali che deroghino alla disciplina ivi stabilita, garantendo in tal modo agli ordinamenti giuridici interni un maggior margine di manovra in materia. Legislazioni di questo tipo rientrano, infatti, nello spazio attuativo della direttiva *e-privacy* (e del GDPR) in questo esse introducono significative eccezioni al generale sistema di tutele previsto dal diritto comune e dunque a prescindere dagli artt. 15 della direttiva *e-privacy* o 23 GDPR. Anzi, in mancanza di disposizioni che, analogamente a questi ultimi, positivizzino i principi elaborati dalla giurisprudenza UE alla luce tra l'altro dell'art. 52, par. 1, della Carta, l'individuazione delle condizioni di compatibilità con il sistema UE delle legislazioni interne derogatorie alla disciplina comune sarebbe allora lasciata all'apprezzamento caso per caso dei giudici e dei garanti degli Stati membri, anche attraverso il coinvolgimento della Carta mediante il rinvio pregiudiziale di cui all'art. 267 TFUE.

[52] In tal senso, Corte giust., *SpaceNet* cit., punto 63.
[53] Così, Corte giust., *Schrems I* cit., punto 94; nonché, quanto all'obiettivo della lotta alla criminalità, *Digital Rights Ireland e a*. cit., punto 39.
[54] In merito, Corte giust., *Schrems II* cit., punti 173-175; parere 1/15 *Canada/UE* cit., punto 139.
[55] Al riguardo, Corte giust., *Schrems II* cit., punto 176; parere 1/15 *Canada/UE* cit., punti 140-141.

5. *Segue*: …e questioni disciplinate dal diritto interno e CEDU.

Le conclusioni a cui si è giunti nel paragrafo precedente – ossia che le legislazioni nazionali che derogano, per motivi di sicurezza nazionale, agli obblighi e ai diritti previsti dal diritto derivato comune in materia di protezione dei dati rientrano nell'ambito di applicazione di quest'ultimo e sono sottoposte alle condizioni di compatibilità previste agli artt. 15 della direttiva *e-privacy* o 23 GDPR – sono state invero circoscritte dalla Corte di giustizia, quantomeno nelle pronunce *La Quadrature du Net* e *Privacy International*, a quelle misure che disciplinano un caso specifico di accesso ai dati UE da parte delle autorità di *intelligence*, ossia quello c.d. mediato che presuppone la divulgazione a queste ultime dei dati UE ad opera dei fornitori di servizi di comunicazione. Quando invece gli ordinamenti interni attuano direttamente misure nazionali che derogano alla riservatezza delle comunicazioni, senza cioè imporre obblighi di trattamento ai predetti operatori, la protezione dei dati degli utenti ricade viceversa nell'ambito attuativo del diritto degli Stati membri, nonché per tale via della CEDU[56]. Un po' sorprendentemente, l'applicazione del diritto dell'Unione europea e l'effettività delle tutele ivi previste sembrerebbe allora dipendere dalle modalità di acquisizione dei dati da parte delle autorità di *intelligence*, essendo quest'ultima esclusa ogni volta in cui i predetti servizi di sorveglianza impieghino autonomi mezzi d'intercettazione sia per raccogliere direttamente specifiche informazioni sia per accedere a dati detenuti da operatori privati.

Ora, tale precisazione dei giudici di Lussemburgo, la quale riguarda aspetti eccedenti le cause in esame e costituisce così un *obiter dictum*, pare corretta quando riferita all'accesso, attraverso autonomi mezzi d'intercettazione, dei servizi di *intelligenc*e a informazioni specifiche inerenti determinati individui od organizzazioni. In tal caso, infatti, la fattispecie mancherebbe di ogni elemento di contatto diretto con la disciplina della direttiva *e-privacy*. L'uso di strumenti di intercettazione autonomi da parte di queste ultime esclude in effetti ogni coinvolgimento dei fornitori di servizi di comunicazione anche elettronica, invece presupposto per l'applicazione della direttiva in esame (elemento di contatto soggettivo). In tal modo, le autorità di *intelligence* avrebbero inoltre accesso a dati "nuovi", diversi cioè da quelli raccolti per ragioni commerciali dai fornitori di servizi di comunicazione (elemento di contatto oggettivo). Situazioni di questo tipo, mancando di un elemento di contatto tanto soggettivo quanto oggettivo con la disciplina contenuta nella direttiva oggetto dei rinvii *La Quadrature du Net* e *Privacy International*, sembrano allora rientrare a giusto titolo nell'ambito applicativo dell'art. 4, par. 2, TUE ed essere dunque regolate dal diritto interno e da quello CEDU. Ciò fatto salvo quanto si dirà nel prosieguo relativamente agli effetti che il diritto comune esercita in ogni caso su misure interne anche comprese nella sfera attuativa della predetta norma dei trattati.

Pare invece più difficile applicare queste medesime conclusioni nel caso in cui i servizi di *intelligence* ottengano, ancorché sempre ricorrendo a propri mezzi di intercettazione, informazioni rilevanti per la salvaguardia della sicurezza nazionale accedendo ai dati posseduti dai fornitori dei predetti servizi. In questa occasione, tali autorità non acquisiscono "nuovi" dati, ma attingono invece a quelli già raccolti dagli operatori privati in applicazione alle regole stabilite dalla direttiva *e-privacy*, il che sembra giustificare la comprensione anche della situazione in esame nell'ambito di applicazione del diritto UE in ragione del contatto oggettivo

[56] In tal senso, Corte giust., *La Quadrature du Net* cit., punto 103; *Privacy International* cit., punto 48.

con la disciplina comune. Adottando questa prospettiva, l'elemento in funzione del quale determinare la competenza – dell'Unione europea o invece dei sistemi interni per effetto dell'art. 4, par. 2, TUE – a stabilire le condizioni di accesso ai dati UE da parte dei servizi di *intelligence* degli Stati membri per ragioni di sicurezza nazionale dovrebbe allora essere individuato non tanto nella sussistenza della collaborazione attiva degli operatori privati, quanto nella natura dei dati effettivamente acquisiti. Questa soluzione permetterebbe peraltro di evitare il paradosso per cui le autorità di sorveglianza dei paesi membri potrebbero non richiedere ai predetti operatori l'accesso ai dati personali da loro raccolti – ma ottenerli senza la loro collaborazione, entrando direttamente nei loro server mediante propri mezzi di intercettazione – per rendere di fatto inattuabile il sistema di tutele europeo.

