Regole telecomunicazioni dati nell'Europa digitale

a cura di
Giovanna De Minico e Marco Orofino

ESTRATTO

JOVENE

ISBN 9788824329897

JOVENE EDITORE
Via Mezzocannone 109 - 80134 NAPOLI
Tel. (+39) 081 552 10 19 / 12 74 / 34 71
www.jovene.it info@jovene.it

Stampato in Italia *Printed in Italy*

INDICE

MARCO OROFINO

LA TUTELA DEI DATI PERSONALI NELLE COMUNICAZIONI ELETTRONICHE: DALLA DIRETTIVA *E-PRIVACY* ALLA CRISI DEL MODELLO *E-PRIVACY*

1. *Introduzione*

La tutela dei dati personali e della vita privata nel settore delle comunicazioni elettroniche costituisce ormai da tempo un ambito particolarmente delicato nel quale interagiscono norme costituzionali nazionali dedicate alla tutela della riservatezza, disposizioni della Convenzione europea dei diritti dell'uomo, fonti primarie e atti di diritto derivato dell'Unione europea nonché discipline nazionali.

Sul piano interno, il diritto alla riservatezza non è esplicitamente menzionato come fattispecie autonoma in Costituzione, ma trova fondamento nelle norme costituzionali che tutelano la dignità della persona e la libertà individuale. Esso è tratto in via interpretativa ed estensiva da una lettura congiunta degli articoli 2, 3, 13, 14, 15 e 21 della Costituzione[1].

[1] La Corte costituzionale, a partire dalla sentenza n. 34 del 1973, ha affermato

Sul piano sovranazionale, nella Convenzione europea dei diritti dell'uomo (CEDU), come pure nella Carta dei diritti fondamentali dell'Unione Europea, la tutela della vita privata trova, invece, un riconoscimento espresso e autonomo: l'art. 8 CEDU garantisce il diritto al rispetto della vita privata e familiare[2], mentre gli articoli 7 e 8 della Carta garantiscono, rispettivamente la riservatezza e il diritto fondamentale alla protezione dei dati personali.

Tale intreccio di fonti – costituzionali, convenzionali e unionali – e, a cascata, la sovrapposizione di livelli normativi e istituzionali

---

che "la libertà e la segretezza della corrispondenza e di ogni altro mezzo di comunicazione costituiscono un diritto dell'individuo rientrante tra i valori supremi costituzionali (v., anche, sent. n. 366 del 1991) e che tale libertà ha una stretta attinenza al nucleo essenziale dei valori della personalità nel senso che è "parte necessaria di quello spazio vitale che circonda la persona e senza il quale questa non può esistere e svilupparsi in armonia con i postulati della dignità umana" (v. sentt. nn. 366 del 1991 e 10 del 1993). Da questo discende secondo la Corte un particolare vincolo interpretativo, diretto a conferire a quella libertà, per quanto possibile, un significato espansivo. Questo vincolo ad un'interpretazione espansiva comporta che vada riconosciuto il diritto alla riservatezza dei dati personali, quale manifestazione del diritto fondamentale all'intangibilità della sfera privata (sentenza n. 366 del 1991), così come il diritto di mantenere segreti tanto i dati che possano portare all'identificazione dei soggetti della conversazione, quanto quelli relativi al tempo e al luogo dell'intercorsa comunicazione (sentt. nn. 81 del 1993 e 372 del 2006, 20 del 2019 e 170 del 2023). Questa particolare *vis* espansiva trova un limite solo nel necessario bilanciamento tra la libertà individuale e l'interesse connesso all'esigenza di prevenire e reprimere i reati, vale a dire ad un bene anch'esso oggetto di protezione costituzionale (v. sentt. n. 34 del 1973 e, recentemente, n. 2 del 2023).

[2] La Corte di Strasburgo ha osservato che il concetto di "vita privata" è un termine ampio, non suscettibile di una definizione esaustiva ma che certamente si estende alla protezione dei dati personali riguardanti le informazioni relative alla salute di una persona (si veda Corte EDU, 25 febbraio 1997, *Z c. Finlandia*, n. 22009/93, § 71, Raccolta 1997-I), aspetti dell'identità fisica e sociale dell'individuo (Corte EDU, 7 febbraio 2002, *Mikulić c. Croazia*, n. 53176/99, § 53, CEDU 2002-I), l'identificazione di genere, il nome, l'orientamento sessuale e la vita sessuale (Corte EDU, 6 febbraio 2001, *Bensaid c. Regno Unito*, n. 44599/98, § 47, CEDU 2001-I; Corte EDU, 28 gennaio 2003, *Peck c. Regno Unito*, n. 44647/98, § 57, CEDU 2003-I). Molto importante è in questo senso Corte EDU (Grande Camera), 4 dicembre 2008, *S. and Marper c. Regno Unito*, nn. 30562/04 e 30566/04, in cui la Corte ha stabilito che la conservazione generalizzata e indiscriminata di dati di DNA e di impronte digitali viola l'art. 8 della CEDU. Il riferimento alle nuove tecnologie e ai dati da queste prodotte è continuato in tema di SMS (Corte EDU, 17 dicembre 2020, *Saber c. Norvegia*, n. 459/18 nonché Corte EDU, 5 settembre 2017, Grande Camera, *Bărbulescu c. Romania*, n. 61496/08) e di email (Corte EDU, 3 aprile 2007, *Copland c. Regno Unito*, n. 62617/00, CEDU 2007-I).

fanno del settore delle comunicazioni elettroniche un caso emblematico di costituzionalismo multilivello, nel quale si riflette la logica della governance multilivello tipica dell'ordinamento europeo[3].

Alla luce di tale quadro, il presente contributo si propone di analizzare in modo sistematico la normativa in materia di protezione dei dati nel settore delle comunicazioni elettroniche, con particolare riferimento al Regolamento (UE) 2016/679 (GDPR)[4] ed alla direttiva 2002/58/CE (direttiva *e-Privacy*)[5]. Inoltre si darà conto del tentativo di riforma della direttiva stessa nonché di alcune innovazioni apportate da altri atti appartenenti al c.d. decennio digitale europeo che incidono indirettamente sulla tutela della riservatezza e sulla disciplina del trattamento dei dati personali.

L'analisi si articolerà lungo tre direttrici principali.

In primo luogo, verrà ricostruita la genesi e l'ambito di applicazione della direttiva *e-Privacy*. In secondo luogo, si esaminerà il rapporto tra tale direttiva ed il GDPR, approfondendo i principali nodi interpretativi e applicativi. In terzo luogo si prenderanno in considerazioni le ipotesi di riforma della direttiva *e-Privacy* e le ragioni che hanno condotto la Commissione europea, nel 2025, ad abbandonare definitivamente il progetto nonché le conseguenze di tale stallo sulla capacità della normativa europea di far fronte alle nuove sfide tecnologiche e digitali che si prospettano all'orizzonte.

Sotto il profilo metodologico, la trattazione seguirà un approccio sistematico e giurisprudenziale, volto a evidenziare il dialogo tra le fonti e tra le Corti, nonché le implicazioni pratiche derivanti dalla frammentazione normativa e dalla mancata adozione di un quadro regolatorio unitario.

---

[3] Sia consentito sul tema rinviare a M. Orofino, *Profili costituzionali delle comunicazioni elettroniche nell'ordinamento multilivello*, Giuffrè, Milano, 2008.

[4] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati* (Regolamento generale sulla protezione dei dati - GDPR), in GUUE L 119 del 4.5.2016, p. 1 ss.

[5] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, *relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche* (direttiva sulla vita privata e le comunicazioni elettroniche), GU L 201 del 31.7.2002, p. 37-47.

2. *La genesi ibrida della direttiva 2002/58/CE a cavallo tra il settore della protezione dei dati personali ed il settore delle comunicazioni elettroniche*

La direttiva 2002/58/CE costituisce ancora oggi uno dei principali strumenti normativi di diritto derivato dell'Unione europea in materia di protezione dei dati personali.

In origine, la direttiva *e-Privacy* si collocava a cavallo tra due differenti *framework* normativi: da un lato quello delle comunicazioni elettroniche, disciplinato dal *Framework 2002* e imperniato sulla direttiva quadro 2002/21/CE[6]; dall'altro quello della protezione dei dati, fondato sulla Direttiva 95/46/CE[7].

Questa posizione intermedia tra il diritto delle comunicazioni e il diritto della protezione dei dati le conferiva una natura ibrida, al tempo stesso settoriale e trasversale che, se da un lato rifletteva l'intreccio sempre più stretto tra la regolazione delle reti e dei servizi di comunicazione elettronica e la tutela dei diritti fondamentali connessi al trattamento delle informazioni personali, da un altro lato, conduceva ad una sovrapposizione sostanziale, istituzionale e financo terminologica tra i due ambiti[8].

---

[6] Il *Framework 2002* si componeva di una direttiva quadro – la Direttiva 2002/21/CE (GU L 108 del 24.4.2002, p. 33-50 – e di quattro direttive speciali: la Direttiva accesso 2002/19/CE (GUUE L 108 del 24 aprile 2002, p. 7-20); la Direttiva autorizzazioni 2002/20/CE (GUUE L 108 del 24 aprile 2002, p. 21-32); la Direttiva sul servizio universale 2002/22/CE (GUUE L 108 del 24 aprile 2002, p. 51-77); e la Direttiva *e-Privacy* 2002/58/CE (GUUE L 201 del 31 luglio 2002, p. 37-47). Ad esse si affiancava la Decisione n. 676/2002/CE sullo spettro radio (GUUE L 108 del 24 aprile 2002, p. 1-6). V. per un'analisi dettagliata F. Donati, *L'ordinamento ammnistrativo delle comunicazioni*, Giappichelli, Torino, 2007; G. De Minico, *La sfida europea sulle telecomunicazioni: autori, regole, obiettivi*, in A. Pace, R. Zaccaria, G. De Minico (a cura di), *Mezzi di comunicazione e riservatezza. Ordinamento comunitario e ordinamento interno*, Jovene, Napoli, 2008, p. 153 ss., e, volendo, M. Orofino, *Profili costituzionali delle comunicazioni elettroniche nell'ordinamento multilivello*, cit.

[7] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, GU L 281 del 23.11.1995, p. 31-50. Sul rapporto tra la c.d. direttiva madre e la direttiva 2002/58/CE, v. F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46/CE al nuovo regolamento europeo*, Giappichelli, Torino, 2016, p. 130 ss.

[8] Questo intreccio si è accentuato, come si evince sin dall'intestazione, con l'approvazione della direttiva 2009/136/CE del 25 novembre 2009 *recante modifica della*

Con l'approvazione della direttiva (UE) 2018/1972, che ha istituito il Codice europeo delle comunicazioni elettroniche, questo intreccio si è parzialmente interrotto[9].