A tale teoria si potrebbe invero obiettare che, a differenza di quanto osservato nelle cause *La Quadrature du Net* e *Privacy International* ove le legislazioni nazionali imponevano agli operatori dei servizi di comunicazione regole inerenti al trattamento dei dati sostanzialmente opposte da quelle previste dalla direttiva *e-privacy* (conservazione di tutti i dati degli utenti senza l'applicazione dei limiti quantitativi, qualitativi o temporali stabiliti da quest'ultima), nell'ipotesi appena prospettata le autorità di *intelligence* avrebbero invece avuto accesso solo ai dati raccolti e conservati dai predetti operatori in ossequio alle regole previste dalla predetta direttiva. L'assenza di divergenze rispetto alla disciplina comune potrebbe, in altri termini, indurre a ritenere inapplicabili le condizioni di garanzia previste dall'art. 15 della direttiva *e-privacy*, le quali intervengono proprio laddove il sistema nazionale voglia introdurre deroghe sostanziali al regime europeo. In realtà, posto che l'accesso ai dati raccolti dai fornitori di servizi di comunicazione da parte di terzi diversi dal personale autorizzato può avvenire, senza il consenso degli utenti, solo alle condizioni di cui all'art. 15 della direttiva *e-privacy* (art. 5 della stessa), l'acquisizione di dati da parte dei servizi di *intelligence* – per sua natura effettuata da soggetti non qualificabili come "personale autorizzato" e senza il consenso degli individui intercettati – è di per sé già una deroga alla disciplina prevista nella direttiva, il che presuppone per l'appunto l'applicazione delle condizioni di garanzia previste all'art. 15 della stessa. Ciò pare a maggior ragione vero considerato che la Corte di giustizia, probabilmente consapevole della gravità dei rischi che l'accesso di terzi (e dunque anche delle autorità di *intelligence*) può comportare al diritto della tutela dei dati, ha ripetutamente affermato che tale accesso, se effettuato in deroga alle regole stabilite dal diritto dell'Unione europea (della direttiva ma invero anche del GDPR), costituisce un'ingerenza autonoma nel predetto diritto fondamentale, a prescindere dalla circostanza che le informazioni di cui trattasi abbiano o meno carattere sensibile, o che gli interessati abbiano o meno subito inconvenienti in seguito a siffatta ingerenza, o che i dati personali siano o meno stati utilizzati successivamente[57]. Le autorità di *intelligence* accederebbero poi a dati raccolti per una finalità diversa da quella di garantire la salvaguardia della sicurezza nazionale, ossia quella commerciale, il che costituisce di per sé un'ulteriore deroga al principio generale della limitazione delle finalità previsto all'art. 5, par. 3, della direttiva *e-privacy* (e anche dal GDPR).

[57] Così, Corte giust., *La Quadrature du Net* cit., punto 114-116 e la giurisprudenza ivi citata; nonché la sent. *G.D.*, punti 44 e 47.

Il ragionamento seguito dai giudici di Lussemburgo nelle sentenze *La Quadrature du Net* e *Privacy International* lascia inoltre perplessi anche sotto un ulteriore profilo[58]. Secondo questi ultimi, dalla lettura in combinato disposto degli artt. 2, par. 2, lett. d) e 23, par. 1, lett. d) GDPR si evincerebbe che i trattamenti di dati personali effettuati da autorità pubbliche anche di *intelligence* degli Stati membri sarebbero parimenti esclusi dell'ambito di applicazione del GDPR, il quale coinciderebbe in tal modo con quello della direttiva *e-privacy*. Entrambi gli atti UE disciplinerebbero, in altri termini, i trattamenti di dati effettuati solo da privati (2, par. 2, lett. d) GDPR), cosicché le legislazioni nazionali che prevedono l'accesso delle autorità pubbliche e, tra queste, anche dei servizi di *intelligence* ai dati per ragioni securitarie in deroga alla disciplina generale (23, par. 1, lett. d) GDPR) sarebbero escluse dalla sfera attuativa non solo della direttiva *e-privacy*, ma anche del GDPR ogni volta in cui esse manchino della collaborazione dei predetti operatori. Qualora l'oggetto interpretativo del rinvio pregiudiziale fosse stato il GDPR (e non la direttiva *e-privacy*), la Corte avrebbe, in altri termini, concluso nel medesimo modo, ricomprendendo parimenti il solo accesso mediato ai dati raccolti dai fornitori dei servizi di comunicazione nell'ambito attuativo del diritto UE.

In realtà, come già ricordato, l'ambito attuativo del GDPR è più ampio di quella della direttiva *e-privacy*, ricomprendendo i trattamenti di dati UE posti in essere non solo da ogni persona fisica e giuridica, ma anche da ogni autorità pubblica (artt. 2, par. 1, e 4, parr. 2, 7 e 8) diversa però da quelle che operano in materia penale e di sicurezza nazionale. Tali operazioni, quantomeno quando realizzate dai servizi di sorveglianza con propri strumenti di intercettazione, rientrano, come già ricordato, nell'ambito attuativo del diritto interno per effetto dell'art. 2, par. 2, lett. a) GDPR, il quale riproduce a livello derivato l'art. 4, par. 2, TUE. I trattamenti di dati UE effettuati dalle autorità operanti in ambito penale sono invece esclusi dall'ambito applicativo del GDPR in virtù dell'art. 2, par. 2, lett. d) – erroneamente menzionato in *La Quadrature du Net* e *Privacy International* con riferimento alla sicurezza nazionale, probabilmente assimilando quest'ultima alla, invece diversa, nozione di sicurezza pubblica ivi citata – in quanto essi sono oggetto della disciplina specifica di cui alla già citata direttiva 2016/680. Tenendo conto del diverso ambito attuativo tra gli atti in esame ma applicando al GDPR, a fronte dell'equivalenza sostanziale tra l'art. 23 GDPR e l'art. 15 della direttiva *e-privacy*, i principi elaborati dalla Corte di giustizia nelle pronunce *La Quadrature du Net* e *Privacy International* con riferimento a quest'ultima disposizione, rientrerebbero di conseguenza nell'ambito di applicazione del GDPR quantomeno le misure nazionali che disciplinino l'accesso ai dati personali da parte dei servizi di *intelligence* attraverso l'intermediazione non solo degli operatori privati, ma anche delle autorità pubbliche diverse da quelle operanti in materia penale. Ciò a meno che non si voglia accogliere la tesi qui sostenuta che ricomprende nello spazio attuativo del diritto comune in materia di tutela dei dati anche quelle normative interne che prevedono l'accesso diretto, ad opera dei predetti servizi, ai dati raccolti e conservati, per finalità diverse da quella della sicurezza nazionale, da operatori privati (direttiva *e-privacy*) ed autorità pubbliche distinte da quelle operanti in materia penale (GDPR).

6. L'influenza esercitata dal diritto UE anche in materia di dati personali su questioni attinenti alla sicurezza nazionale tra Stati membri e Paesi terzi.

[58] Analogamente, M. ZALNIERIUTE, *A Struggle for Competence: National Security* cit., spec. pp. 211-212.

L'interpretazione qui proposta che, a differenza di quanto affermato dalla Corte di giustizia nei casi *La Quadrature du Net* e *Privacy International*, attribuisce al sistema dell'Unione europea la competenza a stabilire le condizioni di accesso ai dati personali da parte delle autorità di *intelligence* degli Stati membri anche allorché esso sia attuato accedendo, mediante propri mezzi di intercettazione, ai server dei fornitori di servizi di comunicazione (e nel caso del GDPR di autorità diverse da quelle operanti in ambito penale) sembra inoltre più in linea con la giurisprudenza comune in materia di trasferimenti di dati UE in Stati terzi. Nella sentenza *Schrems II*, i giudici di Lussemburgo hanno precisato che un trasferimento di dati personali UE effettuato a fini commerciali da un operatore economico stabilito in uno Stato membro dell'UE verso un altro operatore economico stabilito in un paese terzo rientra nell'ambito applicativo del GDPR nonostante il fatto che «*durante o in seguito a tale trasferimento*» questi dati possano essere sottoposti a trattamento da parte delle autorità del paese terzo al fine di garantire la sicurezza dello Stato[59]. Almeno quando si tratti dei poteri delle autorità di *intelligence* USA oggetto del rinvio in esame – e, in virtù dell'efficacia *ultra partes* della giurisprudenza comune e della formulazioni in termini generali del detto principio, probabilmente anche di quelle di ogni altro paese terzo – il diritto dell'Unione europea (GDPR e artt. 8 e 52 della Carta) disciplina così le condizioni alle quali queste ultime possono avere accesso ai dati UE non solo quando ciò avvenga mediante la divulgazione degli stessi da parte di fornitori dei servizi di comunicazione situati in nord America ove tali dati sono conservati (*in seguito a tale trasferimento*), ma anche allorché tali autorità li acquisiscano durante il loro transito dai *server* europei a quelli nordamericani (*durante tale trasferimento*), ossia in una circostanza che presuppone l'inconsapevolezza dei predetti operatori e prescinde dalla loro collaborazione. Il controllo che il diritto dell'Unione europea esercita sui poteri dei servizi di *intelligence* nel caso di trasferimenti internazionali di dati UE è allora più esteso e penetrante di quello previsto per le medesime autorità all'interno del sistema comune.

Tale diversità di applicazione del diritto dell'Unione europea non pare doversi ascrivere al diverso atto – direttiva *e-privacy* o GDPR – oggetto di interpretazione rispettivamente nelle sentenze *La Quadrature du Net* e *Privacy International*, da un lato, e nella pronuncia *Schrems II*, dall'altro lato. Come già ricordato, gli artt. 2, par. 2, lett. a) e 23 GDPR inerenti la sicurezza nazionale riproducono il contenuto degli artt. 1, par. 3, e 15 della direttiva *e-privacy*, cosicché teorie interpretative basate su queste ultime (*La Quadrature du Net* e *Privacy International*) sembrano ragionevolmente trasponibili alle prime e viceversa, pena una incoerenza giuridica interna al sistema comune. Seppur invocando disposizioni del GDPR riguardanti la diversa esigenza della lotta alla criminalità in materia penale (artt. 2, par. 2, lett. d) e 23, par. 1, lett. d) h)), tale equivalenza è stata peraltro riconosciuta dalla stessa Corte di giustizia nelle sentenze *La Quadrature du Net* e *Privacy International*, affermando che «l'interpretazione degli artt. 1, par. 3, e 15 della direttiva *e-privacy* è coerente con [… il GDPR]»[60].