Il Codice ha, infatti, riunito e sostituito le quattro direttive del "pacchetto telecomunicazioni 2002", ma non la direttiva *e-Privacy*. L'art. 125 del Codice ha riconosciuto l'autonomia e la permanente vigenza della direttiva *e-Privacy* specificando come le norme codicistiche lasciano "impregiudicate le disposizioni (della direttiva) relative alla tutela della vita privata e dei dati personali nel settore delle comunicazioni elettroniche".

In precedenza, nel 2016 (ma con piena applicazione a far data da maggio 2018) il Regolamento UE 2016/679 aveva abrogato la direttiva 95/46/CE. La direttiva *e-Privacy* è rimasta in vigore mentre è cambiata la sua normativa generale di riferimento. Il passaggio dalla direttiva 95/46/CE al Regolamento (UE) 2016/679 segna non soltanto un mutamento di contenuti, ma soprattutto un profondo cambiamento nella struttura delle fonti del diritto europeo in materia di protezione dei dati[10].

Con l'abrogazione della direttiva e l'adozione del Regolamento, l'Unione ha infatti scelto di superare il modello basato sul recepimento nazionale, sostituendolo con uno strumento di applicazione

---

direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori. Tale normativa, infatti, insieme alla direttiva 2009/140/CE del Parlamento Europeo e del Consiglio del 25 novembre 2009 *recante modifica delle direttive 2002/21/CE che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica, 2002/19/CE relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate, e all'interconnessione delle medesime e 2002/20/CE relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica*, era parte del *Telecom Package* che ha modificato il *Framework* 2002. Le due normative sono state recepite con il d.lgs. n. 196 del 2003. Cfr. M. Orofino, *Il Telecom Package: luci ed ombre di una riforma molto travagliata*, in *Riv. it. dir. pubbl. com.*, n. 2, 2010, p. 514 ss.

[9] Sull'impatto di tale codificazione v. G. Gardini, *Il codice europeo delle comunicazioni elettroniche e l'impatto delle tecnologie sulla "dimensione di libertà" dei cittadini europei*, in *Studium Iuris*, n. 2, 2022, p. 135 ss.

[10] In proposito cfr. F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46/CE al nuovo regolamento europeo*, cit., spec. pp. 150-152.

diretta e uniforme in tutti gli Stati membri. Ne è derivato un rafforzamento dell'immediatezza e dell'omogeneità della tutela, nonché un ridimensionamento del margine di discrezionalità nazionale.

Tale scelta ha però generato un effetto collaterale di natura sistematica: la direttiva 2002/58/CE, rimasta in vigore come disciplina settoriale, si è trovata in una posizione inedita, divenendo *lex specialis* di un atto direttamente applicabile. In altri termini, oggi la relazione tra *e-Privacy* e GDPR non è solo di specialità materiale, ma anche di specialità formale inversa: una direttiva, che continua a richiedere trasposizione e adattamento nazionali, opera come norma speciale rispetto a un regolamento che ha portata generale e immediata.

Questo rovesciamento del rapporto tradizionale tra le fonti europee produce inevitabili tensioni applicative. Le disposizioni di recepimento della direttiva, in quanto fonti nazionali, si trovano a integrare – e talvolta a derogare – una fonte di rango sovraordinato direttamente efficace, con il rischio di compromettere la coerenza e l'uniformità della tutela nell'intero spazio giuridico europeo.

È in questa prospettiva che deve essere letta la funzione di ponte normativo che la direttiva 2002/58/CE avrebbe dovuto svolgere nel periodo di transizione post-GDPR: un atto ormai strutturalmente subordinato quanto alla tecnica legislativa, ma ancora essenziale per colmare le lacune settoriali del Regolamento in materia di comunicazioni elettroniche.

Questa situazione che, nel disegno complessivo della Commissione europea, avrebbe dovuto durare solo il tempo necessario all'approvazione di un nuovo regolamento in materia di *e-Privacy*, perdura tuttora. Il che determina, come si vedrà, sovrapposizioni e zone grigie nell'*enforcement* della normativa, specialmente in ambiti come la sicurezza delle reti, il trattamento dei dati di traffico e l'uso dei cookie e di altre tecnologie di tracciamento.

3. *L'ambito di applicazione ed i contenuti della direttiva* e-Privacy

Al fine di collocare correttamente le questioni aperte occorre partire ricordando che la direttiva *e-Privacy* è stata oggetto di due interventi normativi modificativi.

Il primo, piuttosto limitato, con la direttiva 2006/24/CE, c.d. direttiva *data retention*, dichiarata invalida dalla Corte di giustizia con sentenza dell'8 aprile 2014 (cause riunite C-293/12 e C-594/12), che regolamentava la conservazione (compresi i tempi) di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione[11]. Il secondo intervento normativo, piuttosto esteso, è avvenuto con la direttiva 2009/136/CE con l'obiettivo di aggiornarla al nuovo contesto tecnologico e rafforzare la tutela dei diritti degli utenti nel quadro del più ampio pacchetto telecomunicazioni del 2009.

La versione oggi consolidata è costruita attorno a un presupposto fondamentale ossia la necessità di garantire che lo sviluppo delle nuove tecnologie e dei servizi di comunicazione elettronica avvenga nel rispetto dei diritti e delle libertà fondamentali delle persone fisiche, in particolare del diritto alla riservatezza e alla protezione dei dati personali.

Questo è precisato nel par. 1, dell'art. 1, che fonda l'armonizzazione delle disposizioni nazionali sia sull'obiettivo di "assicurare un livello equivalente di tutela dei diritti e delle libertà fondamentali (…) con riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche" sia sulla necessità "di assicurare la libera circolazione di tali dati e delle apparecchiature e dei servizi di comunicazione elettronica all'interno della Comunità". Entrambi gli obiettivi sono da intendersi come indipendenti dalla tecnologia utilizzata per la trasmissione delle comunicazioni.

Per quanto riguarda il suo ambito di applicazione, l'art. 3 prevede che la direttiva *e-Privacy* si applichi al trattamento dei dati per-

[11] La direttiva 2006/24/CE introduceva all'articolo 15 della direttiva 2002/58/CE il paragrafo 1-*bis* che chiariva come le limitazioni al principio di riservatezza delle comunicazioni previste nell'art. 15, par. 1, non si applicassero ai dati la cui conservazione era imposta dalla direttiva 2006/24/CE sulla c.d. *data retention*. La clausola è rimasta tuttavia priva di applicazione sostanziale a seguito della dichiarazione di invalidità della direttiva 2006/24/CE da parte della Corte di giustizia. V. anche per gli effetti di tale pronuncia sulla norma italiana di recepimento, F. VECCHIO, *L'ingloriosa fine della Direttiva Data retention, la ritrovata vocazione costituzionale della Corte di giustizia e il destino dell'art. 132 del Codice della privacy*, in *www.dirittticomparati.it*, 12 giugno 2014.

sonali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche, comprese le reti di comunicazione pubbliche che supportano i dispositivi di raccolta e di identificazione dei dati.

Per servizi di comunicazione elettronica si intendono i servizi forniti di norma a pagamento, consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche. Ne sono un esempio i tradizionali servizi di telefonia fissa e mobile, comprensivi sia del traffico voce sia dei servizi SMS, così come i servizi di accesso a Internet forniti dai principali operatori commerciali attraverso reti a banda larga o ultra larga (ADSL, fibra ottica) oppure mediante reti mobili 4G e 5G. Possono essere ricompresi in questa categoria anche i servizi di connettività Wi-Fi pubblica offerti in luoghi aperti al pubblico, nonché i servizi di trasporto del segnale radiotelevisivo forniti su reti via cavo o satellitari, sempre nella misura in cui essi non riguardano i contenuti diffusi, ma esclusivamente l'infrastruttura di trasmissione. Allo stesso modo, devono considerarsi servizi accessibili al pubblico anche le attività di trasmissione di dati svolte dagli operatori che forniscono connettività o trasporto del segnale a utenti finali o ad altri operatori, purché tali prestazioni si risolvano nella messa a disposizione del mezzo trasmissivo.

Rimangono, invece, esclusi i servizi che, pur utilizzando reti pubbliche, forniscono principalmente contenuti o applicazioni – come i servizi di streaming, le piattaforme social, i servizi di posta elettronica basati sul web o le applicazioni di messaggistica OTT – poiché in questi casi l'elemento caratterizzante non è la trasmissione del segnale, ma il contenuto o la funzionalità erogata all'utente.

La nozione di reti di comunicazione pubbliche fa, a sua volta, riferimento a reti utilizzate interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico. Si tratta, dunque, delle reti telefoniche fisse e mobili gestite dagli operatori nazionali, delle reti a banda larga e ultra-larga che consentono l'accesso a Internet, nonché delle reti via cavo o satellitari impiegate per la diffusione e il trasporto dei segnali radiotelevisivi. Rientrano in questa categoria anche le reti di trasporto e dorsali in

fibra ottica messe a disposizione degli operatori per l'erogazione di servizi al pubblico, così come le infrastrutture Wi-Fi distribuite in luoghi aperti al pubblico – quali stazioni ferroviarie, aeroporti, biblioteche o piazze – ogniqualvolta esse siano utilizzate per fornire connettività a un numero indeterminato di utenti.

In questa prospettiva, devono considerarsi escluse dalla nozione di rete pubblica di comunicazione elettronica una serie di infrastrutture che, pur impiegate per il trasporto di segnali, non sono destinate all'erogazione di servizi di comunicazione elettronica al pubblico. Si tratta, innanzitutto, delle reti private realizzate per esigenze interne di soggetti pubblici o privati, come le intranet aziendali, le reti domestiche o le reti universitarie chiuse, il cui utilizzo è ristretto a una cerchia determinata di utenti e non è aperto all'accesso generalizzato del pubblico.

A queste si aggiungono le porzioni di rete gestite dai cosiddetti operatori OTT (Over-The-Top), le quali, pur coesistendo fisicamente con le reti pubbliche e spesso interconnesse con esse, non svolgono la funzione di fornire connettività agli utenti finali. Le infrastrutture degli OTT, quali le *Content Delivery Network*, i sistemi di caching distribuiti, i *data center* e le piattaforme *cloud*, hanno una funzione meramente interna al servizio digitale offerto e vengono utilizzate per ottimizzare la distribuzione dei contenuti o delle applicazioni. Esse si configurano quindi come reti non accessibili al pubblico, certamente destinate all'erogazione di servizi della società dell'informazione, ma, secondo la definizione adottata, non sottoposte alle regole della direttiva.

La direttiva è, quindi, ancorata ad una doppia distinzione tra servizi di comunicazione elettronica accessibili al pubblico (servizi di telefonia, ISP, provider di e-mail) e servizi privati (servizi intranet aziendali, servizi di messaggistica interna) e tra rete pubblica di comunicazione elettronica ossia infrastrutture di telecomunicazioni accessibili al pubblico quali reti telefoniche e reti internet e reti private ossia reti interne aziendali o domestiche, non accessibili al pubblico.

Sempre per quanto riguarda l'ambito di applicazione materiale occorre aggiungere che la direttiva *e-Privacy* si applica alle persone fisiche e, almeno in parte, anche alle persone giuridiche. Questo

perché talune norme riguardano gli abbonati ai servizi di comunicazione elettronica che possono evidentemente essere sia individui sia soggetti collettivi (imprese, associazioni, fondazioni etc.).

L'impianto normativo della direttiva *e-Privacy*, così come aggiornato dalla direttiva 2009/136/CE, si fonda oggi in particolare, su tre assi portanti:

a) la riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati sul traffico (articolo 5);

b) la sicurezza del trattamento con riferimento ai servizi accessibili al pubblico e alle reti pubbliche (articolo 4);

c) la regolamentazione dell'uso dei dati di traffico, dei dati di ubicazione e dei c.d. cookie (articoli 6 e 9, nonché articolo 5, paragrafo 3).

A queste tre macroaree si aggiungono gli interventi specifici e puntuali volti a tutelare gli utenti e riguardanti le comunicazioni indesiderate, gli elenchi abbonati e il trasferimento automatico della chiamata.

3.1. *Riservatezza delle comunicazioni e tutela dei dati di traffico e di ubicazione*

Il principio cardine della direttiva 2002/58/CE, sancito dall'articolo 5, è il diritto alla riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico.

La norma dispone che gli Stati membri provvedano a garantirlo attraverso la legislazione nazionale. Nel rinviare alle legislazioni nazionali, la norma europea specifica come debba essere vietata qualsiasi forma di intercettazione o sorveglianza delle comunicazioni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza il consenso degli utenti interessati. Esula dal divieto solo la memorizzazione tecnica necessaria alla trasmissione della comunicazione. Appare evidente come la norma costituisca oggi una specifica attuazione, per il settore delle comunicazioni elettroniche, del più ampio diritto al rispetto della vita privata e fa-

miliare dall'articolo 8 della CEDU, dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea. Un diritto sancito nella Costituzione italiana e in tutte le Costituzioni degli Stati membri, risultando pure ascrivibile alla categoria delle tradizioni costituzionali comuni[12].

La norma lascia inalterato l'equilibrio esistente tra il diritto dei cittadini alla vita privata e la possibilità per gli Stati membri di prendere i provvedimenti di cui all'articolo 15, paragrafo 1, della presente direttiva, necessari per tutelare la sicurezza pubblica, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) e l'applicazione della legge penale.

Il che significa che, se da un lato la direttiva *e-Privacy* non pregiudica la facoltà degli Stati membri di effettuare intercettazioni legali di comunicazioni elettroniche o di prendere altre misure, se necessario, per ciascuno di tali scopi, da un altro lato chiarisce come ciò debba avvenire conformemente all'art. 15 della direttiva stessa, che richiama in maniera quasi testuale le condizioni per restringere la libertà di comunicazione ai sensi della CEDU[13].

La giurisprudenza della Corte di giustizia dell'Unione europea ha progressivamente delineato una lettura rigorosa e sistematica dell'art. 15, par. 1, della direttiva 2002/58/CE, consolidando un

---

[12] Com'è noto, la Corte costituzionale con la sentenza n. 81 del 1993, nell'ambito di una pronuncia interpretativa di rigetto ha affermato che "la particolare disciplina predisposta dagli artt. 266-271 c.p.p. sulle intercettazioni … si applica soltanto a quelle tecniche che consentono di apprendere … il contenuto di una conversazione o di una comunicazione … e non sono, pertanto, estensibili a differenti forme di intervento nella sfera di riservatezza delle comunicazioni … né ad aspetti diversi da quello attinente al contenuto delle comunicazioni medesime". Pur non applicando gli artt. 266-271 c.p.p. ai dati di traffico in quanto tali, la Corte ha comunque ritenuto che anche tali dati rientrino nell'area di tutela dell'art. 15 Cost., ossia nella protezione della libertà e segretezza delle comunicazioni. In questo modo ha allargato l'ambito del diritto costituzionalmente tutelato in modo tale "da ricomprendere fra i propri oggetti anche i dati esteriori di individuazione di una determinata conversazione telefonica (identità dei soggetti, tempo e luogo della comunicazione stessa)".

[13] Occorre in proposito rammentare che la direttiva non poteva, nel momento in cui venne approvata, riferirsi direttamente alla Carta dei diritti fondamentali dell'UE che era stata proclamata nel contesto del Consiglio europeo di Nizza, il 7 dicembre 2020, ma senza entrare formalmente in vigore. La Carta è divenuta giuridicamente vincolante solo con l'entrata in vigore del Trattato di Lisbona il 1° dicembre 2009.

orientamento fortemente garantista in materia di conservazione e trattamento dei dati relativi alle comunicazioni elettroniche.

Fin dalle sentenze *Digital Rights Ireland* e *Tele2 Sverige*[14], la Corte ha chiarito che la direttiva *e-Privacy* costituisce attuazione diretta degli artt. 7 e 8 della Carta dei diritti fondamentali e che il principio generale di riservatezza delle comunicazioni, sancito dagli artt. 5, 6 e 9 della direttiva, impone agli Stati membri l'obbligo di garantire che comunicazioni e dati ad esse correlati non siano oggetto di archiviazione o trattamento da parte di terzi, salvo che ciò avvenga nel quadro di eccezioni strettamente circoscritte. L'art. 15, par. 1, è pertanto qualificato (*Commissioner of An Garda Síochána*, ptt. 40 e 57)[15]) come disposizione derogatoria, soggetta a interpretazione restrittiva, la cui applicazione non può trasformare l'eccezione in regola, pena lo svuotamento di contenuto del principio di riservatezza.

La Corte ha altresì riconosciuto che qualsiasi misura nazionale (dopo la dichiarazione di invalidità della norma europea) che imponga la conservazione dei dati relativi al traffico o all'ubicazione comporta un'ingerenza nei diritti fondamentali garantiti dagli artt. 7, 8 e 11 della Carta, indipendentemente dall'eventuale sensibilità dei dati o dal concreto uso che ne venga fatto (*Commissioner of An Garda Síochána*, ptt. 44-46 e *La Quadrature du Net*, 6 ottobre 2020, C-511/18, C-512/18 e C-520/18, ptt. 121-123)[16].

L'ingerenza è qualificata come particolarmente grave poiché tali dati sono idonei a rivelare aspetti altamente sensibili della vita privata degli individui, consentendo – anche attraverso trattamenti automatizzati – la ricostruzione dettagliata dei loro spostamenti, delle abitudini di vita, delle frequentazioni e delle relazioni sociali, fino alla formazione di veri e propri profili individuali (*La Quadrature du Net*, ptt. 117-118; *Tele2 Sverige*, ptt. 99-101). Ciò implica che le misure derogatorie devono rispettare il principio dello "stretto necessario", fondarsi su norme chiare, precise e giuridica-

[14] CGUE, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB e Secretary of State for the Home Department*.

[15] CGUE, 5 aprile 2022, causa C-140/20, *Commissioner of An Garda Síochána*, spec. parr. 40 e 57.

[16] CGUE, 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, *La Quadrature du Net e a.*

mente vincolanti e prevedere garanzie procedurali e materiali adeguate contro i rischi di abuso (*Digital Rights Ireland*, ptt. 54-69; *Commissioner of An Garda Síochána*, pt. 54).

Un ulteriore asse centrale della giurisprudenza riguarda la qualificazione degli obiettivi di interesse generale che possono legittimare tali deroghe. La Corte ha affermato che solo finalità di rango particolarmente elevato, come la salvaguardia della sicurezza nazionale, sono idonee a giustificare misure di conservazione generalizzata e indiscriminata dei dati (*La Quadrature du Net*, cit., ptt. 135-139; *Commissioner of An Garda Síochána*, pt. 58), e ciò esclusivamente in presenza di una minaccia grave, reale e attuale o prevedibile, accertata tramite controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente.

Per contro, negli ambiti della prevenzione, ricerca e repressione dei reati, solo la lotta ai reati gravi può giustificare ingerenze significativamente invasive, senza tuttavia consentire – secondo costante giurisprudenza – la conservazione generalizzata e indiscriminata dei dati di traffico e di ubicazione (*Tele2 Sverige*, ptt. 107-112; *La Quadrature du Net*, cit., ptt. 140-144; *Commissioner of An Garda Síochána*, cit., pt. 65; *VD e SR* 20 settembre 2022 C-339/20 e C-397/20[17]).

Al di fuori del perimetro ristretto della sicurezza nazionale, la Corte ammette esclusivamente forme meno intrusive di conservazione dei dati. Tra queste rientrano: la conservazione mirata, delimitata secondo criteri oggettivi e non discriminatori relativi alle categorie di persone interessate o al contesto geografico (*La Quadrature du Net*, ptt. 150-152); la conservazione generalizzata e indiscriminata degli indirizzi IP assegnati all'origine della connessione, per un periodo limitato allo stretto necessario (*La Quadrature du Net*, pt. 150); la conservazione generalizzata dei dati identificativi di base degli utenti (*Tele2 Sverige*, cit., pt. 157); e la conservazione rapida ("quick freeze") disposta mediante ordine giudiziario o dell'autorità competente (*La Quadrature du Net*, cit., pt. 159).

Complessivamente, la Corte ha così sviluppato un sistema coerente che, pur riconoscendo obblighi positivi degli Stati nella tutela

[17] CGUE, 20 settembre 2022, cause riunite C-339/20 e C-397/20, *VD* e *SR*.

della sicurezza e nella protezione delle persone vulnerabili, preserva il primato del principio di riservatezza delle comunicazioni e circoscrive con rigore le condizioni che possono giustificare deroghe, confermando una lettura dell'art. 15, par. 1, ancorata a un elevato livello di tutela dei diritti fondamentali.

Un punto assai interessante che emerge tanto dal dato normativo che da quello giurisprudenziale è che la direttiva *e-Privacy* riconosce che la riservatezza delle comunicazioni implica non soltanto la protezione del contenuto della comunicazione, ma anche dei dati relativi al traffico.

Si tratta dei dati che accompagnano la comunicazione e che sono ritenuti anch'essi idonei a rivelare aspetti essenziali della vita privata degli individui potendo infatti consentire un'accurata ricostruzione di relazioni sociali, spostamenti geografici, abitudini di vita, preferenze anche intime dell'utente, e quindi incidere in modo profondo sulla sua sfera personale.

La definizione normativa di tali dati ai sensi della direttiva è piuttosto concisa per cui si tratterebbe di "qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione". Questi dati comprendono, ad esempio: l'origine e la destinazione della comunicazione (numeri chiamante e chiamato, indirizzi IP, ecc.); la data, l'ora, la durata e il tipo di comunicazione; l'apparecchiatura utilizzata (es. IMEI, indirizzi MAC); la posizione del dispositivo al momento della comunicazione.