Se allora il più esteso sindacato rivendicato dai giudici di Lussemburgo quanto all'accesso ai dati UE da parte dei servizi di *intelligence* di Stati terzi rispetto a quelli dei paesi membri non dipende dal diverso atto oggetto d'interpretazione, essa è allora probabilmente da ascriversi alla maggior facilità d'applicazione del diritto dell'Unione europea e della Carta dei

[59] Così, Corte giust., *Schrems II* cit., punti 88-89.
[60] In tal senso, Corte giust., *La Quadrature du Net* cit., punto 102; *Privacy International* cit., punto 47.

diritti fondamentali in caso dei trasferimenti internazionali di dati UE. In quest'ultima occasione, infatti, l'attuazione del diritto UE discende direttamente dal fatto che le misure di sicurezza nazionale adottate da un sistema terzo sono uno degli elementi espressamente presi in considerazione dalla Commissione europea per valutare l'adeguatezza dello stesso agli standard di tutela stabiliti dal sistema comune (art. 45, par. 2, GDPR). Viceversa, il fatto che all'interno dell'Unione europea, il diritto UE tratti della sicurezza nazionale prevalentemente in negativo – vuoi per attribuirne la competenza agli Stati membri (art. 4, par. 2, TUE) vuoi per escluderla dal proprio ambito attuativo (considerando 16 e art. 2, par. 2, lett. a) GDPR; art. 1, par. 3, direttiva *e-privacy*) – rende quantomeno più complesso, anche alla luce del contenuto derogatorio di norme come gli artt. 23 GDPR o 15 della direttiva *e-privacy*, stabilire i confini d'applicazione del diritto comune e della Carta in relazione alla competenza nazionale.

L'approccio ambivalente della Corte di giustizia potrebbe invero spiegarsi anche alla luce di un diverso elemento, ossia l'influenza esercitata dalla CEDU nei confronti degli Stati membri e non invece di paesi terzi come, ad esempio, gli USA di cui alle pronunce *Schrems I* e *Schrems II*. Il sistema CEDU, a differenza di quello dell'Unione europea, non contiene una norma analoga all'art. 4, par. 2, TUE ed è dunque certamente competente a pronunciarsi in materia di sicurezza nazionale. A fronte della maggior facilità di tale ordinamento a ragionare sul punto di equilibrio tra quest'ultima esigenza e la tutela dei dati, non sorprende allora che la Corte di Strasburgo, a differenza di quella di Lussemburgo, sia stata già da tempo ripetutamente sollecitata a pronunciarsi sull'ampiezza dei poteri di accesso ai dati UE da parte dei servizi di *intelligence* di Stati aderenti per motivi di sicurezza nazionale, in via tanto diretta quanto mediata. Ciò ha così dato vita ad una copiosa giurisprudenza che subordina la compatibilità con l'art. 8 CEDU in materia di tutela della vita privata di legislazioni interne inerenti al trattamento dei dati da parte delle predette autorità per motivi securitari al rispetto di condizioni e limiti ispirati al principio di proporzionalità (indicazione dei casi nei quali i servizi di *intelligence* sono abilitati a intercettare le comunicazioni, dei soggetti suscettibili di essere intercettati, previsione di limiti temporali all'esecuzione di tali misure restrittive, dei casi nei quali le predette autorità sono obbligate a distruggere i dati ivi raccolti, di regole per la diffusione di questi ultimi a soggetti terzi, controllo da parte di un'autorità giurisdizionale indipendente dai governi) analoghi a quelli stabiliti dalla Corte di giustizia sulla base dell'art. 52 della Carta quanto all'accesso ai dati UE almeno da parte delle autorità di *intelligence* di Stati terzi (*Schrems I* e *Schrems II*)[61]. In tale contesto, attribuire allora alla competenza degli Stati membri – che aderiscono tutti alla CEDU – la valutazione della legalità delle misure interne che disciplinano l'accesso diretto delle autorità di *intelligence* ai dati UE significa di fatto sottoporre queste ultime a un *test* di compatibilità CEDU basato su principi analoghi a quelli applicati all'interno dell'Unione europea relativamente a normative nazionali adottate nell'ambito di applicazione del diritto comune. La maggior severità dimostrata dalla Corte nei confronti dell'esercizio dei poteri dei servizi di *intelligence* di Stati terzi che, come, ad esempio, gli USA non aderiscano alla CEDU, trova allora forse giustificazione nell'assenza in questi casi di una rete di tutele internazionali adeguata.

Sebbene si possano comprendere le ragioni di ordine partico e le difficoltà giuridiche che hanno spinto i giudici dell'Unione europea a sviluppare tale giurisprudenza "a doppia

[61] In merito, v. la giurisprudenza CEDU e la dottrina già cit. alla nota 14 del presente contributo.

velocità", la soluzione di escludere dall'ambito di applicazione del diritto comune le legislazioni interne che regolano l'accesso diretto ai dati UE da parte dei servizi di sorveglianza dei paesi membri per motivi securitari non appare del tutto soddisfacente. Innanzitutto, essa individua il diritto applicabile, nazionale o comune, in funzione di meri elementi tecnici, peraltro variabili nel tempo, come la tecnologia usata per l'accesso ai dati e/o la partecipazione attiva delle imprese alla loro acquisizione. E ciò nonostante, nella pronuncia *Schrems I* relativa al trasferimento internazionale di dati di utenti europei, la stessa Corte di giustizia abbia affermato che il diritto alla riservatezza delle comunicazioni di cui all'art. 8 della Carta può dirsi effettivamente protetto esclusivamente in presenza di determinate salvaguardie applicabili non solo in situazioni di accesso ai dati che coinvolgono le imprese, ma anche qualora quest'ultimo venga effettuato direttamente dalle autorità pubbliche competenti, senza cioè che a tal riguardo rilevi il metodo usato per accedere ai predetti dati. La soluzione proposta nelle sentenze *La Quadrature du Net* e *Privacy International* crea inoltre un'incoerenza tra l'applicazione del medesimo diritto fondamentale UE – ossia quello di cui all'art. 8 della Carta – all'interno o all'esterno dell'Unione europea, in tal modo facendo variare l'effettività di tale diritto fondamentale in funzione di un ulteriore elemento, ossia il fatto che i dati personali UE siano o meno trasferiti in sistemi giuridici extra-UE.