Essi sono nel linguaggio tecnico i c.d. metadati ossia le informazioni che descrivono il flusso delle comunicazioni su una rete, ma non specificamente il contenuto puntuale della medesima.

3.2. *Sicurezza delle reti e dei servizi di comunicazione*

Accanto al principio di riservatezza delle comunicazioni, la direttiva 2002/58/CE attribuisce un ruolo centrale al tema della sicurezza dei dati e delle reti.

L'art. 4, par. 1, impone ai fornitori di servizi di comunicazione elettronica accessibili al pubblico l'obbligo di adottare misure tecniche e organizzative adeguate a salvaguardare la sicurezza dei pro-

pri servizi, nel caso congiuntamente con il fornitore della rete pubblica di comunicazione, assicurando un livello di protezione proporzionato al rischio. Un rischio che deve essere parametrato sulla rete e sul servizio utilizzato così come sui dati trattati.

Il par. 1-*bis* identifica le misure minime di sicurezza prevedendo che i fornitori delle reti e dei servizi debbano quanto meno: *a*) garantire che i dati personali siano accessibili solo al personale autorizzato; *b*) tutelare i dati personali archiviati e trasmessi tanto dalla distruzione e dalla alterazione (siano esse accidentali o meno) quanto da archiviazione, trattamento, accesso o divulgazione non autorizzata; *c*) garantire l'attuazione di una politica di sicurezza. Con riferimento a tali misure minime così come ad altre adottate il compito di controllarne il rispetto è posto in capo all'Autorità indipendente competente.

Nell'ottica di garantire una maggiore trasparenza e comprensione dei rischi, i parr. 2 e 3 dell'art. 4 impongono anche al fornitore di un servizio di comunicazione elettronica un doppio obbligo di notifica. Il primo nel caso in cui rilevino un particolare rischio di violazione della sicurezza della rete pubblica. Il secondo nel caso in cui si verifichi effettivamente un *data breach*. In entrambi i casi la notifica deve essere effettuata innanzitutto a favore dell'Autorità competente e solo nei casi più gravi anche a favore degli abbonati o di altra persona coinvolta.

Si tratta di un precedente significativo rispetto al modello generale di notifica dei *data breach* poi previsto dal Regolamento (UE) 2016/679 (articoli 33 e 34). La direttiva *e-Privacy* ha dunque, in questo caso, anticipato, ancorché in ambito settoriale, l'esigenza di garantire trasparenza e tempestività nella gestione degli incidenti di sicurezza, ponendo le basi per un approccio sistemico alla *cybersecurity* come componente della protezione dei dati personali.

La nozione di sicurezza impiegata dalla direttiva assume un significato ampio e multilivello.

Essa include non solo la sicurezza tecnica delle infrastrutture (riservatezza, integrità e disponibilità dei dati), ma anche la prevenzione di accessi non autorizzati, intercettazioni o alterazioni delle comunicazioni, nonché la protezione contro la perdita o la distruzione accidentale dei dati. In questo senso, la sicurezza si configura

come una dimensione funzionale del diritto alla riservatezza, piuttosto che come un ambito autonomo: non si limita a un obbligo tecnologico, ma costituisce un presupposto necessario per l'effettività del diritto fondamentale alla protezione dei dati personali nelle comunicazioni elettroniche.

L'articolo 4 presenta, inoltre, un profilo di governance multilivello, poiché richiede la collaborazione tra i diversi attori del sistema: operatori di rete, fornitori di servizi, autorità di regolazione nazionali e autorità di protezione dei dati. In Italia, ad esempio, la cooperazione tra l'Autorità per le garanzie nelle comunicazioni (AGCOM), il Garante per la protezione dei dati personali e l'Agenzia per la cybersicurezza nazionale (ACN) evidenzia la dimensione interistituzionale della sicurezza dei servizi digitali.

La progressiva convergenza tra protezione dei dati personali e sicurezza informatica si riflette oggi anche nel nuovo quadro europeo: la direttiva *e-Privacy* convive, infatti, con la Direttiva (UE) 2022/2555 (NIS 2), che definisce obblighi di sicurezza e di notifica a carico di un'ampia gamma di soggetti operanti nei settori critici e nei servizi digitali essenziali tra cui specificamente i fornitori di reti pubbliche e i fornitori di servizi di comunicazione elettronica accessibili al pubblico. Tali obblighi si aggiungono a quelli previsti dalla direttiva *e-Privacy*. Questo, pur confermando che la sicurezza delle reti non è più un mero requisito tecnico, ma un elemento strutturale della *governance* europea del rischio digitale, determina una sovrapposizione di obblighi meritevole di attenzione[18].

3.3. *La regolamentazione dell'uso dei dati di traffico, dei dati di ubicazione e dei c.d. cookies*

La terza macroarea su cui interviene la direttiva *e-Privacy* è la regolamentazione dell'uso dei dati di traffico, dei dati di ubicazione e dei c.d. cookie.

---

[18] V. per un'analisi complessiva di tali strumenti e per l'emersione di una nuova dimensione della cybersecurity, E. LONGO, *La disciplina della cybersecurity nell'Unione europea e in Italia*, in *La regolazione europea della società digitale*, cit., p. 203 e ss.; M. PIETRANGELO, *La dimensione plurale della cybersicurezza: da potere invisibile a processo collaborativo*, in *Rivista Italiana di Informatica e Diritto*, 2, 2024, p. 13 e ss. La natura

Per quello che attiene ai dati di traffico, l'articolo 6 della direttiva *e-Privacy* definisce in modo puntuale le condizioni e i limiti entro i quali i fornitori di reti pubbliche o di servizi di comunicazione elettronica possono, in quanto titolari, trattare i dati degli utenti e/o degli abbonati.

Il par. 1 dell'art. 6, dispone la regola generale per cui essi devono essere cancellati o resi anonimi non appena cessano di essere necessari per garantire la trasmissione della comunicazione. Questa previsione è certamente in linea con il principio di finalità del trattamento inteso in senso stretto.

A questa previsione si accompagnano alcune limitate eccezioni.

La prima eccezione riguarda la possibilità di continuare a trattare i dati necessari ai fini della fatturazione per l'abbonato e dei pagamenti di interconnessione. Questo, specifica la norma, è legittimo solo sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento. In ogni caso, comunque, l'abbonato o l'utente devono essere informati sulla natura dei dati relativi al traffico che sono sottoposti a trattamento e sulla durata del trattamento per le finalità su esposte.

La seconda eccezione è per i trattamenti connessi alla conservazione dei dati al fine della salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica nonché della prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. In questo caso, dopo che la Corte di giustizia ha dichiarato l'invalidità della direttiva *data retention* sono gli Stati membri a definire i termini di conservazione di tali dati.

La terza eccezione, introdotta nel 2009, riguarda il trattamento dei dati ai fini della commercializzazione dei servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto. Il par. 3 dell'art. 6 prevede che il fornitore di un servizio di comuni-

---

di direttiva di tali strumenti implica una loro trasposizione sul piano interno. V. in proposito A. Iannuzzi, *Considerazioni sul disegno di legge «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici» (AC 1717)*, in *Rivista Italiana di Informatica e Diritto*, 1, 2024, p. 59 ss.

cazione elettronica accessibile al pubblico possa trattare i dati nella misura e per la durata necessaria per siffatti servizi, o per la commercializzazione, alla condizione esclusiva che l'abbonato o l'utente a cui i dati si riferiscono abbiano espresso preliminarmente il proprio consenso. Così come lo hanno prestato, specifica la disposizione, agli abbonati o agli utenti deve essere consentita la possibilità di ritirare il loro consenso al trattamento dei dati relativi al traffico in qualsiasi momento.

Per ognuna delle citate eccezioni, resta inteso che l'attività di trattamento deve essere sempre effettuata da personale specificamente autorizzato, nel rispetto del principio di stretta necessità e delle garanzie di sicurezza e riservatezza previste dal diritto europeo. Inoltre, la normativa riconosce alle autorità competenti la possibilità di accedere ai dati di traffico soltanto nei casi previsti dalla legge, in particolare per la risoluzione di controversie in materia di interconnessione e fatturazione o per esigenze di giustizia e sicurezza pubblica.

Analogamente, l'articolo 9 disciplina l'uso dei dati di ubicazione – ossia delle informazioni diverse dai dati di traffico che indicano la posizione geografica degli utenti o degli abbonati di reti e servizi di comunicazione elettronica – quando tali dati non sono strettamente necessari alla trasmissione della comunicazione stessa.

Il par. 1 dell'art. 9 prevede che il loro trattamento, nei limiti e per la durata strettamente necessari alla fornitura di un servizio a valore aggiunto, sia lecito solo se essi siano resi anonimi, fuoriuscendo dunque dal perimetro di applicazione della norma in materia di dati personali, o dietro consenso esplicito e previamente informato dell'utente o dell'abbonato.

Il consenso al trattamento deve essere in ogni momento revocabile sia in via definitiva, come è nella logica, sia, in questo caso, in via provvisoria. In proposito, il par. 2 dell'art. 9 prevede che l'utente e l'abbonato devono avere la possibilità "di negare, in via temporanea, mediante una funzione semplice e gratuitamente, il trattamento di tali dati per ciascun collegamento alla rete o per ciascuna trasmissione di comunicazioni".

L'impianto complessivo della direttiva riflette quindi un modello di tutela preventiva, fondato sull'idea che la protezione della

riservatezza debba operare non *ex post*, ma al momento stesso della generazione e della trasmissione dei dati.

Infine, *per quanto riguarda la regolazione dei c.d. cookies*, l'articolo 5, paragrafo 3, introduce (dopo la riforma del 2009) una specifica disciplina per l'uso di tecnologie di memorizzazione o di accesso a informazioni nei terminali degli utenti[19].

Fanno eccezione soltanto i casi in cui l'archiviazione o l'accesso ai dati siano "strettamente necessari" per effettuare la trasmissione di una comunicazione o per fornire un servizio esplicitamente richiesto dall'utente (ad esempio, *cookies* tecnici di sessione o di bilanciamento del carico).

La c.d. "cookie rule" prevede che gli Stati membri garantiscano che la memorizzazione di informazioni o l'accesso a informazioni già memorizzate nel terminale di un utente siano consentiti solo a condizione del soddisfacimento di una duplice condizione ovvero che

a) l'utente abbia ricevuto informazioni chiare e complete in conformità con la direttiva 95/46/CE (oggi ai sensi del GDPR), e

b) abbia espresso il proprio consenso in modo preventivo.

Questa disposizione, apparentemente tecnica, ha assunto nel tempo una portata centrale nel dibattito sulla protezione dei dati online.

La Corte di giustizia dell'Unione europea, nella nota sentenza *Planet49 GmbH* (C-673/17, 2019), ha chiarito che il consenso richiesto dall'articolo 5, paragrafo 3, deve essere libero, specifico, informato e inequivocabile[20]. La Corte ha altresì precisato che il consenso deve essere attivo: non è cioè valido un consenso prestato mediante caselle preselezionate o con formule di *opt-out*; che il consenso deve essere espresso con un'azione positiva inequivocabile (ad esempio, la selezione esplicita di un'opzione); e che la regola si applica indipendentemente dalla natura dei dati memorizzati, anche se non contengono informazioni personali identificabili, poiché, in

[19] I *cookies* sono file che il fornitore di un sito web installa nel computer dell'utente di tale sito e ai quali il fornitore può nuovamente accedere durante una nuova visita del sito da parte dell'utente, per facilitare la navigazione in Internet o transazioni oppure al fine di ottenere informazioni sul comportamento dell'utente.

[20] CGUE, 1° ottobre 2019, causa C-673/17, *Planet49 GmbH.*

questo caso, il semplice accesso al terminale costituisce un'ingerenza nella sfera privata dell'utente. Di qui l'estensione della norma anche ai dati non personali.

Tali principi sono stati ulteriormente sviluppati dal Comitato europeo per la protezione dei dati (EDPB) nelle Linee guida 5/2020 sul consenso e, più recentemente, nelle Linee guida 2/2023 sull'articolo 5, paragrafo 3, della direttiva *e-Privacy*.

Innanzitutto, l'EDPB ha chiarito attraverso i due interventi che la norma non si limita ai soli *cookies* tradizionali bensì a qualsiasi tecnologia di memorizzazione o accesso che consenta di leggere o scrivere dati sul terminale dell'utente, come ad esempio: identificatori anonimi di pubblicità mobile[21], tecniche di browser finger printing, strumenti di tracciamento cross-device, Software Development Kit (SDK) integrati nelle applicazioni mobili[22], tecniche di rilevamento via Wi-Fi o Bluetooth.

In secondo luogo, il Comitato ha offerto una lettura estremamente restrittiva del criterio della necessità tecnica e, dunque delle ipotesi in cui il consenso preventivo ed informato dell'utente non è richiesto. Nello specifico ha affermato che sono "strettamente necessarie" solo quelle tecnologie di memorizzazione e accesso che sono strettamente indispensabili al funzionamento del servizio. Quelle cioè senza le quali il servizio non potrebbe funzionare. Ogni altra tecnologia – anche se utile a fini statistici o per il miglioramento dell'esperienza utente – richiede sempre il consenso preventivo.

In terzo luogo, l'EDPB ha sottolineato come la disciplina del consenso sia strettamente connessa anche ai meccanismi di *design* e di interfaccia. A tal proposito il Comitato, seguendo le sollecitazioni delle autorità nazionali (in particolare la CNIL francese e il Garante

[21] Un advertising ID è un identificatore univoco e anonimizzato dell'utente. Si tratta di una combinazione di lettere e numeri assegnata a un dispositivo, come uno smartphone, un computer o un tablet. I più noti sono al momento gli *Apple's Identifier for Advertisers* (IDFA), i *Google's Advertising Identifier* (GAID) e gli *Amazon Advertising ID*.

[22] Gli SDK (*Software Development Kit*) integrati nelle applicazioni mobili sono insiemi di strumenti, librerie e componenti software forniti da terze parti o dallo stesso sviluppatore della piattaforma che vengono inseriti all'interno di un app per aggiungere funzionalità senza doverle programmare da zero. Essi possono comportare raccolta di dati, tracciamento degli utenti, o influenzare performance e sicurezza dell'app.

italiano[23]) ha ribadito che *cookie wall*, *scrolling* o navigazione implicita non possono costituire forme valide di consenso, in quanto non garantiscono in modo effettivo la libertà di scelta. Inoltre il consenso deve poter essere rifiutato o revocato con la stessa facilità con cui è prestato, e le opzioni devono essere chiare, simmetriche e prive di pressioni o incentivi indebiti.

Da quanto qui ricostruito può dirsi che sotto il profilo sistematico, la "cookie rule" evidenzia in modo emblematico la complessa interazione tra diritto della protezione dei dati ed architettura tecnologica. Essa incarna plasticamente l'idea che la protezione dei dati non si esaurisca in un problema di liceità del trattamento, ma riguardi *hardware*, *middleware* e *software* nella misura in cui governano anche il controllo dell'accesso ai dispositivi e alle informazioni che essi contengono.

In altri termini, l'articolo 5, paragrafo 3, sposta il baricentro della tutela dalla "circolazione dei dati" alla protezione dell'ambiente digitale personale dell'utente, anticipando quella che oggi viene, comunemente, definita una prospettiva di protezione dei dati *by design*.

3.4. *Altre questioni di interesse e profili trasversali della direttiva* e-Privacy

Oltre alle tre direttrici fondamentali – riservatezza delle comunicazioni, sicurezza delle reti e dei servizi, e trattamento dei dati di traffico, ubicazione e terminali – la direttiva 2002/58/CE presenta una serie di profili ulteriori di interesse, che ne completano il quadro sistematico. Si tratta di regole relative agli elenchi abbonati, al trasferimento di chiamata, alla fatturazione e alle comunicazioni indesiderate.

Proprio la *disciplina delle comunicazioni indesiderate a fini commerciali* di cui all'art. 13, della direttiva merita una particolare attenzione in quanto rappresenta uno dei primi interventi organici del legislatore europeo di intervenire in materia di marketing di-

[23] V. in proposito le *Linea Guida cookie e altri strumenti di tracciamento* adottate dal Garante per la Protezione dei Dati Personali il 10 giugno 2021, pubblicate sulla G.U. n. 163 del 9 luglio 2021.

retto elettronico. In questo senso, l'intervento normativo europeo realizzato con la direttiva *e-Privacy* costituisce un passaggio fondamentale nel processo di costruzione di un sistema di tutela della riservatezza nelle comunicazioni digitali.

La norma introduce al par. 1, dell'art. 13 il principio generale del consenso preventivo (c.d. *opt-in*), prevedendo che l'uso di strumenti automatizzati di comunicazione – quali ad esempio dispositivi di chiamata senza operatore, telefax o posta elettronica – per finalità promozionali sia consentito esclusivamente nei confronti di quegli utenti o abbonati che abbiano espresso preliminarmente il loro consenso rispetto allo specifico trattamento dei loro dati di contatto.

La previsione del consenso come unica condizione di legittimità è la prova del fatto che il "legislatore" europeo ha inteso riconoscere all'utente un potere effettivo di autodeterminazione rispetto alla ricezione di messaggi pubblicitari.

Accanto alla regola generale dell'*opt-in*, il par. 2 del medesimo articolo introduce una deroga limitata, nota come c.d. *soft spam*, che consente al fornitore di utilizzare l'indirizzo elettronico del cliente, acquisito nel contesto di una precedente vendita o trattativa commerciale, per promuovere prodotti o servizi analoghi, a condizione che l'interessato sia stato informato in modo chiaro e trasparente e che gli sia garantita in ogni momento la possibilità di opporsi gratuitamente al trattamento dei propri dati per tali finalità.

Questa eccezione, di natura strettamente funzionale, risponde all'esigenza di bilanciare la libertà di iniziativa economica con la tutela dei diritti degli utenti, evitando che la disciplina si traduca in un ostacolo sproporzionato per le attività legittime di comunicazione commerciale. Inoltre, il fatto che la disposizione si limiti ai contatti via email risponde all'obiettivo di minimizzare l'intrusione nella vita privata che, invece, si verifica attraverso la ricezione di chiamate o messaggi indesiderati.

Per quanto riguarda i casi non rientranti nel par. 1 – ossia senza l'uso di strumenti automatici – né nel par. 2 riguardante il c.d. soft spam, l'art. 13 della direttiva consente agli Stati membri un margine di discrezionalità per determinare se adottare un regime di *opt-in* (comunicazioni consentite solo previo consenso) oppure di *opt-out* (comunicazioni vietate solo in presenza di un'esplicita opposizione).

Quale che sia l'opzione prescelta, il legislatore nazionale deve assicurare che le comunicazioni indesiderate possano essere rifiutate senza oneri per l'utente e che siano vietate pratiche scorrette, quali la falsificazione dell'identità del mittente o l'invio di messaggi privi di un indirizzo valido per l'esercizio del diritto di opposizione.

Infine, la disposizione europea prevede meccanismi di tutela giurisdizionale e amministrativa, riconoscendo a chiunque abbia subito un pregiudizio – ivi compresi i fornitori di servizi di comunicazione elettronica – il diritto di promuovere un'azione per far cessare o vietare le violazioni della disciplina. In tal modo, l'articolo 13 concretizza, in un settore specifico, il principio di autodeterminazione informativa dell'individuo, anticipando concetti e strumenti di tutela che saranno successivamente formalizzati e ampliati dal Regolamento (UE) 2016/679 (GDPR). La norma assume pertanto un valore paradigmatico nell'evoluzione del diritto europeo delle comunicazioni elettroniche, segnando il passaggio da una logica meramente economico-concorrenziale a una visione centrata sulla protezione dei diritti fondamentali e sulla responsabilizzazione dei titolari del trattamento nell'ambito delle pratiche di marketing digitale.

In conclusione, come si evince dall'analisi delle tre macroaree d'intervento nonché della disciplina sulle c.d. comunicazioni commerciali, la direttiva 2002/58/CE si configura come un atto di diritto derivato ibrido e settoriale, che ha però anticipato molti principi ed istituti poi consolidatisi nel GDPR, ma che oggi risente dei limiti del suo impianto originario e della frammentazione derivante dai diversi recepimenti nazionali. Queste criticità, insieme alla rapida evoluzione tecnologica e al mutato ecosistema digitale, costituiscono le premesse per comprendere le ragioni dei tentativi di riforma e, al tempo stesso, i motivi del loro fallimento, temi che saranno approfonditi nel paragrafo successivo.

4. *Il rapporto tra la direttiva* e-Privacy *e il GDPR: specialità e integrazione*

Nel sistema europeo di tutela dei dati personali, la direttiva 2002/58/CE e il Regolamento (UE) 2016/679 intrattengono un rap-

porto di specialità e complementarità funzionale, non di successione.

Gli artt. 94 e 95 del GDPR chiariscono oggi questi rapporti.

In primo luogo, l'art. 94 del GDPR, dopo aver stabilito al primo comma, l'abrogazione della direttiva 95/46/CE a far data dall'applicazione del GDPR, nel secondo comma specifica che i riferimenti ed i rinvii che la direttiva *e-Privacy* fa alla direttiva 95/46/CE si intendono fatti, dopo l'abrogazione di quest'ultima, al GDPR.

In secondo luogo, l'art. 95 GDPR stabilisce che il Regolamento non impone alle persone fisiche e alle persone giuridiche obblighi supplementari nelle materie per le quali sono soggetti a obblighi specifici fissati dalla direttiva 2002/58/CE (e recepiti sul piano nazionale) a patto che le norme eventualmente sovrapponibili siano ispirate dal medesimo fine.

Le due norme del GDPR perseguono tre obiettivi che devono guidare l'interpretazione nei casi in cui si verifica una sovrapposizione di norme.