7. Il tipo di controllo esercitato dal diritto UE anche in materia di dati personali su misure di diritto interno rientranti nell'ambito d'applicazione dell'art. 4, par. 2, TUE.

Al di là della teoria che si ritenga più convincente quanto all'estensione dell'ambito di applicazione del diritto UE in materia di protezione dei dati e/o di quello del corrispondente art. 4, par. 2, TUE, sembra ora opportuno chiedersi quale sia l'influenza esercitata dal sistema comune sulle misure interne comprese nello spazio attuativo di quest'ultima disposizione dei trattati. Pur potendo anche ammettere che essa implichi il rispetto di condizioni meno severe di quelle imposte dagli artt. 15 direttiva *e-privacy* e 23 GDPR a normative interne pienamente rientranti nella sfera applicativa del diritto dell'Unione europea, l'adozione da parte degli Stati membri di legislazioni che regolino l'accesso diretto ai dati UE da parte dei servizi di *intelligence* per motivi securitari non comporta l'inapplicabilità totale del diritto comune, ma anzi, come già ricordato, costituendo quest'ultima l'esercizio di una facoltà riconosciuta ai paesi membri dal trattato (art. 4, par. 2, TUE), essa presuppone proprio il mantenimento di un certo controllo da parte di quest'ultimo. E in effetti, l'analisi della recente giurisprudenza relativa a quest'ultima disposizione[62] mostra proprio come la Corte di giustizia, probabilmente per salvaguardare l'effetto utile della disciplina UE in materia di tutela dei dati, non abbia esitato ad esercitare il proprio controllo giurisdizionale per definire la linea di demarcazione tra il diritto dell'Unione europea e quello interno.

Tale controllo di confine non sembra tuttavia essere stato esercitato dai giudici dell'Unione in un modo lineare, cosicché, quantomeno allo stato attuale dell'evoluzione della giurisprudenza UE, non è facile individuarne con precisione la natura e la portata. La diversità di approccio interpretativo relativo all'art. 4, par. 2, TUE emerge confrontando, ad esempio, tra loro due recenti pronunce UE – *B. c. Lettonia* e *B.K. c. Slovenia* – rese a un solo mese di distanza (rispettivamente giugno e luglio 2021) dalla medesima sezione giurisdizionale UE, ossia la

[62] Così, Corte giust., *B.K. c. Slovenia* cit. e *B. c. Lettonia* cit.

Grande Sezione. Mentre in effetti nella sentenza *B. c. Lettonia*, quest'ultima sembra riconoscere all'art. 4, par. 2, TUE un ruolo e un peso maggiore – quasi come se esso assolvesse alla funzione di ripartire le competenze tra sistema UE e diritto interno – nella sentenza *B.K. c. Slovenia* essa pare invece ricondurne il funzionamento al classico schema interpretativo tra regola generale (libertà di circolazione) ed eccezioni (ordine pubblico, pubblica sicurezza, sanità pubblica, nonché le esigenze imperative d'interesse UE) impiegato, ad esempio, nell'interpretazione della disciplina in materia di mercato unico.

In particolare, la causa *B. c. Lettonia* verteva sulla compatibilità con il GDPR di una legislazione lettone che obbligava l'organismo pubblico responsabile del registro in cui sono iscritti i punti di penalità inflitti ai conducenti di veicoli per infrazioni stradali a rendere tali dati accessibili al pubblico anche in assenza di un interesse legittimo. Nel procedimento nazionale era stato tuttavia eccepita l'inapplicabilità del GDPR in virtù dell'art. 2, par. 2, lett. a) dello stesso, il quale, riproducendo il contenuto dell'art. 4, par. 2, TUE, esclude dal proprio ambito attuativo la materia della sicurezza nazionale. Almeno secondo la Lettonia, le predette attività riguardanti la sicurezza stradale, svolte da autorità pubbliche e riconducibili allo Stato, erano finalizzate a ridurre le infrazioni gravi al codice della strada ed erano allora dirette a salvaguardare la sicurezza nazionale, ossia una materia esclusa dall'ambito di applicazione del GDPR. Anche considerato che, come già ricordato, l'art. 2, par. 2, lett. a) GDPR, derogando a un regime generale UE, deve essere interpretato restrittivamente, i giudici dell'Unione hanno tuttavia respinto questa tesi ritenendo che le attività inerenti la sicurezza stradale non fossero ricomprese tra quelle volte a salvaguardare la sicurezza nazionale in quanto non tutelavano le funzioni essenziali dello Stato e gli interessi fondamentali della società. Il mero fatto che l'attività fosse propria dello Stato non era allora sufficiente perché l'eccezione di cui all'art. 2, par. 2, lett. a) GDPR fosse ivi applicabile, in tal determinando l'inapplicabilità di quest'ultimo alla fattispecie giuridica in esame.

Ora, in tal caso, il controllo di confine esercitato dai giudici di Lussemburgo si è concentrato sui motivi invocati a livello nazionale per sottrarre una certa misura di diritto interno (legislazione lettone in materia di sicurezza stradale) dall'ambito attuativo del diritto dell'Unione europea (GDPR) in virtù della clausola derogatoria di cui all'art. 2, par. 2, lett. a) GDPR inerente alla sicurezza nazionale. Il fatto che questa valutazione non sia stata lasciata alla competenza degli Stati membri, ma sia invece stata effettuata direttamente dalla Corte – peraltro sia in positivo (perché un'attività sia finalizzata a tutelare la sicurezza nazionale essa deve essere riconducibile allo Stato, nonché difendere gli interessi essenziali della società) sia in negativo (la sicurezza stradale non è un'attività volta a salvaguardare la sicurezza nazionale in quanto non difende gli interessi essenziali della collettività) – pone così le basi per l'elaborazione di una nozione autonoma UE di «sicurezza nazionale»[63]. Se allora il potere di controllo dei giudici di Lussemburgo relativamente all'art. 4, par. 2, TUE si sostanzia nell'accertamento, in base a una propria analisi, della legittimità dei motivi inerenti la sicurezza nazionale invocati dagli Stati membri per giustificare l'inapplicabilità di una certa disciplina comune, la quale è da effettuarsi alla luce della nozione UE di sicurezza nazionale, il controllo

[63] Al riguardo, c'è da chiedersi se la eventuale futura elaborazione di una nozione UE autonoma di sicurezza nazionale possa poi eventualmente giustificare la competenza comune in questo ambito anche alla luce dell'art. 352 TFUE.

operato da questi ultimi in base ai principi di necessità e proporzionalità è allora solo preliminare, nonché volto esclusivamente ad evitare che i paesi membri invochino abusivamente clausole derogatorie come l'art. 2, par. 2, lett. a) GDPR per limitare l'applicazione delle tutele comuni. Dall'approccio suggerito dalla Corte di giustizia in questa pronuncia sembra così potersi dedurre che qualora quest'ultima, in base a una propria disamina, concordasse con lo Stato membro quanto alla necessità d'invocare motivi securitari per escludere l'applicabilità di tutele comuni in un certo ambito, il sindacato UE non potrebbe spingersi fino ad operare una valutazione sostanziale delle misure interne, la quale spetterebbe alla competenza nazionale anche in base ai parametri di compatibilità previsti dalla giurisprudenza CEDU, i quale sono peraltro analoghi a quelli impiegati nell'Unione europea.

Le considerazioni appena svolte non devono tuttavia indurre a sottovalutare l'importanza attribuita dai giudici di Lussemburgo al controllo esercitato da quest'ultima nell'ambito di applicazione dell'art. 4, par. 2, TUE. Anzi, proprio il fatto che, anche in un caso come quello in esame ove il rigetto delle motivazioni invocate dalla Lettonia per sostenere l'inapplicabilità del GDPR era scontato – la sicurezza stradale difficilmente avrebbe potuto essere qualificata come un'esigenza di sicurezza nazionale! – quest'ultima si sia premurata di interpretare la norma dei trattati in esame, ivi inclusa la nozione stessa di sicurezza nazionale, sembra sottintendere la volontà dei giudici dell'Unione europea di sottoposte al proprio controllo giurisdizionale – seppur circoscritto ad escludere gli abusi della competenza interna – ogni iniziativa nazionale adottata in materia di sicurezza sulla base giuridica degli artt. 2, par. 2, lett. a) GDPR e 4, par. 2, TUE.

L'influenza esercitata dal sistema UE su misure nazionali rientranti nell'ambito attuativo dell'art. 4, par. 2, TUE così come descritta nella pronuncia *B. c. Lettonia* differisce tuttavia da quella delineata nella sentenza *B.K. c. Slovenia*. In quest'ultimo caso la Corte era stata chiamata ad accertare l'applicabilità di una direttiva concernente taluni aspetti dell'organizzazione dell'orario di lavoro a un'attività di guardia svolta da un militare, la quale, almeno secondo la Slovenia, era diretta a garantire la sicurezza dello Stato e sarebbe così rientrata nella sfera di applicazione esclusiva dei paesi membri in virtù dell'art. 4, par. 2, TUE. Nel rispondere al quesito pregiudiziale, i giudici di Lussemburgo hanno precisato che qualora, come nel caso di specie, l'applicazione della disciplina UE (in materia di organizzazione dell'orario di lavoro) possa pregiudicare l'esercizio di determinate attività d'interesse nazionale, quali per l'appunto quelle delle guardie militari, essa può essere limitata per tenere conto delle predette esigenze interne attraverso limitazioni proporzionate che non vadano oltre quanto necessario per la tutela degli interessi nazionali (l'adeguata programmazione dell'orario lavorativo di cui alla direttiva in esame è, ad esempio, esclusa per i militari esclusivamente quando coinvolti in eventi eccezionali che non permettano l'avvicendamento degli organici). In tale contesto, i giudici di Lussemburgo hanno così dato vita a un controllo UE più tradizionale e pervasivo fondato sull'applicazione, anche nell'ambito dell'art. 4, par. 2 TUE, dei classici principi comuni volti a bilanciare esigenze confliggenti, ossia quelli di necessità e di proporzionalità, così come peraltro previsto dalla giurisprudenza UE anche per ambiti di competenza esclusiva nazionale non menzionati nei trattati[64]. In questo caso, l'art. 4, par. 2,

[64] Seppur basandosi sulla giurisprudenza più risalante e, in particolare, sulla già più volte menzionata pronuncia *ZZ c. Regno Unito*, questa pare essere anche l'interpretazione accolta da G. DI FEDERICO, *L'identità nazionale* cit.,

TUE pare allora essere considerato dai giudici di Lussemburgo non tanto come una norma sulla ripartizione di competenze tra diritto UE e diritto interno, ma come una disposizione che si limita a riconoscere l'importanza di alcuni interessi degli Stati membri atti a giustificare talune limitazioni – peraltro solo se necessarie e proporzionate – alla disciplina comune. E in effetti nella pronuncia *B.K. c. Slovenia* la Corte di giustizia non ha esitato ad affermare che la sicurezza nazionale di cui all'art. 4, par. 2 TUE deve essere solo «*debitamente presa in considerazione*»[65], dal rispetto dovuto dall'Unione alle funzioni essenziali dello Stato non discendendo l'inapplicabilità del diritto UE alle decisioni dei paesi membri relative all'organizzazione delle forze armate.[66]