Il primo obiettivo è evitare una duplicazione di oneri regolamentari[24].

Il secondo obiettivo è confermare che tra le due fonti si applica, nei casi in cui vi sia sovrapposizione di norme adottate per perseguire gli stessi fini, il criterio di specialità: il Regolamento, prendendo il posto della direttiva 95/46/CE è la nuova norma generale, mentre la direttiva *e-Privacy* rimane la norma speciale.

Il terzo obiettivo è quello di rendere manifesto che, se non c'è sovrapposizione né contrasto tra le due normative europee, la direttiva *e-Privacy* può anche integrare il Regolamento.

Non può sfuggire però come il confine tra prevalenza ed integrazione sia sottile, rimesso come è all'individuazione di obiettivi comuni o meno nel caso di sovrapposizioni normative. Inoltre, non si può dimenticare che il rapporto che in precedenza si ribaltava, completamente, sulle fonti di trasposizione interna, ora crea un'interessante asimmetria perché si instaura tra una fonte regolamen-

[24] Si veda il caso degli obblighi di notifica dei *data breaches* che sono disciplinati in entrambi gli atti normativi.

tare europea (il GDPR) e le fonti nazionali di trasposizione della direttiva adottate dagli Stati membri[25].

Proprio al fine di sciogliere le possibili criticità, l'EDPB ha adottato il Parere n. 5 del 2019[26]. Il Comitato nel definire il rapporto tra le due normative ha parlato di precisazione (specialità) ed integrazione.

Le aree di sovrapposizione che occorre specificamente osservare sono ben note. Esse riguardano:

a) il trattamento dei dati di comunicazione (traffico, ubicazione, metadati);

b) l'uso dei terminali e delle tecnologie di tracciamento (cookie, identificatori pubblicitari, *fingerprinting*);

c) le comunicazioni promozionali automatizzate e il marketing diretto.

I casi più noti di precisazione, e quindi di applicazione del criterio di specialità, riguardano le condizioni di legalità del trattamento. In questo caso la *lex generalis* è l'art. 6 del GDPR che individua le basi giuridiche del trattamento dei dati personali, cioè le condizioni che rendono lecito il trattamento. La norma come noto individua accanto al consenso altre cinque basi legali tra cui vi sono l'esecuzione di un contratto, l'obbligo legale, la salvaguardia degli interessi vitali, l'esecuzione di pubblici poteri e il legittimo interesse del titolare purché non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato.

La direttiva *e-Privacy* richiede, invece, *ex* artt. 5, 6 e 9 il consenso esplicito e preliminare dell'interessato per i trattamenti che consistono nell'archiviazione o accesso ai dispositivi degli utenti, per il trattamento dei dati di traffico, per i trattamenti dei dati rela-

---

[25] Come evidenziato dal Garante europeo della protezione dei dati (EDPS), la permanenza di una direttiva come fonte speciale rispetto a un regolamento direttamente applicabile genera una anomalia strutturale. Cfr. *Opinion 6/2017 on the Proposal for a Regulation of Privacy and Electronic Communications (e-Privacy Regulation).*

[26] EDPB, *Opinion 5/2019 on the interplay between the e-Privacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities* (12 March 2019). Cfr. C. Etteldorf, *EDPB on the interplay between the e-Privacy Directive and the GDPR*, in *European Data Protection Law Review (EDPL)*, 2019, vol. 5, n. 2, pp. 224-231.

tivi all'ubicazione. In questi casi, in quanto *lex specialis* la direttiva *e-Privacy*, e gli atti nazionali di recepimento prevalgono sul GDPR. Il che significa che né il fornitore di una rete pubblica né il fornitore di un servizio accessibile al pubblico possono ricorrere al contratto o all'interesse legittimo come base legale del trattamento.

Questo determina un'evidente asimmetria oggi rispetto ad alcuni fornitori di servizi di comunicazione c.d. *overthetop* che offrono servizi di comunicazione ormai ampiamente sostitutivi rispetto quelli forniti dai fornitori di servizi di comunicazione elettronica.

Per quanto riguarda l'integrazione tra le norme del GDPR e quelle della direttiva *e-Privacy* si pensi alle numerose disposizioni di quest'ultima che hanno lo scopo proteggere gli "abbonati" ad un servizio di comunicazione elettronica accessibile al pubblico.

Come noto, l'ambito di applicazione del GDPR riguarda i dati personali delle sole persone fisiche laddove invece la precedente direttiva consentiva agli Stati membri di estendere la protezione alle persone giuridiche.

Gli abbonati a un servizio di comunicazione elettronica accessibile al pubblico possono essere, come la direttiva *e-Privacy* specifica, sia persone fisiche che persone giuridiche. La direttiva *e-Privacy*, integra in questo caso la tutela che il GDPR offre ai diritti fondamentali delle persone fisiche e in particolare il loro diritto alla vita privata, con la tutela degli interessi legittimi delle persone giuridiche.

Lo stesso accade per la c.d. *cookie rule* di cui all'art. 5 della direttiva *e-Privacy*. Le norme ivi contenute si applicano, come precisato dalla Corte di giustizia, anche ai dati che non consentono l'identificazione della persona a cui si riferiscono e che, dunque, ai sensi del GDPR non sono dati personali e, quindi fuoriescono dal perimetro dell'intervento regolamentare.

Vi sono poi casi, come ad esempio, per ciò che riguarda le misure di sicurezza in cui specialità ed integrazione si sovrappongono. Da un lato, la direttiva *e-Privacy* richiede al fornitore di reti o servizi di comunicazione elettronica l'adozione di specifiche misure di sicurezza, secondo una logica che in parte richiama quella della direttiva 95/46/CE e, dall'altro lato, il GDPR impone loro di definire

le misure di sicurezza necessarie sulla base di una valutazione del rischio.

In questo si vede in modo evidente come la direttiva *e-Privacy*, adottata in un contesto tecnologico precedente all'entrata in vigore del Regolamento, continui a disciplinare il trattamento dei dati personali nel settore nelle comunicazioni elettroniche, dentro il modello normativo precedente che pure ha contribuito in alcuni casi a superare.

Un ulteriore profilo critico in cui sono possibili deleterie sovrapposizioni è quello del regime di *enforcement*.

Il GDPR prevede che le Autorità nazionali di controllo (e il Comitato europeo di protezione dei dati) siano i bracci armati del regolamento al fine di garantirne un'attuazione uniforme[27]. Esse, garantite da una posizione di indipendenza, hanno poteri trasversali (cioè su ogni trattamento dati) molto ampi ed incisivi al fine *ex* art. 51, par. 1 di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione. Rispetto a questa competenza generale, le limitazioni o le deroghe sono formulate in modo esplicito.

Ad esempio, il Regolamento stesso identifica un'eccezione per i trattamenti di dati personali effettuati dalle autorità giurisdizionali nell'esercizio delle loro funzioni giurisdizionali (articolo 55, paragrafo 3) e una possibilità di derogare a questo mandato per i trattamenti effettuato a scopi giornalistici o di espressione accademica, artistica o letteraria (articolo 85).

La direttiva *e-Privacy* non contiene al suo interno disposizioni analoghe. L'art. 15-*bis*, introdotto nel 2009 e rubricato *Attuazione e controllo dell'attuazione* si limita a specificare che gli Stati membri debbano garantire che l'autorità nazionale competente e, se del caso, altri organismi nazionali dispongano dei poteri per far cessare le violazioni così come delle risorse e delle competenze necessarie. A questa previsione si aggiungono solo una pluralità di rinvii all'autorità nazionale di regolazione, c.d. ANR disciplinata dalla direttiva

[27] Così F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati*. II. *Il Regolamento europeo 2016/679*, Giappichelli, Torino, 2016, p. 103.

quadro 2002/21/CE, come "l'organismo o gli organismi incaricati da uno Stato membro di svolgere le funzioni di regolamentazione fissate dalla presente direttiva e dalle direttive particolari"[28]. La direttiva *e-Privacy* letta alla luce della direttiva 2002/21/CE lasciava dunque agli Stati il compito di ripartire i compiti di sorveglianza tra le Autorità di regolazione nel settore delle comunicazioni elettroniche e le autorità di protezione dei dati. Nella quasi totalità degli Stati membri si è optato per una suddivisione tra diverse Autorità. Il che ha ovviamente generato non poche sovrapposizioni ed incertezze nella *governance* ed ha inciso negativamente sulla coerenza applicativa[29].

Il punto in questione è quindi se, nell'ambito dei rapporti tra GDPR e direttiva *e-Privacy*, sia ancora consentita una deroga alla competenza generale delle autorità per la protezione dei dati nei casi in cui al trattamento in questione si applicano le disposizioni della direttiva *e-Privacy*.

Nel caso italiano, che rappresenta in questo caso una best practice, le funzioni di sorveglianza della direttiva *e-Privacy* sono state tutte affidate al Garante per la protezione dei dati prevedendo al contempo un meccanismo di cooperazione sistematica (tramite un Accordo interistituzionale) tra il Garante e l'Autorità per le garanzie nelle comunicazioni, che è invece stata notificata come Autorità nazionale di regolazione nel settore delle comunicazioni elettroniche.

Come emerge dalle questioni proposte, il rapporto tra la direttiva *e-Privacy* (le discipline nazionali) e il GDPR non può essere descritto unicamente in termini di specialità, ma piuttosto di integrazione reciproca e tensione sistemica. In teoria, la direttiva *e-Privacy* assicura un livello di tutela più elevato per la riservatezza delle comunicazioni, mentre il Regolamento ne garantisce l'armonizzazione

[28] Tra l'altro occorre rilevare che le ANR, a norma della direttiva quadro sono indipendenti nei confronti degli operatori e, di conseguenza, obbligatoriamente nei confronti del Governo solo se lo Stato mantiene il controllo di uno o più operatori di mercato. Il che naturalmente rende il requisito dell'indipendenza diverso rispetto a quanto previsto nel GDPR.

[29] Cfr. J. Dumortier, E. Kosta, *e-Privacy Directive: Assessment of Transposition, Effectiveness and Compatibility with the Proposed Data Protection Regulation*, studio per la Commissione europea, DG CONNECT, 10 giugno 2015.

minima e i principi generali di trattamento. Nella sostanza però, questo determina, come l'EDPB ha sottolineato un "fragmented landscape" che ostacola la prevedibilità per gli operatori economici e riduce l'efficacia delle tutele per gli interessati[30].

5. *Il tentativo (non riuscito) di sostituire la direttiva* e-Privacy *con un nuovo regolamento settoriale e la ricerca di una nuova strada*

La mancata armonizzazione dei recepimenti nazionali, unita alla rapida obsolescenza tecnologica, ha reso il quadro normativo instabile e frammentato, ponendo le basi per la proposta di un nuovo Regolamento *e-Privacy*, concepito per sostituire l'attuale direttiva con uno strumento di portata uniforme.

Il GDPR definiva, nel considerando 173, la coesistenza con la direttiva *e-Privacy* come provvisoria prevedendo che essa avrebbe dovuto essere presto aggiornata. D'altra parte già nel 2015, la Commissione europea nel contesto della Strategia per il Mercato unico digitale, aveva preannunciato l'avvio di un processo di revisione della direttiva *e-Privacy* al fine di renderla coerente con il nuovo quadro generale in materia di protezione dei dati personali nonché di superare la differenziazione normativa tra fornitori di servizi di comunicazione elettronica e fornitori di servizi digitali[31].

Nell'ambito del Refit dedicato alla direttiva *e-Privacy*, la Commissione europea ha individuato due criticità principali[32]. La prima è la frammentazione dovuta ai recepimenti nazionali eterogenei, ca-

---

[30] EDPB, *Parere 5/2019*, cit., § 15.

[31] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Strategia per il mercato unico digitale in Europa*, COM(2015) 192 final, Bruxelles, 6 maggio 2015.

[32] Il *Regulatory Fitness and Performance Programme* (Refit) è il programma dell'Unione europea per l'adeguatezza e l'efficacia della regolamentazione. Esso, introdotto nel 2012, mira a rendere la legislazione dell'UE più semplice, ridurre gli oneri amministrativi, garantire che la normativa produca risultati concreti. Non si tratta di un atto normativo bensì di un processo permanente di revisione applicato a tutta la produzione normativa dell'UE. Commissione europea, *Programma per l'adeguatezza e l'efficacia della regolamentazione (REFIT). Bilancio della regolamentazione dell'UE*, COM(2012) 746 final, Bruxelles, 12 dicembre 2012.

pace di ostacolare la certezza del diritto e la parità di condizioni nel mercato interno; la seconda è l'inadeguatezza tecnologica della direttiva rispetto ai nuovi servizi digitali e alle piattaforme over-the-top (OTT)[33].

Sulla base delle risultanze del *refit*, la Commissione presentò nel 2017 la proposta di un nuovo regolamento *e-Privacy* che avrebbe dovuto abrogare la direttiva 2002/58/CE ed assicurare uniformità, immediatezza applicativa e coerenza, anche sistematica, con il GDPR[34].

Il regolamento proposto era concepito come un testo di complemento settoriale al GDPR, volto a disciplinare in modo unitario: *a*) la riservatezza delle comunicazioni elettroniche, estesa ai servizi di messaggistica, VoIP, e-mail e social media; *b*) l'uso dei dispositivi terminali e delle tecnologie di tracciamento (cookie, identificatori pubblicitari, IoT); *c*) le comunicazioni a fini di marketing diretto; *d*) le interferenze legittime per motivi di sicurezza pubblica o prevenzione dei reati[35].

Nonostante l'urgenza riconosciuta dalla Commissione europea così come dalle altre Istituzioni europee, il processo legislativo si è arenato sin dalle prime fasi dei negoziati in seno al Consiglio dell'Unione europea.

Diverse ragioni politiche e istituzionali ne hanno determinato lo stallo.

In primo luogo, gli Stati membri hanno espresso posizioni divergenti sulla ripartizione delle competenze tra autorità nazionali: alcuni ritenevano opportuno mantenere un ruolo per le autorità di

---

[33] Commissione europea, *Evaluation and review of the e-Privacy Directive (2002/58/EC)*, SWD(2016) 223 final, Bruxelles, [2016].

[34] *Proposta di regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla protezione dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla privacy e le comunicazioni elettroniche)*, COM(2017) 10 final, Bruxelles, 10 gennaio 2017. V. in proposito, anche con riferimento agli apporti del Parlamento, durante l'iter E. Gil González, P. De Hert, V. Papakonstantinou, *The Proposed e-Privacy Regulation: The Commission's and the Parliament's Drafts at a Crossroads?*, *Brussels Privacy Hub - Working Paper*, vol. 6, n. 20, marzo 2020, *https://brusselsprivacyhub.eu*.

[35] Cfr. L. Bolognini, C. Bistolfi, G. Crea, *e-Privacy Regulation: legal principles and impacts on the digital economy*, Studio dell'Istituto Italiano per la Privacy e la Valorizzazione dei Dati, 21 marzo 2018, disponibile su *www.istitutoitalianoprivacy.it*.

regolazione delle comunicazioni, mentre altri (tra cui l'Italia) preferivano attribuire la vigilanza esclusiva alle autorità di protezione dei dati personali[36].

In secondo luogo, le imprese del settore digitale hanno esercitato forti pressioni contro la generalizzazione del regime del consenso, a discapito del ricorso all'interesse legittimo, ritenendolo eccessivamente oneroso per i modelli di business fondati sulla pubblicità comportamentale.

Infine, la complessità tecnica del testo e la necessità di coordinarlo con altri strumenti normativi (in particolare la Direttiva NIS 2, il Codice europeo delle comunicazioni elettroniche e, più tardi, il *Digital Services Act*) hanno ulteriormente rallentato i lavori.

Dopo ripetuti tentativi di compromesso e varie versioni di testo su cui non si è mai raggiunto un accordo politico definitivo tra Commissione, Consiglio e Parlamento europeo, l'attenzione delle istituzioni si è progressivamente spostata verso nuove priorità, legate alla transizione digitale e all'economia dei dati, sfociate nell'adozione di numerosi Regolamenti, i c.d. *Acts* con cui l'Unione europea mira a regolare la società digitale europea (*Digital Services Act*, *Digital Markets Act*, *Data Governance Act*, *Data Act*, *AI Act*)[37]. Pur non trattandosi di normative in materia di protezione di dati (e tanto meno volte ad abrogare la direttiva *e-Privacy*), esse hanno in parte assorbito la funzione di aggiornamento tecnologico, affrontando questioni – come la pubblicità personalizzata, la moderazione dei contenuti o l'interoperabilità dei servizi – che incidono indirettamente anche sulla sfera della riservatezza.

---

[36] Sulle divergenze emerse in seno al Consiglio v. i *Progress report on the proposal for a Regulation on Privacy and Electronic Communications*, doc. 9079/18 (25 maggio 2018); ST-14491/18 INIT (25 maggio 2018); ST-12891/20 INIT (18 novembre 2020), dove si dà atto che, mentre alcune delegazioni potevano sostenere l'attribuzione delle competenze alle autorità responsabili dell'applicazione del GDPR, "most delegations seek further flexibility with regards to the supervisory authorities".

[37] Per un'analisi di tali interventi normativi sia consentito rinviare a F. Pizzetti, S. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino, *La regolazione europea della società digitale*, Giappichelli, Torino, 2024. V. specificamente sul modello di regolazione europeo e sul ruolo della tecnica, G. De Minico, *Unione europea, mercato, tecnica*. Relazione al Convegno annuale dell'Associazione Italiana dei Costituzionalisti su "L'Unione europea a confronto con la Costituzione della Repubblica italiana" tenutosi a Torino il 10-11 ottobre 2025, in corso di pubblicazione sulla Rivista AIC.

Nel 2025, dopo oltre otto anni di negoziati infruttuosi, la Commissione ha infine deciso di ritirare formalmente la proposta di regolamento *e-Privacy*, riconoscendo l'impossibilità di raggiungere un consenso politico nel Consiglio e l'obsolescenza della proposta alla luce delle norme più recentemente approvate[38].

La decisione segna dunque la fine di un lungo processo di riforma, rimasto incompiuto, che lascia il settore delle comunicazioni elettroniche ancora regolato da una direttiva e da ventisette diverse legislazioni nazionali concepite per un'epoca tecnologica ormai superata.

Proprio mentre maturava la decisione di ritirare la Proposta di regolamento *e-Privacy*, la Commissione europea avanzava una Proposta di Regolamento c.d. *GDPR Omnibus*, volto ad emendare la normativa esistente al fine di operare una semplificazione degli obblighi oggi a carico di piccole e medie imprese[39], una Proposta di Regolamento c.d. *Digital Omnibus* volto a semplificare il quadro regolamentare digitale nonché una consultazione pubblica per la definizione di una proposta di regolamento in materia di reti digitali (c.d. *Digital Networks Act*) che si inserisce in una più ampia strategia di revisione dell'intero ecosistema delle comunicazioni elettroniche.

La proposta di regolamento c.d. *GDPR omnibus*, così come presentata dalla Commissione, non prevede alcuna disposizione volta ad abrogare la direttiva *e-Privacy* né parti di essa. Le misure di alleggerimento degli obblighi normativi introdotte dalla proposta – peraltro circoscritte e rivolte principalmente alle piccole e medie imprese – appaiono destinate ad avere un impatto molto limitato sui fornitori di reti e servizi di comunicazione elettronica, i quali, per dimensioni e struttura, normalmente non rientrano nel perimetro soggettivo delle PMI. Inoltre, il contenuto della proposta, volto

[38] V. Allegati I a V a Commissione europea, *Programma di lavoro della Commissione per il 2025*. COM(2025) 45 final, Strasburgo, 11 febbraio 2025.

[39] European Commission, *Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2016/1036, (EU) 2016/1037, (EU) 2017/1129, (EU) 2023/1542 and (EU) 2024/573 as regards the extension of certain mitigating measures available for small and medium sized enterprises to small mid-cap enterprises and further simplification measures*, COM(2025) 501 final, Brussels, 21 May 2025, 2025/0130 (COD).

essenzialmente a intervenire su obblighi di registrazione, codici di condotta e meccanismi di certificazione, non incide in modo significativo né sulle norme della direttiva *e-Privacy* né sulle corrispondenti disposizioni nazionali di recepimento.

Per quel che riguarda la Proposta di Regolamento *Digital Omnibus*, esso contiene, invece, misure idonee ad impattare direttamente su alcune norme della Direttiva *e-Privacy*[40]. Innanzitutto, la Proposta in questione mira ad abrogare l'art. 4 della direttiva *e-Privacy* riconducendo integralmente la disciplina della sicurezza nell'ambito del GDPR e della direttiva NIS 2[41]. In secondo luogo, si propone la limitazione dell'ambito di applicazione della c.d. *cookies rule* dettata all'art. 5, par. 3 della direttiva *e-Privacy* che rimane in vigore solo per la memorizzazione e l'accesso ai dispositivi di abbonati e/o utenti che siano persone giuridiche. Per ciò che riguarda, invece, la memorizzazione e l'accesso ai dispositivi di persone fisiche la nuova proposta mira ad integrare una nuova *cookie rule* orizzontale nel GDPR superando, quindi, la specialità relativa alle reti pubbliche e ai servizi accessibili al pubblico di comunicazione elettronica attualmente prevista ai sensi della direttiva *e-Privacy*[42].

Assai rilevante è, inoltre, nella Proposta la nuova definizione di dato personale in cui si specifica come l'identificabilità della persona a cui il dato si riferisce debba essere valutata nel contesto reale e non solo potenzialmente. Questa modifica potrebbe evidentemente incidere anche sulla qualifica di molti dati elettronici come dati personali.

Per quel che attiene all'annunciato *Digital Networks Act*, la proposta di regolamento, inizialmente programmata per il quarto

---

[40] V. *Proposal of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)*, 19 November 2025 {SWD(2025) 836 final}.

[41] Cons. 48 e Art. 5 *Proposal Digital Omnibus.*

[42] V. Cons 44 e art. 3 par. 15 della *Proposal Digital Omnibus* che mira a introdurre nel GDPR l'art. 88a rubricato *Processing of personal data in the terminal equipment of natural persons* al fine di specificare quando è necessario il consenso dell'interessato e quando è possibile prescinderne.

trimestre del 2025 è stata ora posposta a gennaio 2026. Con essa l'Unione europea si propone non soltanto di modernizzare la disciplina delle reti e dei servizi di comunicazione elettronica, ma anche di superare i limiti strutturali derivanti dall'attuale frammentazione del mercato e dalla natura direttiva del Codice europeo delle comunicazioni elettroniche (EECC)[43].

La consultazione preliminare avviata dalla Commissione evidenzia, infatti, come la proliferazione di normative nazionali eterogenee, la lentezza dei recepimenti e l'eterogeneità delle condizioni di autorizzazione e assegnazione dello spettro radio costituiscano oggi uno dei principali ostacoli alla creazione di un vero mercato unico delle comunicazioni elettroniche. Il nuovo atto normativo, dovrebbe, ai sensi della consultazione, affrontare tali criticità attraverso un quadro giuridico più armonizzato, potenzialmente unificato in un unico strumento regolamentare che riassorba l'EECC, il regolamento BEREC, le norme sulla neutralità della rete e la politica europea sullo spettro radio[44].

È significativo osservare che la consultazione non menzioni il problema qui discusso della persistenza in vigore della direttiva *e-Privacy*. Tuttavia il tema della sua modifica, quando non direttamente della sua abrogazione, emerge come necessaria al fine di correggere l'attuale asimmetria regolamentare in molti dei contributi presentati dai soggetti che hanno partecipato alla consultazione[45].

---

[43] V. anche COMMISSIONE EUROPEA, *Libro bianco - Come affrontare adeguatamente le esigenze dell'Europa in termini di infrastruttura digitale?*, COM(2024) 81 final, Bruxelles, 21 febbraio 2024.

[44] L'iniziativa assume certamente una dimensione politico-strategica: la Commissione sembra infatti interpretare l'evoluzione delle reti digitali come un fattore essenziale per la competitività dell'Unione, la resilienza economica e la sicurezza, in linea con quanto emerso e sottolineato nei rapporti di Mario Draghi (*The Future of European Competitiveness - A Competitiveness Strategy for Europe*, presentato il 9 settembre 2024 ed Enrico Letta (*Much more than a Market - Speed, Security, Solidarity. Empowering the Single Market to Deliver a Sustainable Future and Prosperity for All EU Citizens*, presentato il 17-18 aprile 2024).

[45] V. in proposito i commenti inviati da Connect Europe, Telefónica S.A. (Spain), Liberty Global (Netherlands), Telenor Group (Norway), Telekom Austria AG - A1 Group (Austria) e Orange S.A. (France), nell'ambito della consultazione pubblica della Commissione europea sulla proposta di Digital Networks Act.

6. *Osservazioni conclusive*

Alla luce del quadro ricostruttivo svolto, la direttiva 2002/58/CE appare, sotto molti profili, ancorata a un contesto tecnologico e regolatorio ormai superato.

Ciò non toglie, tuttavia, che essa abbia svolto – e continui in parte a svolgere – una funzione importante nella protezione della riservatezza delle comunicazioni elettroniche. Da un lato, grazie all'elaborazione giurisprudenziale della Corte di giustizia, la direttiva *e-Privacy* è divenuta il perno di un sistema particolarmente avanzato di tutela della segretezza delle comunicazioni e dei c.d. metadati. Questo è avvenuto soprattutto grazie all'elaborazione di criteri molto rigorosi per le deroghe al regime di segretezza giustificate da esigenze di sicurezza nazionale o di contrasto ai reati. Dall'altro lato, la sua riforma del 2009 ha, come si è visto, anticipato istituti che sono poi confluiti nel GDPR: basti pensare all'obbligo di notifica delle violazioni di dati personali (*data breach*) agli utenti e alle autorità competenti, alla centralità della sicurezza delle reti e dei servizi come componente essenziale della tutela dei dati, nonché alla configurazione di un consenso informato, specifico e preventivo per l'uso dei terminali e delle tecnologie di tracciamento (la c.d. "cookie rule"), che costituirà il modello di riferimento per l'approccio successivo alla profilazione *online*.

La criticità più evidente riguarda il rapporto tra direttiva *e-Privacy* e GDPR.

Esso non può essere attualmente descritto in termini meramente lineari, come se la direttiva fosse una semplice *lex specialis* rispetto al regolamento qualificato come *lex generalis*. Le due fonti si collocano, piuttosto, in un rapporto che è in parte di specialità, in parte di integrazione e talvolta di sovrapposizione. Questo genera non poche incertezze nell'applicazione da parte degli operatori. Accanto alle aree in cui la direttiva specifica prevalendo sul quadro generale del GDPR – si pensi alle regole sui dati di traffico, sui dati di ubicazione o sull'accesso ai terminali – vi sono, infatti, ambiti in cui la disciplina settoriale integra il regolamento, estendendo la tutela anche alle persone giuridiche o a dati che, di per sé, non rientrerebbero nel perimetro del dato personale.

Al tempo stesso, la coesistenza di una fonte regolamentare direttamente applicabile e di discipline nazionali di recepimento della direttiva, crea una "specialità" che nella sostanza è tra norme di ordinamenti diversi. Il che sommato alla pluralità di autorità potenzialmente coinvolte nell'*enforcement*, contribuisce a disegnare un paesaggio frammentato, nel quale il confine tra prevalenza, integrazione e sovrapposizione non è sempre agevole da tracciare.

In questo quadro, uno dei nodi centrali è rappresentato dalla generalizzazione del consenso esplicito e preventivo quale presupposto di liceità dei trattamenti effettuati dai fornitori di reti e servizi di comunicazione elettronica. La direttiva e-*Privacy*, in linea con l'impostazione originaria della direttiva 95/46/CE, costruisce buona parte della tutela sull'idea di un consenso fortemente formalizzato, sia per l'utilizzo dei dati di traffico e di ubicazione, sia per l'accesso ai terminali. Tale scelta, se da un lato assicura un elevato grado di autodeterminazione informativa agli interessati – soprattutto rispetto alle forme di tracciamento e di marketing diretto più invasive – dall'altro si confronta con un modello, quello del GDPR, che ha riequilibrato il ruolo del consenso, affiancandogli in modo più netto ulteriori basi giuridiche del trattamento e invitando a un'applicazione meno "consenso-centrica" del sistema.

Ancora più marcata è la distanza rispetto agli atti del c.d. decennio digitale europeo, che pongono al centro la circolazione e la riutilizzabilità dei dati (personali e non personali) – pur entro cornici di garanzia – per finalità sia economiche sia sempre più apertamente funzionali alla garanzia dei diritti fondamentali[46].

Il risultato è una asimmetria regolamentare non irrilevante, soprattutto se la si osserva dal punto di vista concorrenziale: i fornitori tradizionali di servizi di comunicazione elettronica restano vincolati a un regime di consenso preventivo particolarmente stringente, mentre i molti fornitori di servizi digitali *over-the-top* operano sulla base di equilibri normativi in cui l'interesse legittimo e al-

[46] Sia consentito rinviare a M. Orofino, *The New Balance Between Data Circulation and Data Protection in the Digital Single Market*, in I. Anrò, F. Rossi Dal Pozzo (a cura di), *Il mercato unico digitale, tra antichi problemi e nuove sfide*, Fascicolo Speciale, 2025, Eurojus.

tre basi giuridiche (come ad esempio il contratto) trovano un terreno più ampio, con effetti potenzialmente distorsivi sul *level playing field*.

Il fallimento del progetto di regolamento e-*Privacy* ha lasciato questa situazione sostanzialmente immutata. Dopo anni di negoziati infruttuosi, la decisione della Commissione di ritirare la proposta appare, sotto certi aspetti, una presa d'atto di un mutato contesto: nel frattempo, il settore delle comunicazioni elettroniche ha perso parte della sua originaria specificità, inserendosi in un ecosistema digitale in cui reti, servizi di comunicazione, piattaforme e applicazioni convivono e competono nello stesso spazio di mercato, spesso offrendo funzionalità sostitutive.

Insistere su un regolamento settoriale concepito su una distinzione netta tra "operatori di comunicazione elettronica" e "altri fornitori di servizi digitali" rischiava probabilmente di cristallizzare una dicotomia che la realtà tecnologica e industriale aveva già superato. In questo senso, l'abbandono del progetto di riforma non è solo un indice di difficoltà politica, ma anche il sintomo di una tensione concettuale tra un approccio categoriale di matrice telco e una realtà in cui le comunicazioni elettroniche sono ormai una componente diffusa e trasversale del sistema digitale.

Resta allora la domanda, inevitabile, su quale debba essere il futuro della disciplina della riservatezza nelle comunicazioni elettroniche. Una possibile strada – sostenuta da numerosi attori del settore – è quella dell'abrogazione della direttiva e-*Privacy* e della sua piena integrazione in un quadro giuridico più armonizzato e orizzontale. Questa opzione appare a chi scrive percorribile ad un'unica condizione: che venga salvaguardato il principio fondamentale della segretezza delle comunicazioni, garantito dalle Costituzioni, dagli artt. 7 e 8 della Carta e dalla Corte di giustizia.

Questo principio, che costituisce il nucleo duro della direttiva e-*Privacy* fin dalla sua adozione ed è stato progressivamente rafforzato dalla giurisprudenza della Corte di giustizia, dovrebbe essere preservato e al tempo stesso integrato in un *framework* unitario che si applichi in modo eguale a tutti i fornitori di servizi di comunicazione, indipendentemente dalla qualifica formale e dalla tecnologia utilizzata.

Un tale intervento potrebbe avvenire, *de iure condenso*, sia con il *Digital Omnibus* (che in parte prevede l'abrogazione di singole norme della direttiva e-*Privacy*), sia con il *Digital Networks Act* ricomponendo le regole sulla riservatezza delle comunicazioni, sugli obblighi di sicurezza e sulle condizioni di accesso ai terminali, lungo l'intera filiera dei servizi di comunicazione digitale. Solo seguendo questa strada sarà possibile superare l'attuale frammentazione, garantire un equilibrio più coerente tra tutela dei diritti fondamentali e circolazione dei dati e, soprattutto, assicurare che il principio di segretezza delle comunicazioni continui a svolgere la sua funzione di presidio sostanziale della libertà individuale nell'ecosistema digitale contemporaneo.