L'approccio interpretativo appena descritto affonda probabilmente le proprie radici nella risalente giurisprudenza comune inerente l'art. 4, par. 2, TUE, ossia le già menzionate sentenze *ZZ c. Regno Unito* del 2013, *Commissione c. Italia* del 2009 e *Commissione c. Spagna* del 1999. In effetti, in tutti questi casi, i giudici di Lussemburgo, nel valutare la legittimità di misure interne (il diniego d'ingresso di un cittadino UE nel Regno Unito; l'esenzione da talune imposte per l'importazione e l'esportazione di armi nelle cause italiana e spagnola) derogatorie a una certa disciplina europea (rispettivamente la libera circolazione delle persone e delle merci) per motivi inerenti la salvaguardia della sicurezza nazionale, hanno parimenti sottoposto le predette misure interne al test di compatibilità fondato sui principi UE di necessità e di proporzionalità. In realtà, un'attenta lettura di queste pronunce evidenzia come, anche nei casi *ZZ c. Regno Unito, Commissione c. Italia* e *Commissione c. Spagna*, il diritto comune derogato (la direttiva 2004/38/CE relativa al diritto dei cittadini europei e dei loro familiari di circolare e soggiornare liberamente nel territorio degli Stati membri[67]; il regolamento (CE) n. 150/2003 che sospendeva i dazi doganali applicabili alle attrezzature ad uso militare[68]; la direttiva 77/388/CEE in materia di armonizzazione delle legislazioni degli Stati membri relative alle imposte[69]) contenesse disposizioni che autorizzavano i paesi membri ad introdurre eccezioni al regime generale UE ivi previsto proprio per ragioni di sicurezza nazionale (art. 30 direttiva 2004/38; art. 2, par. 2, regolamento 150/2003; punti 23-25 all. F della direttiva 77/388/CEE). Le fattispecie *ZZ c. Regno Unito, Commissione c. Italia* e *Commissione c. Spagna* assomiglierebbero allora a quelle oggetto d'analisi nelle sentenze *La Quadrature du Net* e *Privacy International*, cosicché l'applicazione anche nei primi del classico test UE di compatibilità fondato sui principi di necessità e proporzionalità discenderebbe dalla volontà non tanto di impiegare tali principi comuni nell'ambito attuativo dell'art. 4, par. 2, TUE, quanto

p. 110; nonché S. MONTALDO, *Il bilanciamento tra esigenze di pubblica sicurezza e diritti processuali dell'individuo: convergenze e divergenze tra Lussemburgo e Strasburgo*, in *Diritti umani e diritto internazionale*, 2013, p. 813 ss.

[65] Corte giust., *B.K. c. Slovenia* cit., punto 44.

[66] *Ibidem*, punto 39.

[67] Direttiva 2004/38/CE del Parlamento europeo e del Consiglio del 29 aprile 2004 relativa al diritto dei cittadini dell'Unione e dei loro familiari di circolare e di soggiornare liberamente nel territorio degli Stati membri, che modifica il regolamento (CEE) n. 1612/68 ed abroga le direttive 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE e 93/96/CEE, in *GUUE* L 158, del 30 aprile 2004, p. 77.

[68] Regolamento (CE) n. 150/2003 del Consiglio, del 21 gennaio 2003, che sospende i dazi doganali applicabili a talune armi e attrezzature ad uso militare, in *GUUE* L 25, del 30 gennaio 2003, p. 1.

[69] Sesta direttiva 77/388/CEE del Consiglio, del 17 maggio 1977, in materia di armonizzazione delle legislazioni degli Stati membri relative alle imposte sulla cifra di affari – Sistema comune di imposta sul valore aggiunto: base imponibile uniforme, in *GUCE* L 145, del 13 giugno 1977, p. 1.

dalla qualificazione delle legislazioni nazionali oggetto di scrutinio come rientranti nell'ambito di applicazione del diritto comune derogato in virtù di disposizioni interne all'atto stesso.

Tali considerazioni potrebbero peraltro valere anche per la fattispecie alla base della pronuncia *B.K. c. Slovenia*, escludendo l'art. 2, par. 2 della direttiva 89/391[70] dall'ambito di applicazione della stessa «alcune attività specifiche del pubblico impiego come quelle delle forze armate». Sebbene la genericità di tale inciso renda quest'ultimo difficilmente assibilabile all'art. 15 della direttiva *e-privacy*, esso di fatto autorizza gli Stati membri ad adottare normative interne inerenti gli orari di lavoro delle forze armate solo in circostanze eccezionali, cosicché, in virtù dei principi elaboratori nelle pronunce *La Quadrature du Net* e *Privacy International*, tali provvedimenti nazionali rientrerebbero nell'ambito attuativo della predetta diretta e dovrebbero essere ammessi solo se deroghino alla disciplina generale europea in maniera proporzionata e in ogni caso solo ove necessario.

Almeno fino a quando una nuova pronuncia comune non chiarisca in modo definitivo il tipo di controllo che il diritto dell'Unione può esercitare su misure interne rientranti nell'ambito applicativo dell'art. 4, par. 2, TUE, la qualificazione delle fattispecie di cui alle cause *ZZ c. Regno Unito*, *Commissione c. Italia*, *Commissione c. Spagna* e *B.K. c. Slovenia* come comprese nella sfera di applicazione del diritto derivato UE derogato in virtù di una espressa norma dello stesso dovrebbe allora indurre a ritenere più appropriato l'uso nei casi di esame dei principi di proporzionalità e necessità solo per escludere abusi della competenza degli Stati membri in materia di sicurezza nazionale.

8. Conclusioni

La definizione dell'ambito di applicazione dell'art. 4, par. 2, TUE e il tipo di controllo, più o meno penetrante, che il diritto dell'Unione europea può esercitare, in virtù di quest'ultima norma, su misure interne che deroghino, per motivi di sicurezza nazionale, alla disciplina comune tra l'altro in materia di tutela dei dati personali è ormai una questione sempre più frequente nel dibattito anche istituzionale europeo. L'uso da parte di taluni Stati (Ungheria, Polonia, Spagna e Grecia) di un *software* – *Pegasus* – per raccogliere informazioni su giornalisti, oppositori politici, diplomatici, avvocati ed altri attori anche economici della società civile nazionale ha, infatti, indotto il Parlamento europeo a creare, ad aprile 2022, un'apposita commissione interna d'inchiesta[71], nonché la Commissione europea a richiedere formalmente, ad agosto 2022, ai paesi membri coinvolti delucidazioni in merito[72], in tal modo dimostrando la convinzione, quantomeno di tali istituzioni, di poter sottoporre al sindacato UE anche fattispecie di accesso diretto a dati "nuovi" da parte delle autorità di *intelligence* dei paesi membri allorché ciò violi, ad esempio, i valori a fondamento del sistema comune (art. 2 TUE). L'eventuale futuro intervento della Corte di giustizia in un caso che, come *Pegasus*, non implica una deroga diretta al diritto derivato UE in materia di tutela dei dati personali in virtù di una norma espressa di quest'ultimo – il che può avvenire attraverso il ricorso in infrazione nel caso

[70] Direttiva 89/391/CEE del Consiglio, del 12 giugno 1989, concernente l'attuazione di misure volte a promuovere il miglioramento della sicurezza e della salute dei lavoratori durante il lavoro, in *GUCE* L 183, del 29 giugno 1989, p. 1.

[71] https://www.europarl.europa.eu/news/it/press-room/20220412IPR27117/pegasus-and-other-spyware-inquiry-committee-begins-its-work-on-19-april.

[72] https://www.europarl.europa.eu/doceo/document/E-9-2022-001677-ASW_EN.pdf

in cui, ad esempio, la Commissione decida di avviare una procedura *ex* art. 258 TFUE per violazione dell'art. 2 TUE o con il rinvio pregiudiziale per effetto dell'iniziativa di individui od associazioni davanti alle autorità di protezione dei dati nazionali, come peraltro pare essere già il caso in Ungheria e Polonia – potrebbe allora indurre quest'ultima a porre per la prima volta al centro della propria interpretazione l'art. 4, par. 2, TUE, in tal modo quantomeno aggiungendo un ulteriore tassello alla delicata questione dell'esercizio della competenza interna in materia di sicurezza nazionale da parte dei servizi di sorveglianza dei paesi membri.

L'importanza di tali questioni di confine non è peraltro circoscritta al solo contesto dell'Unione. A dicembre 2020, il Comitato di politica economica digitale dell'OCSE, preoccupato dell'impatto economico di una crescente "crisi di fiducia" nei flussi di dati personali derivante da forme di accesso ai dati raccolti dagli operatori economici, ha in effetti deciso di avviare dei negoziati tra i suoi trentasei paesi aderenti (tra cui ventitré Stati membri, a cui si aggiunge la Commissione europea che partecipa ai lavori dell'OCSE) per definire regole e limiti condivisi all'accesso di questi ultimi ai predetti dati (apposite basi giuridiche su cui i governi possono imporre l'accesso ai dati; quest'ultimo deve poi essere svolto solo per soddisfare finalità legittime e in osservanza dei principi di necessità e di proporzionalità; rispetto di procedure di autorizzazione dell'accesso e di limitazioni al trattamento dei dati acquisiti, comprese le garanzie di riservatezza, integrità e disponibilità; tali attività devono essere sottoposte a un controllo indipendente e di mezzi efficaci di ricorso ecc.). L'OCSE prevede di concludere i suoi lavori per la fine dell'anno 2022. Sarà allora interessante osservare i punti, più o meno marcati, di convergenza tra i principi sviluppati a livello internazionale (da paesi cioè appartenenti a ordinamenti giuridici e tradizioni diverse da quelle degli Stati membri dell'Unione europea come, ad esempio, Stati Uniti, Canada, Messico, Cile, Giappone, Nuova Zelanda ecc.) e le esigenze poste dal diritto e dalla giurisprudenza UE su un tema – quello dei trasferimenti dei dati in un'economia digitale sempre più dematerializzata – per natura transfrontaliero e che richiede pertanto soluzioni il più possibile condivise[73].

I futuri interventi delle istituzioni europee (giurisdizionali ma anche politiche) e internazionali (CEDU e OCSE), che quantomeno al momento si fondano su principi tendenzialmente comuni, dovrebbero allora contribuire a costruire un quadro giuridico chiaro, preciso e adeguato all'azione dei servizi di *intelligence* che permetta di perseguire gli obiettivi di interesse generale della sicurezza nazionale, senza per questo pregiudicare i diritti fondamentali UE e CEDU e, in particolare, di quello della protezione dei dati personali che, forse più di altri, è atto ad essere compromesso dalle interferenze attuate per esigenze securitarie. Né beneficerebbero non solo le autorità preposte alla tutela della sicurezza nazionale ma anche, e prima di tutto, i cittadini, i cui dati personali sono sempre più oggetto di operazioni di raccolta e trattamento, nonché gli operatori commerciali, le cui attività dipendono sempre più dallo scambio di tali dati.

[73] https://www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm