UNIVERSITÀ DEGLI STUDI DI PAVIA

DOTTORATO DI RICERCA IN DIRITTO PUBBLICO, GIUSTIZIA PENALE E INTERNAZIONALE

XXXIII ciclo

LA TUTELA COSTITUZIONALE DELLA SEGRETEZZA DELLE COMUNICAZIONI E DELLA CORRISPONDENZA ALLA PROVA DELLE TECNOLOGIE EMERGENTI: PROFILI COMPARATI

Relatore: Chiar.mo Prof. Giovanni CORDINI

Tesi dottorale di

Davide ZECCA

Anno accademico 2019-2020

La tutela costituzionale della segretezza delle comunicazioni e della corrispondenza alla prova delle tecnologie emergenti: profili comparati

Introduzione **1**

I. La segretezza delle comunicazioni e della corrispondenza nell'ordinamento italiano 8

1. Le radici storiche 8
   1.1. La nascita dei servizi postali e l'epoca dell'Assolutismo 8
   1.2. Le prime rivendicazioni fra Rivoluzione e Restaurazione 10
   1.3. Il regime statutario nell'Italia liberale 12
2. Il dibattito in Assemblea Costituente 14
3. Lo statuto costituzionale della libertà e segretezza della corrispondenza 17
   3.1. La natura della prerogativa 17
   3.2. Comunicazione privata e comunicazione al pubblico: il valore distintivo della segretezza 19
   3.3. L'ambito di applicazione 20
   3.4. La struttura della posizione giuridica soggettiva 21
4. Libertà personale, tutela del domicilio e del segreto epistolare: quali differenze? 22
5. Segretezza delle comunicazioni e riservatezza della vita privata 25
   5.1. I primi passi della dottrina italiana 25
   5.2. Il contributo della giurisprudenza ordinaria e costituzionale 27
   5.3. L'intervento del legislatore 29
   5.4. Affinità e differenze 30
6. I limiti alla tutela costituzionale del segreto epistolare 31
   6.1. Natura della riserva di legge 31
   6.2. Natura della riserva di giurisdizione 33
   6.3. Le limitazioni disposte dalla legge 36

II. I tradizionali strumenti di intrusione e indagine del potere pubblico 42

1. Il controllo sulle comunicazioni postali 42

1.1. Il segreto postale nell'Italia liberale 42
1.2. Dalla riforma di epoca fascista all'età repubblicana 44
1.3. L'eco della Consulta: dal nuovo codice postale alla disciplina del Codice Vassalli 46
2. Le intercettazioni telefoniche 50
2.1. I presupposti nel codice del 1930 e l'adeguamento al quadro costituzionale 50
2.2. La nuova disciplina del codice del 1989 58
2.3. La riforma promessa (ma in parte tradita) del decreto Orlando 65
2.4. La funzione della motivazione 72
3. Le intercettazioni cd. ambientali 75
3.1. La disciplina generale 75
3.2. L'intercettazione domiciliare 78
4. Le intercettazioni telematiche 80

III. La segretezza delle comunicazioni e della corrispondenza sul piano internazionale e comparato 83
1. Profili di tutela nel diritto internazionale e sovranazionale 83
1.1. Il segreto delle comunicazioni nelle Carte dei diritti del II dopoguerra 83
1.2. Le garanzie nel sistema del Consiglio d'Europa 87
1.3. L'armonizzazione delle fonti dell'Unione Europea 94
2. La disciplina nell'ordinamento tedesco 98
2.1. La tutela costituzionale nelle Carte di epoca liberale 98
2.2. Il laboratorio di Weimar 102
2.3. Aspettando la Costituzione federale … 105
2.4. La disciplina costituzionale nella *Grundgesetz* 108
2.5. Le limitazioni ordinarie contenute nel codice di procedura penale 111
2.6. La disciplina della G 10 114
3. L'esperienza statunitense 117
3.1. La tutela delle comunicazioni private prima del *bill of rights* 117
3.2. L'interpretazione originaria del IV Emendamento 121
3.3. Le prime avvisaglie di un'evoluzione dell'interpretazione del IV Emendamento 123
3.4. La tutela del segreto delle comunicazioni telefoniche come paradigma del conflitto fra le diverse concezioni di privacy 126

3.5. La prima regolazione del *wiretapping* negli USA: il *Federal Communications Act* (1934) 128

3.6. Il dado è tratto: l'avvento della *reasonable expectation of privacy* e i suoi limiti 130

3.7. Il quadro normativo dopo *Katz* 132

IV. L'avvento delle nuove tecnologie e la crisi del paradigma tradizionale 134

1. Indagini informatiche e tecnologie digitali 134

1.1. Gli strumenti di controllo a distanza: *trojans* e *remote forensic softwares* 134

1.2. La qualificazione giuridica fra sussunzione e categoria ex novo 137

1.3. La protezione degli interessi individuali alla riservatezza 140

1.4. L'utilizzabilità delle prove in giudizio 142

1.5. Natura transfrontaliera ed esigenze di coordinamento 143

2. La Germania come precorritrice in campo europeo 144

2.1. I primi tentativi di disciplina della materia a livello statale. 144

2.2. La giurisprudenza costituzionale e l'inquadramento del BVG. Una prima fase 145

2.3. Gli sviluppi più recenti della giurisprudenza costituzionale 162

3. La tutela dello spazio privato digitale nella giurisprudenza statunitense 177

3.1. L'origine della sorveglianza da remoto: strumenti e strategie delle agenzie di *law enforcement*. 177

3.2. La rilettura della *reasonable expectation of privacy* nella recente giurisprudenza federale. 183

3.3. La giurisprudenza delle corti inferiori 184

3.4. La giurisprudenza della Corte Suprema 186

4. La giurisprudenza italiana sull'utilizzo del captatore informatico 196

4.1. Il ruolo di supplenza del giudice di legittimità 196

4.2. Non così in fretta: i distinguo della sentenza Musumeci e le minacce ai diritti costituzionali dei singoli 198

4.3. Un momentaneo punto fermo: il *laissez faire* della sentenza Scurato 199

4.4. Il doppio binario processuale: la perimetrazione degli effetti della pronuncia 201

4.5. La delega parlamentare e la riforma promessa (ma sospesa) 203

V. La tutela della riservatezza delle comunicazioni digitali: dai nuovi diritti all'equo bilanciamento fra valori divergenti 207

1. L'autonomia del diritto alla segretezza della corrispondenza oggi 207
2. Derogare sì, ma quando? 212
3. Alla ricerca dell'equilibrio: il criterio di ragionevolezza come panacea? 215

Bibliografia 219

Alla memoria di Valeria Solesin e Giulio Regeni

Introduzione

La scelta di un tema di ricerca è intimamente legata alla disciplina di studio e, a modo suo, aiuta a descrivere la concezione che della materia ha chi intraprende un percorso di approfondimento. Il punto di partenza di un lavoro di questo genere si ritiene dover consistere in un *actio finium regundorum*, che circoscriva il campo entro il quale ci si muove ma, al contempo, getti luce su che cosa l'ambito di studio prescelto rappresenta per chi si accinge a svolgere un lavoro di questo genere.

Volgendo lo sguardo all'area di studi pubblico-comparatistici, è dunque d'uopo interrogarsi su quale siano le motivazioni che orientano l'attenzione, nel ricco paniere di argomenti e temi a disposizione, verso le questioni prese in considerazione e quale sia la rilevanza delle stesse nel complesso degli studi della materia.

Studiare il diritto pubblico comparato può dare luogo a diversi sbocchi, in quanto il confronto fra gli ordinamenti giuridici nella loro evoluzione lungo l'arco del tempo oppure fotografandone le differenze in un dato momento temporale può assumere una grande varietà di profili anche sensibilmente diversi, dal funzionamento delle istituzioni ai rapporti che intercorrono tra di esse, dalla distribuzione del potere politico fra gli enti di un dato ordinamento all'indagine sull'effettività della tutela in concreto dei diritti riconosciuti ai cittadini e agli individui.

L'angolo visuale adottato in questo lavoro pertiene a questo ultimo ambito, prefiggendosi lo scopo di studiare l'emersione della prerogativa oggetto di interesse dai suoi albori nell'epoca moderna attraverso l'evoluzione delle forme di Stato e del costituzionalismo occidentale, non mancando di evidenziare, ove presenti, i passaggi a vuoto e i passi indietro nella tutela del diritto in oggetto.

Concentrarsi sulla protezione del segreto delle comunicazioni ha il pregio di consentire di occuparsi di un diritto civile della sfera privata, per ciò stesso appartenente alla prima categoria di libertà riconosciute agli individui nell'evoluzione del costituzionalismo, potendo tuttavia apprezzare il diverso grado di tutela e di attenzione a esso tributato rispetto ad altri diritti inerenti la personalità, quali la libertà personale e il domicilio.

D'altronde, se fin dalle sue prime manifestazioni il costituzionalismo ha quale propria ragion d'essere quella di costituire un argine al potere pubblico, sia esso

esercitato da un signore feudale, un monarca assoluto o un organo dello Stato, lo studio delle garanzie accordate alla segretezza del contenuto delle comunicazioni ben si sposa con tale scopo, essendo legato a quella forma di esercizio del potere coercitivo dello Stato che è la giurisdizione penale. È infatti a fini processuali o, per meglio dire, di persecuzione dei reati o di prevenzione delle condotte antigiuridiche e antisociali che si danno la maggioranza dei casi entro i quali i testi costituzionali occidentali moderni consentono deroghe al principio della segretezza del contenuto delle conversazioni che ciascun singolo individuo intrattiene con gli altri consociati.

Identificare quali siano le ipotesi ove tali eccezioni a un principio generale siano consentite e cercare di metterne in luce i profili di compatibilità o meno con il dato costituzionale rende possibile valutare l'efficacia in concreto e la precettività del principio sancito nel testo fondamentale su cui si fonda il *pactum societatis*. Ciò implica senz'altro la necessità di considerare una pluralità di fonti o, per meglio dire, di formanti[1] che plasmano il dato normativo e rendono più o meno favorevole al cittadino il trattamento da parte del potere pubblico. Il riferimento al testo costituzionale non potrà quindi prescindere da un'attenta valutazione della sua capacità di orientare il legislatore nelle scelte che quest'ultimo è chiamato a fare, servendosi nel giudizio di bilanciamento fra valori della bussola che è la stessa Costituzione. In quest'ottica non può essere sottovalutato il ruolo della giurisprudenza, che nelle sue varie articolazioni (ordinaria, di merito, di legittimità e costituzionale) offre spunti e mette alla prova quotidianamente il dato costituzionale, mettendo in luce i limiti delle discipline legislative o proponendo ricostruzioni alternative che non di rado assumono funzione preponderante nell'applicazione di una determinata disciplina.

All'inquadramento del contesto storico-costituzionale, quindi, ci si prefigge di affiancare costantemente il quadro normativo applicabile, sì da poter trarre conclusioni informate sulla capacità dei testi costituzionali di incidere sulla realtà giuridica in concreto. Tale impatto sarà valutato in primo luogo per mezzo della

[1] Sulla teoria dei formanti v. R. Sacco, *Introduzione al diritto comparato*, Torino, UTET, 1992; l'autore ha ripreso il tema, tra l'altro, in *Id.*, *Legal Formants: A Dynamic Approach to Comparative Law (Installment I of II)*, in *The American Journal of Comparative Law*, Vol. 39, No. 1. (Winter, 1991), 1-34, spec. 21 ss.

considerazione della giurisprudenza rilevante in materia, non dimenticando il ruolo della dottrina giuridica nella ricostruzione degli istituti e nell'orientamento dell'attività interpretativa, anche in sede giudiziale.

Se quanto detto vale a inquadrare l'oggetto dello studio, è opportuno dar conto delle ragioni che hanno orientato la scelta degli ordinamenti di riferimento, ben consapevoli che ciò limita la portata delle osservazioni che verranno svolte, ma prendendo coscienza altresì che una trattazione a più ampio raggio e dedicata a un numero più consistente di ordinamenti più difficilmente avrebbe potuto essere sviluppata in questa sede in termini analoghi.

Le ragioni che fondano la scelta del primo ordinamento, quello italiano, se possono sembrare semplicemente connesse alla lingua di redazione dell'elaborato e alla conoscenza diretta da parte di chi scrive, sono in realtà ben più rilevanti e significative. In particolare, il caso italiano consente di prendere in considerazione un quadro costituzionale che a questo riguardo varia non poco fra l'esperienza statutaria e quella repubblicana e che si caratterizza altresì per una disciplina dei mezzi di ricerca della prova che incidono sul segreto delle comunicazioni che si è rivelata particolarmente cangiante e magmatica. L'analisi dell'evoluzione della regolamentazione delle intercettazioni di telecomunicazioni e le più recenti vicende relative all'uso del captatore informatico hanno infatti reso il caso italiano un adeguato metro di paragone dal quale partire nello sforzo di comparazione.

Per il secondo ordinamento la scelta è ricaduta sulla Germania, per una serie di motivi che rendono l'ordinamento tedesco oggetto di studio assai fruttuoso in questa materia, specie in parallelo a quanto accaduto in Italia. Le vicende del costituzionalismo che caratterizzano il caso tedesco sono infatti non del tutto sovrapponibili con quelle italiane, in particolar modo nel corso della seconda metà del XIX secolo, ove in Germania prende piede un pensiero costituzionalistico originale ma che rimane in parte isolato[2]. Non si può poi ignorare che da un certo punto in avanti del Novecento le strade di Italia e Germania viaggiano sempre più una a fianco dell'altra, sia nei momenti più bui che in quelli di grande innovazione e rinascita. La comune esperienza dello stato totalitario e l'appartenenza dei due testi costituzionali

[2] G.F. Ferrari, *Le libertà. Profili comparatistici*, Torino, Giappichelli, 2011, 131-141.

allo stesso ciclo, quello post-bellico, avvicina le due esperienze, che peraltro si distinguono dall'altra costituzione europea occidentale del tempo, quella francese del 1947, per la previsione di estesi cataloghi di diritti[3].

A ciò, si aggiunga la comune partecipazione al percorso di integrazione europeo che ha portato dalle iniziali quattro libertà fondamentali alla base della comunità europea a forme di armonizzazione e persino identità delle discipline nazionali in ragione della forza uniformatrice del diritto dell'Unione Europea, che giova dei principi dell'effetto diretto e del primato sul diritto nazionale, pur con i distinguo che le due corti costituzionali hanno ritenuto di formulare. All'appartenenza al progetto europeo si affianca altresì la partecipazione al Consiglio d'Europa, che approssima ancora di più le esperienze di Italia e Germania in considerazione del comune approccio dualista nei confronti della penetrazione del diritto internazionale nell'ordinamento interno[4], tale da rendere assimilabile la posizione delle disposizioni della Convenzione Europea per i Diritti dell'Uomo nel rango delle fonti del diritto dei due Stati. La compresenza di questi due ordinamenti in un contesto come quello europeo del XXI secolo, ove si è affermato il cd. 'costituzionalismo multilivello', rende dunque ancora più interessante il paragone fra i due Paesi, anche per verificare se vi è identità di ricezione degli input comuni tratti dalla partecipazione a queste organizzazioni internazionali.

Il terzo e ultimo ordinamento preso in considerazione è quello statunitense, che invece marca una differenza non da poco con i due precedenti sotto numerosi profili. In primo luogo, si tratta di uno Stato la cui tradizione giuridica prevalente è derivata da quella di *common law*, laddove tanto l'Italia quanto la Germania sono sussumibili sotto la famiglia di *civil law*[5]. Ciò premesso, come si vedrà ciò che rende interessante il paragone è proprio la diversità delle tecniche adottate, non tanto in fase di attuazione

---

[3] *Ibid.*, 211.

[4] L. Montanari, *Le tecniche di adattamento alla Cedu come strumento di garanzia dei diritti: un'analisi comparata delle soluzioni adottate negli ordinamenti nazionali*, in Atti del Colloquio biennale dell'Associazione italiana di diritto comparato tenutosi a Messina-Taormina, 31 maggio-2 giugno 2001, *I diritti fondamentali in Europa*, Milano, Giuffrè, 2002, 522-557.

[5] Sulle differenze fra il sistema di *Civil law* e quello di *Common law* nell'ambito della cd. famiglia a dominanza professionale (o a egemonia del diritto), v. G.F. Ferrari, *«Civil law» e «common law»: aspetti pubblicistici*, in P. Carrozza-A. Di Giovine-G.F. Ferrari (a cura di), *Diritto costituzionale comparato*, Roma-Bari, Laterza, 2009, 645-673.

da parte del legislatore, quanto piuttosto in sede di redazione del testo costituzionale e dunque di predisposizione delle garanzie a favore dei cittadini. D'altronde, sotto quest'ultimo profilo si può apprezzare tutta la distanza storica che intercorre tra il costituzionalismo liberale americano di fine XVIII secolo e quello moderno che contraddistingue le costituzioni italiana e tedesca di metà XX secolo.

In particolare, l'approfondimento del caso degli Stati Uniti offre spunti di riflessione sull'autonomia residua della prerogativa oggetto di studio, in specie con riferimento alle evoluzioni più recenti sotto il profilo tecnologico, invitando a interrogarsi sull'opportunità di prevedere delle forme di tutela dei diritti della personalità più omogenee e ad ampio spettro, anziché parcellizzate in una serie di pretese ciascuna distinta dalle altre.

Individuato l'oggetto principale dello studio e tracciati i confini della trattazione in chiave comparatistica, rimane da argomentare l'attualità di uno studio su questo tema. Non si tratta di un filone di approfondimento del tutto nuovo, poiché esistono studi precedenti che si occupano, anche diffusamente, dell'argomento[6]. Tuttavia, proprio la distanza temporale e l'intervento di assai numerosi mutamenti nel modo di vivere e, in particolare, di comunicare pongono nuovi interrogativi a fronte di testi costituzionali che fotografano una situazione di partenza risalente nel tempo (in particolar modo quello statunitense).

Se l'innovazione tecnologica offre una straordinaria possibilità di estendere la propria rete di relazioni sociali e di avere contatti con un numero di soggetti ben superiore rispetto a quello mai avuto a disposizione da alcuno altro nel corso della storia della civiltà umana, queste opportunità sono suscettibili di essere un'arma a doppio taglio, in ragione della possibilità del potere pubblico di poterne sfruttare le potenzialità a fini intrusivi e di controllo della popolazione, tali da ledere in modo assai rilevante quelle prerogative costituzionalmente protette.

In accordo con lo spirito che caratterizza le scelte politiche nelle forme di Stato contemporanee di democrazia pluralista, i testi costituzionali presi in considerazione offrono un affresco di principi e valori ampio ma non sempre conciliabile fra le varie

[6] In lingua italiana v. A. Valastro, *Libertà di comunicazione e nuove tecnologie. Inquadramento costituzionale e prospettive di tutela delle nuove forme di comunicazione interpersonale*, Milano, Giuffrè, 2001; in lingua inglese si veda B.R. Ruiz, *Privacy in Telecommunications*, L'Aja, Kluwer Law International, 1997.

istanze, tale da implicare il ricorso a giudizi di bilanciamento da parte del decisore politico. La valutazione sull'esistenza o meno di una tendenza di massima nella configurazione dei rapporti fra le istanze securitarie della collettività e la protezione delle prerogative riconosciute ai singoli costituisce uno dei punti d'approdo auspicati del presente lavoro, che si interroga altresì sull'opportunità o meno di sfumare sempre di più i confini fra i diritti della personalità nella loro accezione comune.

Il percorso prende le mosse, nel primo capitolo, da una ricostruzione delle manifestazioni più risalenti di un riconoscimento del segreto della corrispondenza come diritto, esplorandone l'evoluzione nel passaggio dall'*ancién regime* allo Stato liberale. Particolare attenzione viene dedicata alla configurazione dello stesso nella Costituzione repubblicana italiana, evidenziandone affinità e differenze con altri diritti civili sanciti dalla Carta, nonché distinguendolo dal diritto alla riservatezza della sfera privata e illustrandone i limiti, insieme alle garanzie preposte alla sua tutela nei casi di deroga dal principio generale.

Nel secondo capitolo si illustrano gli strumenti attraverso i quali il legislatore italiano ha nel corso del tempo introdotto delle limitazioni al godimento del diritto in parola, a partire dal controllo effettuato sulla corrispondenza postale fino all'intercettazione delle conversazioni telefoniche o tra presenti, senza dimenticare un cenno alle intercettazioni telematiche.

Il terzo capitolo è dedicato ad ampliare lo sguardo, dando conto del riconoscimento dell'inviolabilità del segreto delle comunicazioni in numerose carte dei diritti stipulate a livello sovranazionale, nonché offrendo una sintesi della tutela predisposta in questo ambito dal sistema CEDU e dal diritto UE. Segue un'analisi dell'evoluzione della tutela costituzionale del diritto in oggetto nei due ordinamenti selezionati ai fini di comparazione, orientata a evidenziare eventuali variazioni nella concezione della prerogativa nel corso del tempo, nonché a fornire alcune coordinate sui principali poteri di sorveglianza e interferenza con il segreto epistolare predisposti nei due Paesi.

Il quarto capitolo, preso atto dello *status quo ante*, tenta di qualificare entro una delle categorie giuridiche note e pre-esistenti i nuovi e intrusivi strumenti di indagine ai quali le autorità inquirenti hanno accesso e dispiegano ai fini di persecuzione dei

reati o di prevenzione degli stessi. Segue una descrizione dettagliata delle soluzioni che la giurisprudenza ha ritenuto di adottare con riferimento al bilanciamento di valori fra l'accertamento delle responsabilità penali e l'interesse a serbare segreto il contenuto delle proprie comunicazioni ma anche dei propri dispositivi informatici, mettendo in luce il diverso ruolo dei vari attori istituzionali nei tre ordinamenti considerati.

Il lavoro si conclude con alcune considerazioni di sintesi sulle analogie e differenze nell'approccio alla tutela costituzionale del segreto epistolare e delle comunicazioni digitali fra i sistemi analizzati, riflettendo inoltre sull'adeguatezza delle soluzioni concrete in prospettiva e sull'opportunità di ripensare le categorie di diritti in termini più liquidi e meno rigidi di quanto la tradizione abbia insegnato a fare finora.

I. La segretezza delle comunicazioni e della corrispondenza nell'ordinamento italiano

Sommario: 1. Le radici storiche. – 1.1. La nascita dei servizi postali e l'epoca dell'Assolutismo. – 1.2. Le prime rivendicazioni fra Rivoluzione e Restaurazione. – 1.3. Il regime statutario nell'Italia liberale. – 2. Il dibattito in Assemblea Costituente. – 3. Lo statuto costituzionale della libertà e segretezza della corrispondenza. – 3.1. La natura della prerogativa. – 3.2. Comunicazione privata e comunicazione al pubblico: il valore distintivo della segretezza. – 3.3. L'ambito di applicazione. – 3.4. La struttura della posizione giuridica soggettiva. – 4. Libertà personale, tutela del domicilio e del segreto epistolare: quali differenze? – 5. Segretezza delle comunicazioni e riservatezza della vita privata. – 5.1. I primi passi della dottrina italiana. – 5.2. Il contributo della giurisprudenza ordinaria e costituzionale. – 5.3. L'intervento del legislatore. – 5.4. Affinità e differenze. – 6. I limiti alla tutela costituzionale del segreto epistolare. – 6.1. Natura della riserva di legge. – 6.2. Natura della riserva di giurisdizione. – 6.3. Le limitazioni disposte dalla legge. – 6.3.1. Limitazioni in tempo di guerra. – 6.3.2. Limitazioni in tempo di pace. – 6.3.3. Come muta la natura delle limitazioni.

1. Le radici storiche

1.1. La nascita dei servizi postali e l'epoca dell'Assolutismo

La libertà di comunicare segretamente fra privati ha origini risalenti e si caratterizza per il diverso ambito di applicazione che nel corso della storia essa ha avuto; infatti, è d'uso distinguere fra la tutela del segreto epistolare (o assimilabile) dall'indebita intrusione di terzi privati e da quella dei pubblici poteri. D'altronde, fino al termine del XVIII secolo le autorità di governo esercitavano un controllo pressoché illimitato sulla corrispondenza dei cittadini, giustificando tale condotta con il perseguimento di fini di protezione e garanzia dell'ordinamento dalla diffusione di fattori destabilizzanti per l'ordine costituito.

La prima ideale proclamazione del principio di segretezza della corrispondenza viene ricondotto da alcuni autori all'ingresso del *Postmaster General* nel *Privy Council* britannico nel 1649[7], anche se fu pochi anni dopo, durante il Protettorato cromwelliano, che l'approvazione del *First Post Office Act* (1656) sancì l'opportunità

[7] P. Barile-E. Cheli, *Corrispondenza (libertà di)*, in *Enc. del dir.*, X, Milano, 1962, 746.

dell'esercizio del servizio postale in regime di monopolio governativo al fine di "*scoprire e prevenire molti pericolosi e malvagi disegni, … escogitati quotidianamente contro la pace e il benessere del Commonwealth, le cui informazioni non possono essere ben comunicate che per mezzo di lettere per iscritto*"[8]. Invero, se al momento della restaurazione della monarchia Stuart sotto Carlo II il contenuto dell'atto precedente venne in sostanza inglobato in un ampio testo che disciplinava la materia del servizio postale (1660)[9], fu con una proclamazione regia del 1663 che lo stesso monarca proibì l'apertura di lettere o pacchi di cui non si fosse destinatari, salvo che su mandato del Segretario di Stato[10]. Tale provvedimento, se da un lato conferma l'esistenza di un potere dell'autorità pubblica di violare la segretezza della corrispondenza, dall'altro riconosce che il contenuto della comunicazione fra privati non può essere conosciuto se non dal destinatario dell'atto comunicativo, con ciò dando una sanzione formale al principio generale di inviolabilità della corrispondenza.

Questo riconoscimento non valse tuttavia a far includere la prerogativa in oggetto fra le libertà contemplate nel *Bill of Rights* votato dai Comuni e dai Lord all'esito della cd. *Glorious Revolution* (1689): il documento contempla infatti esclusivamente la libertà di manifestazione del pensiero all'interno del Parlamento, sancendone la sindacabilità solo in quella sede, per proteggere i rappresentanti del popolo dall'ingerenza del potere giudiziario, senza disporre in merito alla libera manifestazione del pensiero da parte dei privati cittadini o alla segretezza della corrispondenza fra gli stessi.

Dall'altra parte della Manica, già da quando fu avviato un servizio di amministrazione postale sotto Luigi XI[11] le lettere trasportate dai corrieri reali venivano preventivamente lette, anche se è all'epoca in cui il Cardinal Richelieu esercitava le funzioni di Primo ministro di Luigi XIII (1624-1642) che si fa risalire

---

[8] A.M. Ogilvie, *The Rise of the English Post Office*, in *The Economic Journal*, Vol. 3, No. 11 (Sett. 1893), 443-457.

[9] *Charles II, 1660: An Act for Erecting and Establishing a Post Office*, in J. Raithby (a cura di), *Statutes of the Realm: Volume 5, 1628-80*, (s.l, 1819), 297-301. Il testo dell'atto è altresì disponibile sul sito *British History Online* (http://www.british-history.ac.uk/statutes-realm/vol5/pp297-301 [ultimo accesso: 21 luglio 2019]).

[10] Proclamation of May 25, 1663, App. LXI, Parliamentary Papers, Volume 14, H.M. Stationery Office, 1844, 582.

[11] Édit du 19 juin 1464.

l'istituzione di un apposito ufficio investito del compito di verificare il contenuto della corrispondenza, in particolare quando si trattasse di soggetti particolarmente in vista: si tratta del *Cabinet du secret des postes*, passato alla storia come *Cabinet Noir*[12]. Durante il regno di Luigi XIV (seconda metà del XVII secolo) e sotto gli auspici del Segretario di Stato alla Guerra e Sovrintendente Generale delle Poste Louvois, al quale invero è stata talora anche attribuita la nascita del *Cabinet* stesso, l'ufficio si perfezionò e il ricorso ad esso si fece sempre più frequente[13].

L'attività di quest'organo divenne ordinaria nel corso del XVIII secolo, quando, durante il regno di Luigi XV, i dipendenti del *Cabinet* divennero maestri nell'arte dell'apertura delle buste senza danneggiare il timbro che ne assicurava la chiusura, così garantendo che il destinatario non potesse avvedersi dell'avvenuta lettura del contenuto della missiva[14]. Va precisato che, ad ogni modo, l'interferenza della pubblica autorità nella corrispondenza privata si coniugava con un impegno a vigilare sulle modalità dell'esercizio dell'attività di intercettazione svolta dai funzionari pubblici addetti al servizio postale, che erano assoggettati all'irrogazione di misure punitive per la violazione dei propri doveri d'ufficio[15].

1.2. Le prime rivendicazioni fra Rivoluzione e Restaurazione

Fu solo alla vigilia della Rivoluzione del 1789 che iniziò ad affermarsi la necessità di predisporre una qualche forma di protezione avverso la violazione del segreto epistolare; la lettura dei *cahiers des doléances* raccolti in vista della riunione degli Stati Generali consente di ravvisare come, in realtà, la tutela della segretezza del contenuto delle comunicazioni fosse fra le priorità manifestate dai rappresentanti del cd. Terzo Stato, che percepivano l'intrusione dei poteri pubblici in materia come dispotica e lesiva delle prerogative di ciascun individuo[16]. L'Assemblea Nazionale discusse il

---

[12] Sul tema v. E. Vaille, *Le cabinet noir*, Paris, Presses universitaires de France, 1950, 67.
[13] *Ibid.*, 68-69 e 82.
[14] A. Belloc, *Les postes françaises: recherches historiques sur leur origine, leur développement, leur législation*, Paris, Firmin-Didot, 1886, 151 ss. e 205 ss.
[15] E. Vaille, *op. cit.*, 89.
[16] Per alcuni esempi v. A. Belloc, *op. cit.*, 252 ss.; parimenti E. Vaille, *op. cit.*, 207.

tema dell'inviolabilità del segreto delle lettere in più sedute (25 e 27 luglio, 5 dicembre 1789), senza che ciò conducesse all'approvazione di alcun atto vincolante in materia.

Di lì a pochi mesi, tuttavia, lo stesso consesso, nel sanzionare la condotta della municipalità di Saint-Aubin, colpevole di aver aperto e letto corrispondenza destinata all'intendente generale delle poste e a ministri stranieri, sancì nel Preambolo del decreto del 10 agosto 1790 l'inviolabilità del segreto delle lettere, impegnandosi a farne garantire il rispetto sia da parte di individui privati che da parte di organi amministrativi[17]. Dopo meno di tre settimane il decreto approvato dall'Assemblea per riformare il sistema postale fu proclamato dal Re e divenne legge: il testo conteneva l'obbligo per commissari, amministratori e impiegati delle poste di prestare giuramento affinché serbassero il segreto dovuto alle lettere e denunziassero le violazioni di cui fossero venuti a conoscenza[18].

Dopo il breve e fallimentare tentativo di fuga del monarca nel giugno 1791, che aveva spinto alcune municipalità ad adottare nuovamente prassi di sorveglianza sulla corrispondenza fra privati, per evitare gli abusi dei decenni precedenti l'Assemblea Nazionale approvò un decreto che ordinava espressamente agli organi amministrativi di vigilare sull'esecuzione del decreto dell'agosto 1790, garantendo l'inviolabilità del segreto delle lettere e astenendosi dal porre in essere alcuna misura che incidesse nell'ambito del servizio postale[19]. Poche settimane più tardi la stessa Assemblea inserì nel codice penale una disposizione atta a punire con la perdita dei diritti civili la soppressione di una lettera destinata alla posta o la rottura del timbro e la violazione del segreto della stessa[20].

Nonostante l'ordinamento costituzionale rivoluzionario appaia propenso alla tutela della libertà in questione, sembra rilevante sottolineare l'assenza di riferimenti al carattere inviolabile del segreto della corrispondenza nei documenti di maggior valore politico-programmatico di quegli anni: infatti, tanto la Dichiarazione dei diritti dell'uomo e del cittadino (1789) quanto la Costituzione del 13 settembre 1791 non vi

[17] Per il testo del decreto v. A. Belloc, *op. cit.*, 265.
[18] Art. 2, Loi de 22, 23, 24, 26 et 29 Aout 1790 contenant une nouvelle organisation des postes aux lettres, des postes aux chevaux et des messageries.
[19] Décret du 10 juillet 1791 sur le secret et l'inviolabilité des lettres.
[20] Art. 23, Code penal, 25 septembre 1791, Article punissant la violation du secret des lettres.

fanno menzione, limitandosi a sancire il valore costituzionale della libertà di manifestare il proprio pensiero, intesa nel senso della facoltà di darne pubblica diffusione[21]. L'assenza di alcuna disciplina costituzionale esplicita di questa libertà si trascina peraltro ben oltre il periodo rivoluzionario e le numerose Costituzioni proclamate in tale epoca (1793, 1795, 1799, 1802, 1804), dato che né la Carta della Restaurazione del 1814, né la Carta del 1830 della cd. Monarchia di luglio, né infine le Costituzioni della II (1848) e della III Repubblica (1875) contemplano l'inviolabilità della segretezza della corrispondenza fra le prerogative tutelate dallo Stato avverso l'intrusione non autorizzata (in particolare dei pubblici poteri).

Invero, l'inviolabilità del segreto della corrispondenza privata nei confronti della pubblica autorità era contemplata da alcune delle Carte costituzionali ottriate della prima metà del XIX secolo, quali la Costituzione dei Paesi Bassi del 1815 (art. 154), la Costituzione del Belgio del 1831 (art. 22), la Costituzione del Regno delle Due Sicilie del 1848 (art. 29) e la Costituzione di Prussia del 1850 (art. 33), seppur tale divieto fosse puntualmente temperato dal richiamo alla disciplina dettata per legge, stilema tipico della forma di regolazione dei diritti caratteristica delle Costituzioni di epoca liberale[22].

1.3. Il regime statutario nell'Italia liberale

Rivolgendo lo sguardo al contesto italiano, il primo riferimento non può che essere lo Statuto del Regno di Piemonte e Sardegna concesso da Re Carlo Alberto di Savoia nel 1848, che fu esteso all'Italia unificata al termine delle guerre d'indipendenza. Il cd. Statuto Albertino non contemplava la segretezza della corrispondenza all'interno del catalogo di diritti riconosciuti ai regnicoli, il quale includeva invece la protezione avverso le violazioni della libertà personale e della libertà di domicilio[23]. La mancata menzione di tale prerogativa non impedì alla dottrina giuridica dei decenni successivi

[21] Sulla distinzione fra libertà di manifestazione del pensiero e libertà e segretezza della corrispondenza v. *infra*, §3.2.
[22] P. Ridola, *Preistoria, origini e vicende del costituzionalismo*, in P. Carrozza-A. Di Giovine-G.F. Ferrari (a cura di), *Diritto costituzionale comparato*, Roma-Bari, Laterza, 2009, 44.
[23] Rispettivamente artt. 26 e 27 Statuto Albertino.

di sostenere l'esistenza di una garanzia a favore della libertà e dell'inviolabilità della corrispondenza, desumendola vuoi dalla libertà personale[24], vuoi da quella domiciliare[25]. D'altronde, si sosteneva nel più noto testo di commento allo Statuto, la libertà della comunicazione e l'inviolabilità del segreto epistolare discendevano come corollari indispensabili dalla libertà individuale e insieme a essa e alla libertà di domicilio e di manifestazione del pensiero pubblicamente costituivano un nucleo intangibile di prerogative riconosciute alla persona umana[26].

Tale ricostruzione teorica, che faceva leva sulle riserve di legge previste dal testo statutario a tutela delle libertà in esso sancite, non si dimostrò un presidio efficace per la garanzia della segretezza della corrispondenza, come dimostrano le deroghe a tale principio rintracciabili nel codice postale e nel codice penale dell'Italia liberale, le cui disposizioni erano piuttosto volte a proteggere il contenuto della comunicazione dall'intrusione privata che non da quella dei pubblici poteri[27].

Il codice di procedura penale del 1913, che sostituì per un breve lasso di tempo quello sabaudo prima della entrata in vigore dell'analogo testo di epoca fascista (1930), distingueva i due profili di libertà e segretezza della corrispondenza, disponendo che il giudice potesse ordinare il sequestro di messaggi o altre forme di corrispondenza dirette a un imputato (profilo attinente alla libertà), sancendo al contempo il divieto di apertura di pacchi e altra corrispondenza sigillata agli operatori di polizia giudiziaria responsabili per il sequestro (profilo della segretezza)[28].

La garanzia meramente formale di età liberale transitò altresì nella normativa fascista: infatti, il codice postale del 1936 sanciva sì il principio dell'inviolabilità del segreto epistolare, ma prevedeva la facoltà della pubblica autorità di visionare, fare copia e sequestrare la corrispondenza, nei casi e modi stabiliti dalla legge, condizione

---

[24] G. Maranini, *Le origini dello Statuto albertino*, Firenze, Vallecchi, 1926, 191-192.
[25] A. Brunialti, *Prefazione. La libertà nello stato moderno*, in *Id.* (a cura di), *Biblioteca di scienze politiche*, Vol. V, Torino, Unione tipografico-editrice, 1890, CLXXIV-CLXXV.
[26] F. Racioppi-A. Brunialti, *Commento allo Statuto del Regno*, II, Torino, UTET, 1909, 63; in particolare, Brunelli, in nota al primo paragrafo di commento all'art. 26, ritiene opportuno il riferimento alla garanzia del segreto postale, che Racioppi non aveva menzionato, se non *en passant*, nel commento all'art. 27.
[27] V., per esempio, art. 27, l. postale 5 maggio 1862, e successive leggi 2442/1875, 6151/1889 e 6889/1890, cfr. P. Caretti, *Corrispondenza (Libertà di)*, in *Dig. disc. pubbl.*, vol. IV, Torino, 1989, 200.
[28] Art. 238 c.p.p. del 1913.

che non si risolveva in altro che una mera clausola di stile[29]. D'altronde, la natura flessibile di questa costituzione – come di tutte quelle di epoca liberale – esponeva le garanzie contenute nel testo alla deroga a opera della mera legge ordinaria, anche quando non espressamente previsto dalla disposizione. L'intervento dell'autorità giudiziaria e delle forze di pubblica sicurezza era disciplinato da apposite disposizioni dei codici di rito, alle quali si affiancava una fattispecie specifica volta a punire le violazioni del segreto della corrispondenza. I frequenti abusi del potere di intercettazione di cui le pubbliche autorità si resero autrici nel corso del Ventennio contribuirono a rendere fertile il terreno in Assemblea Costituente per l'introduzione di una garanzia volta specificamente a proteggere il segreto epistolare.

Fu sulla cornice normativa appena delineata che intervenne l'art. 15 della Costituzione repubblicana del 1948, che convisse tuttavia per venticinque anni con il vecchio codice postale e con una disciplina delle intercettazioni telefoniche non innovata.

2. *Il dibattito in Assemblea Costituente*

L'art. 15 della Costituzione della Repubblica italiana afferma che "La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili" [c.1] e prosegue sancendo che "La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge" [c.2].

Il presente testo è l'esito, come d'altronde tutta la Carta, dell'elaborazione e delle discussioni dell'Assemblea Costituente fra il luglio del 1946 e il dicembre del 1947; è proprio seguendo il percorso che ha condotto al testo corrente dell'art. 15 che si può trarre spunto per interrogarsi sulla natura e sui limiti che la Costituzione detta in materia. Un utile contributo a questo scopo possono offrire i resoconti delle sedute della I sottocommissione (a cui era assegnata l'elaborazione delle disposizioni relative a diritti e doveri dei cittadini) della cd. Commissione dei 75 (Commissione per la Costituzione).

[29] Rispettivamente, Art. 38 e Art. 12, r.d. 27 febbraio 1936, n. 645.

Si segnala, ad esempio, come il primo progetto complessivo presentato dai redattori per la sezione in parola contemplasse, nel novero delle libertà civili, il "Diritto alla libertà di corrispondenza postale, telegrafica e telefonica e alla segretezza di essa"[30]. La prima formulazione della disposizione in oggetto, che si deve alla stesura preliminare dei costituenti Giorgio La Pira (DC) e Lelio Basso (PSIUP), era più articolata di quella definitiva e si componeva di quattro commi. Il primo comma recitava "La libertà e la segretezza di comunicazione e di corrispondenza in qualsiasi forma sono garantite" e fu approvato all'unanimità dai membri della sottocommissione. Il secondo precisava che "Può derogarsi a questa disposizione per specifica decisione dell'autorità giudiziaria" e fu modificato, su proposta del Presidente Umberto Tupini (DC), sostituendo la parola "specifica" con "motivata", a fini di maggiore chiarezza. Il terzo aggiungeva che "Durante il tempo di guerra, per disposizioni di legge, possono essere stabilite limitazioni e istituite censure" e fu emendato modificando l'ordine delle parole, così da prevedere che "La legge può stabilire limitazioni ed istituire censure per il tempo di guerra". Il quarto e ultimo sanciva che "La divulgazione di notizie conosciute per questi tramiti è vietata per legge" e venne approvato con la sola soppressione delle parole "per legge". La disposizione nella sua interezza fu così votata all'unanimità dai membri della I sottocommissione[31].

Come noto, il progetto di Costituzione approvato dalle tre sottocommissioni fu poi sottoposto a un'opera di amalgama e revisione da parte del cd. Comitato dei 18 (Comitato di coordinamento), della cui attività non è purtroppo stato redatto verbale alcuno, così impedendo di poter identificare le specifiche ragioni addotte per le modifiche del testo come originariamente elaborato[32]. La disposizione dedicata alla libertà e segretezza della corrispondenza confluì quindi nell'art. 9 del progetto di Costituzione che fu discusso in Assemblea plenaria nel corso del 1947, formulato come

[30] Atti della Commissione per la Costituzione, Vol. IV, Quadri di raffronto proposti, I sottocommissione, Resoconto sommario della seduta del 30 luglio 1946, 6.
[31] Atti della Commissione per la Costituzione, *cit.*, Resoconto sommario della seduta del 20 settembre 1946, 88.
[32] A proposito dei lavori della Commissione dei 75, v. L. Elia, *Il Parlamento italiano 1861-1988*, Vol. XIV, 1946-1947, Milano, Nuova CEI, 1988, 125-139, in particolare v. 129 per riferimento al Comitato di coordinamento.

segue: "La libertà e la segretezza di corrispondenza e di ogni forma di comunicazione sono garantite" (c.1); "La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria, nei casi stabiliti dalla legge" (c.2).

Già nel corso della discussione generale sul Titolo I del progetto, dedicata ai diritti civili, vi furono alcuni interventi che misero in dubbio l'adeguatezza del testo della disposizione. Per il deputato Vincenzo Tieri (Fronte dell'Uomo Qualunque), la gioia con cui il cittadino apprende dell'esistenza della garanzia di cui al primo comma "dura tuttavia solo un attimo, perché lo stesso articolo prepara già le restrizioni di tale libertà e di tale segretezza" (riferimento alle previsioni legislative che codificassero le limitazioni di cui al secondo comma)[33]. Parimenti critico nei confronti della formulazione troppo generica della disposizione fu Giovanni Leone (DC), secondo il quale conveniva esplorare l'opportunità di "precisare più rigorosamente la formulazione delle eccezioni alla libertà di corrispondenza" richiamando l'attinenza delle stesse a indagini in materia penale[34]. Con riferimento a quest'ultimo punto, il deputato Pietro Mastino (PSd'Az) eccepì che la locuzione "nei casi stabiliti dalla legge" poteva aprire la strada a un eccesso di limitazione della libertà in parola in sede giudiziale che, per quanto animata da fini di giustizia, avrebbe rischiato di non conciliare "l'interesse e le necessità delle istruttorie penali col concetto di libertà e segretezza della corrispondenza", a tal fine suggerendo l'aggiunta dell'avverbio "rigorosamente"[35].

Nell'ambito dell'esame delle disposizioni articolo per articolo, dopo avere scartato alcune proposte di emendamento all'art. 9 depositate in precedenza per l'assenza dei deputati firmatari, l'assemblea esaminò l'emendamento proposto dai deputati Orazio Condorelli (Blocco Nazionale della Libertà) e Girolamo Bellavista (Unione Democratica Nazionale), che suggeriva la soppressione del secondo comma della disposizione o, in subordine, l'aggiunta delle parole "ed in pendenza di processo penale" in coda allo stesso secondo comma. Condorelli, nel giustificare la propria

[33] Atti di discussione in Assemblea Costituente, Vol. III, Seduta del 26 marzo 1947, Intervento del deputato Tieri, 2491.
[34] Atti di discussione in Assemblea Costituente, Vol. III, Seduta del 27 marzo 1947, Intervento del deputato Giovanni Leone, 2557.
[35] Atti di discussione in Assemblea Costituente, Vol. III, Seduta del 27 marzo 1947, Intervento del deputato Pietro Mastino, 2569.

proposta, asserì che "enunciare un principio e poi aprire un amplissimo ambito, muovendosi nel quale il potere legislativo può anche distruggere il principio stesso, è un errore di tecnica"; egli aggiunse che il principio in questione andasse affermato senza alcuna limitazione, salvi i casi in cui la Costituzione prevedesse la possibilità di limitare la libertà personale o domiciliare, ma non in casi ulteriori. La tutela garantita dal testo del progetto, secondo lo stesso deputato, era ben fragile perché cedevole dinanzi al mero sospetto di un reato o di una responsabilità penale, motivo per cui la limitazione ulteriore, se prevista, avrebbe dovuto essere connessa esclusivamente alla pendenza di un processo penale[36].

La soppressione del secondo comma non fu approvata, ma l'assemblea votò a favore dell'emendamento proposto in subordine, così che la disposizione prevedesse la limitazione della libertà in parola "nei casi stabiliti dalla legge ed in pendenza di procedimento penale". È curioso notare come, in sede di coordinamento svolto dal Comitato di redazione, il testo cambiò aspetto per un'ultima volta e assunse la formulazione definitiva che ancora oggi è in vigore. Alla mera garanzia prevista dal testo approvato in assemblea plenaria si sostituì il più forte riconoscimento dell'inviolabilità delle prerogative in oggetto, peraltro specificandone l'estensione a ogni altra forma di comunicazione. Inoltre, cadde il riferimento alla pendenza di procedimento penale, la cui causa era stata perorata da alcuni deputati nel timore di un abuso da parte del legislatore della discrezionalità a esso conferita dallo stesso c.2 della disposizione; tuttavia, l'ottica dell'intervento del legislatore fu spostata dalla previsione delle eccezioni ("nei casi") alla disciplina delle garanzie da rispettare in ogni caso.

3. *Lo statuto costituzionale della libertà e segretezza della corrispondenza*

3.1. La natura della prerogativa

La rassegna dei lavori preparatori al testo offre un interessante punto di partenza per analizzare il significato e l'estensione delle tutele di cui all'art. 15 della Costituzione.

[36] Atti di discussione in Assemblea Costituente, Vol. III, Seduta del 11 aprile 1947, Intervento del deputato Orazio Condorelli, 2711-2712.

Tuttavia, il primo e inevitabile interrogativo da porsi riguarda l'oggetto specifico della garanzia costituzionale in questione, sulla cui natura i costituenti non paiono avere discusso in modo particolarmente approfondito (almeno stando ai resoconti pervenutici). Il nucleo concettuale della disposizione si determina identificando cosa si debba intendere per comunicazione, ben potendosi considerare la stessa *genus* del quale la corrispondenza è una *species* (il testo si riferisce a ogni altra forma di comunicazione, con ciò facendo chiaramente intendere di considerare la corrispondenza una manifestazione concreta di questa categoria astratta)[37].

Una dottrina risalente definisce come forme di comunicazione quei rapporti psichici diretti consistenti nella trasmissione di idee o notizie che un individuo rivolge a una o più persone determinate, per il tramite di strumenti idonei alla fissazione, trasmissione e ricezione dell'espressione del pensiero[38]. Un primo elemento chiave di un rapporto comunicativo ai sensi dell'art. 15 Cost. è dunque la presenza di destinatari ben individuati dal mittente: questo profilo è definito dalla dottrina come l'intersoggettività della comunicazione ex-art. 15 Cost. La comunicazione acquisisce tale carattere nel momento in cui sussiste, in capo al mittente, l'intenzione di far pervenire alla conoscenza di uno o più terzi il contenuto del proprio pensiero. Diversamente, fintanto che la manifestazione di tale pensiero, quand'anche fissata con modalità passibili di trasmissione al destinatario, non sia destinata dal suo autore a un determinato soggetto, non gode della copertura della disposizione in oggetto[39]. Il carattere dell'intersoggettività si coniuga con l'attualità del contenuto del messaggio, che rileva ai fini della tutela della segretezza dello stesso[40]. Infatti, l'intenzione di limitare la conoscenza del contenuto di tale messaggio ai terzi non destinatari (cd. *animus*) è il secondo elemento che contraddistingue la fattispecie in esame.

---

[37] Così P. Barile-E. Cheli, *op. cit.*, 744; P. Caretti, *op. cit.*, 201. Diversamente A. Pace, v. *infra*. Il significato di corrispondenza viene fatto coincidere con quello ai sensi delle leggi postali (così escludendo quello desunto da altre branche del diritto) da V. Italia, *Libertà e segretezza delle comunicazioni e della corrispondenza*, Milano, Giuffrè, 1963, 26, secondo il quale la corrispondenza non epistolare sarebbe libera ma non ne sarebbe garantito il segreto, 29.
[38] Così P. Barile-E. Cheli, *op. cit.*, 744.
[39] *Ibid.*, 745.
[40] P. Caretti, *op. cit.*, 202.

3.2. Comunicazione privata e comunicazione al pubblico: il valore distintivo della segretezza

La dottrina prevalente ritiene che la libertà di corrispondere o comunicare e la libertà di manifestare liberamente il proprio pensiero (art. 21 Cost.) condividano la stessa origine concettuale, ma siano distinte in quanto nella prima viene tutelata la segretezza del contenuto della comunicazione[41]. Si tratterebbe, pertanto, di forme di manifestazione del pensiero connotate da un diverso grado di diffusione, dipendente dalla volontà del mittente di raggiungere un destinatario specifico e determinato o un pubblico indistinto e generale[42]. Così argomentando, la segretezza si ritiene tale solo se esplicitamente definita dalla legge ed è una qualificazione giuridica di un rapporto, atta a tutelare la volontà di un soggetto a che certe notizie siano conosciute soltanto da coloro che egli desideri.

Pertanto, si ritiene che l'art. 15 Cost. copra solo quelle manifestazioni del pensiero indirizzate a soggetti individuati e determinati e sottratte alla conoscibilità di terzi per mezzo delle normali cautele disponibili al mittente. La comunicazione a un dato destinatario non avendo cura di adottare modalità atte a escludere i terzi dalla conoscenza del contenuto farebbe transitare la condotta nel dominio della libera manifestazione del pensiero (rivolta a un pubblico indiscriminato)[43]. L'attualità potrebbe invece venire meno una volta che, per il decorso del tempo, il contenuto della comunicazione abbia valore meramente ricostruttivo e, pertanto, non si configuri più come posizione soggettiva costituzionalmente garantita[44]. Sotto il profilo della segretezza, peraltro, la prerogativa in discorso si distingue dal cd. diritto alla privatezza o alla riservatezza (v. *infra*, §5).

---

[41] V. Italia, *op. cit.*, 62.

[42] Invero, vi è chi invece ritiene che la libertà di corrispondenza sia una delle forme in cui è disciplinata in Costituzione la libertà di espressione, non una sottospecie della libera manifestazione del pensiero, v. A. Pace, *Art. 15*, in G. Branca-A. Pizzorusso (a cura di), *Commentario della Costituzione*, Bologna, Zanichelli, 1977, 86. Parimenti scettico su tale ricostruzione è P. Giocoli Nacci, *Libertà di corrispondenza*, in G. Santaniello (a cura di), *Trattato di diritto amministrativo*, vol. XII, *Libertà costituzionali e limiti amministrativi*, Padova, 1990, 108-109.

[43] A. Pace, *Problematica delle libertà costituzionali*, *Parte speciale*, Padova, CEDAM, 1992, 247-249.

[44] Sul tema, tuttavia, dissente A. Pace (*Problematica delle libertà costituzionali*, *Parte speciale*, *op. cit.*, 246-247), il quale ritiene che l'attualità del messaggio cessi dal momento in cui esso sia stato portato alla conoscenza del destinatario; da lì in avanti la segretezza del contenuto sarebbe protetta da altri principi costituzionali (es. tutela avverso le ispezioni e le perquisizioni personali e domiciliari).

3.3. L'ambito di applicazione

Va sottolineato come, *prima facie*, la disposizione non faccia differenza fra i diversi mezzi attraverso i quali l'atto comunicativo sia trasmesso, sempre salvo il requisito dell'idoneità a garantirne la segretezza[45]. Peraltro, è proprio sulla base di questo ultimo requisito che è stato ritenuto che la disposizione copra la libertà e segretezza di comunicare riguardo a tutti i casi in cui ciò avvenga in forma espressiva, così escludendo quelle fattispecie in cui la comunicazione possa dirsi non espressiva. Tale opzione interpretativa impone di intendersi su cosa costituisca una forma espressiva: è il requisito della generale riconoscibilità a determinare la rilevanza dell'atto comunicativo ai fini della tutela costituzionale in oggetto; non si considerano invece protette dalla garanzia in parola quelle forme comunicative che siano riconosciute come tali solo sulla base di usi del mittente e del destinatario (che siano cioè solo convenzionalmente comunicative)[46].

È evidente che, adottando una lettura della disposizione vincolata alla generale riconoscibilità dell'intento comunicativo, non si àncora comunque la protezione accordata a una concezione statica. Infatti, il testo provvede già a tenere in considerazione l'evoluzione tecnologica dei mezzi di comunicazione, ricorrendo a una clausola aperta, formulata così da consentire alla disposizione di ricomprendere nella fattispecie regolata anche quelle forme di comunicazione che il costituente non poteva ancora conoscere.

Per quanto riguarda la titolarità del diritto, il riferimento alla libertà e segretezza della corrispondenza consente di identificare come beneficiario della garanzia costituzionale tanto colui che predisponga il contenuto comunicativo (mittente) quanto colui a cui il messaggio sia indirizzato (destinatario), con ciò escludendo una lettura restrittiva che riconosca la spettanza del diritto al solo autore della comunicazione[47]. Inoltre, mancando un esplicito riferimento alla spettanza in concreto del diritto alla categoria dei cittadini, la dottrina ha ritenuto, anche in ragione della peculiare posizione della prerogativa nel catalogo dei diritti e dell'identità

[45] P. Caretti, *op. cit.*, 201.
[46] A. Pace, *Art. 15*, *op. cit.*, 82-83.
[47] P. Giocoli Nacci, *op. cit.*, 111-112.

terminologica con l'art. 2 Cost. (riconoscimento e garanzia dei "diritti inviolabili dell'uomo"), che siano titolari della libertà in oggetto tutti gli individui che si trovino sottoposti alla giurisdizione territoriale italiana, senza distinzione di status fra cittadini e stranieri[48]. Peraltro, la disposizione in oggetto condivide la qualifica esplicita di diritto inviolabile con la libertà personale (art. 13 Cost.) e l'inviolabilità del domicilio (art. 14 Cost.), per le cui conseguenze si rinvia a una più diffusa trattazione nel paragrafo successivo del presente capitolo (§4).

3.4. La struttura della posizione giuridica soggettiva

Giova precisare che la disposizione dichiara che sono inviolabili la libertà e la segretezza della corrispondenza e delle altre forme di comunicazione[49]. Questa formulazione ha dato adito a descrizioni della situazione giuridica soggettiva protetta come duplice: il contenuto della prerogativa coprirebbe infatti in primo luogo la facoltà di comunicare e corrispondere con i terzi, garantendo in secondo luogo di poterlo fare mantenendo segreto l'oggetto della comunicazione medesima[50]. Questa ricostruzione consente di spiegare come, in particolari circostanze, un atto della pubblica autorità possa interferire con una delle due prerogative, senza per questo inficiare automaticamente il godimento dell'altra (es. fermo della corrispondenza senza apertura della stessa). Tuttavia, anche i sostenitori della suddetta impostazione teorica ritengono che la tutela di cui all'art. 15 Cost. identifichi la libertà come l'intero contenuto del diritto e non, invece, come un presupposto all'esercizio di un diverso diritto di corrispondere e comunicare[51].

Libertà e segretezza della corrispondenza e delle comunicazioni interagiscono così a creare un vincolo di completezza l'una con l'altra, tale per cui è proprio la loro unione a rendere essenziale la garanzia di questa duplice situazione giuridica

---

[48] C. Caruso, *La libertà e la segretezza delle comunicazioni nell'ordinamento costituzionale*, in *Forum di Quaderni costituzionali*, 21 ottobre 2013, 14.

[49] A. Pace preferisce parlare a proposito di riservatezza della comunicazione, ritenendo la segretezza una preclusione assoluta di conoscenza del contenuto, v. *Problematica delle libertà costituzionali*, *Parte speciale*, *op. cit.*, 246.

[50] Contrariamente a questa impostazione e a favore di una ricostruzione della prerogativa in oggetto come una situazione giuridica soggettiva unitaria si esprime A. Pace, *Art. 15*, *op. cit.*, 85.

[51] V. Italia, *op. cit.*, 41-43.

soggettiva ai fini della tutela della dignità umana[52]. Pertanto, la complessità di questa posizione giuridica non ne esclude una fruizione unitaria: è infatti garantita la libertà di quelle comunicazioni che siano materialmente assoggettabili a vincolo di segretezza e che lo siano poi effettivamente in concreto. Peraltro, la struttura binaria della libertà in oggetto si riverbera altresì sulla qualità della tutela che a ciascuna delle due anime della stessa viene riconosciuta. La comunicazione in sé (momento dinamico) può essere protetta anche in modo graduale, ossia essere temporaneamente limitata, purché ciò non ne pregiudichi l'effettiva ricezione da parte del destinatario. La segretezza (momento statico) del contenuto non può che configurarsi, invece, come garanzia assoluta, non essendo possibile concepire una segretezza che sia parziale (salvi, beninteso, gli interventi motivati dell'autorità giudiziaria)[53].

È proprio il riferimento all'effettività della garanzia di questo diritto a rendere opportuno interrogarsi sui limiti che, secondo la Costituzione, possono essere apposti dal legislatore ordinario al godimento della stessa (v. *infra*, §6).

4. *Libertà personale, tutela del domicilio e del segreto epistolare: quali differenze?*

La collocazione della libertà di comunicazione e della pretesa all'inviolabilità della segretezza di ogni sua manifestazione concreta all'inizio del Titolo I della Parte prima della Costituzione sembra naturalmente suggerire una lettura che ne valorizzi l'appartenenza a un insieme unitario, costituito altresì dagli artt. 13 e 14 Cost., che il costituente avrebbe predisposto allo scopo di tutelare la personalità individuale attraverso la garanzia delle sue principali manifestazioni[54].

Nonostante una certa parte della dottrina ritenga che la libertà di corrispondenza vada letta in stretta connessione con la libertà personale[55], essa è

---

[52] *Ibid.*, 92-93.
[53] C. Caruso, *op. cit.*, 5.
[54] V. Italia, *op. cit.*, 24.
[55] P. Biscaretti di Ruffia, *Diritto costituzionale*, Napoli, Jovene, 1965, 717, secondo il quale alla libertà personale si affiancano vari diritti di libertà ad essa strettamente connessi; A. Amorth, *La costituzione italiana. Commento sistematico*, Milano, Giuffrè, 1948, 60 ss., per il quale accanto alla libertà personale in senso stretto il dettato costituzionale contempla altresì alcune tipiche manifestazioni della personalità del singolo.

tuttavia considerata insussumibile sotto la stessa garanzia della tutela della libertà fisica della persona: questa concerne infatti la persona stessa, mentre quella insiste su un bene espressione della persona[56].

La prerogativa in oggetto va altresì distinta dalla inviolabilità del domicilio, in quanto essa si estende anche ai destinatari della comunicazione (cioè la sfera dei titolari della garanzia è più ampia) e, inoltre, il domicilio è una proiezione spaziale della persona, mentre la corrispondenza ne è proiezione spirituale (pertanto la violazione si configura in un caso per mezzo di un'intrusione e nell'altro tramite una sospensione)[57]. Va sottolineato, peraltro, come differente sia la formulazione tecnica delle due disposizioni: l'art. 14 sancisce l'inviolabilità del domicilio, mentre l'art. 15 dichiara che inviolabili sono la libertà e la segretezza di ogni forma di comunicazione. Pertanto, in un caso il cuore della tutela è quella particolare proiezione della persona che è il domicilio, mentre nell'altro la garanzia copre la libertà di comunicare serbando la segretezza del contenuto della comunicazione, non invece la corrispondenza stessa (che è l'oggetto dell'attività in parola).

Oltre alle distinzioni testé illustrate sotto il profilo teorico, è d'uopo sottolineare altresì una rilevante differenza pratica fra la tutela prevista all'art. 15 Cost. e quella a norma delle due precedenti disposizioni. Tanto la libertà personale quanto l'inviolabilità del domicilio, infatti, possono patire limitazioni provvisorie anche per iniziativa delle autorità di pubblica sicurezza (persino in assenza di previo provvedimento di un magistrato), purché tali condotte siano poi sottoposte a motivata convalida dell'autorità giudiziaria competente. L'inviolabilità del segreto epistolare, invece, può derivare esclusivamente da un atto motivato di un magistrato, non configurandosi in questa fattispecie in capo ad alcun altro organo dello Stato la facoltà di porre in essere condotte potenzialmente lesive della situazione giuridica soggettiva protetta dalla Costituzione, neanche in via temporanea.

La dottrina ha provato a spiegare tale differenza riconducendola a contingenti cambi di maggioranza in sede di Assemblea Costituente o comunque negando che l'assenza di un espresso riferimento al potere di polizia preventivo di cui all'art. 13, c.3

[56] V. Italia, *op. cit.*, 58.
[57] *Ibid.*, 59-61.

Cost., come richiamato all'art. 14, c.2 Cost., ostasse alla sua configurabilità anche nei confronti della libertà e segretezza della corrispondenza, auspicando in proposito una revisione del testo della disposizione[58]. Tuttavia, è stato autorevolmente obiettato che di situazione diversa si tratti, in quanto la limitazione del diritto in oggetto interferisce necessariamente anche con la sfera giuridica di un soggetto ulteriore (il terzo destinatario), e di tale considerazione è inevitabile che il costituente abbia tenuto conto[59]. Peraltro, il vivo ricordo delle angherie alle quali le libertà dei cittadini erano state sottoposte nel corso del Ventennio era ben presenti nelle menti dei Padri costituenti, i quali valutarono altresì che le interferenze nel godimento di questo diritto richiedono un dispiegamento di forze minore da parte del potere pubblico rispetto a quelle incidenti sulla libertà personale o di domicilio, ben potendo essere poste in atto anche da remoto, senza la necessaria presenza della persona o sul luogo[60].

Sottolineare questa fondamentale differenza fra la disciplina costituzionale della libertà personale e del domicilio, da un lato, e della libertà e segretezza di corrispondenza, dall'altro, consente di apprezzare la rilevanza della motivazione del provvedimento giurisdizionale che autorizza la limitazione del diritto (a proposito della riserva di giurisdizione v. *infra*, §6.2). Inoltre, accogliere tale distinzione implica accettare che possano verificarsi circostanze in cui, ad esempio, l'autorità pubblica svolga delle perquisizioni presso il domicilio di un cittadino senza che a ciò sia stata autorizzata da un giudice, ma al contempo, qualora rinvenisse in quel luogo corrispondenza non aperta, non potrebbe prenderne visione fintanto che a ciò non abbia consentito l'autorità giudiziaria.

Peraltro, giova precisare come le garanzie di cui l'art. 15 Cost. si fa alfiere non possono prestarsi a usi strumentali atti a sottrarre documenti rinvenuti sulla persona o nel luogo di domicilio alla legittima perquisizione o sequestro da parte dell'autorità di polizia a norma dell'art. 13 o dell'art. 14 Cost. mediante inserimento degli stessi in busta chiusa sigillata e asseritamente destinata a un terzo destinatario[61]. D'altro canto, tale conclusione presta inevitabilmente il fianco alla critica che l'autorità di pubblica

---

[58] *Ibid.*, 134.
[59] A. Pace, *Art. 15*, *op. cit.*, 103-106.
[60] A. Pace, *Problematica delle libertà costituzionali*, *Parte speciale*, *op. cit.*, 264.
[61] *Ibid.*, 265.

sicurezza esercita in questi casi un potere discrezionale di valutazione della credibilità dell'apparenza della corrispondenza. In ogni caso, se l'argomentazione di cui sopra conduce a un assetto potenzialmente lesivo della libertà di comunicazione (che viene compressa in conseguenza di un fermo o di un sequestro), resta impregiudicata la tutela della segretezza della stessa, su cui si può pronunciare solo il magistrato investito della questione a seguito dell'atto di polizia che interrompe il corso della (presunta) corrispondenza.

5. *Segretezza delle comunicazioni e riservatezza della vita privata*

Per tracciare in maniera chiara il perimetro della pretesa all'inviolabilità del segreto della corrispondenza e delle altre forme di comunicazione, non è sufficiente marcare le differenze fra essa e le altre disposizioni costituzionali in tema di libertà della sfera individuale. Infatti, il novero dei diritti costituzionalmente garantiti si estende ben al di là del mero dato letterale della Carta del 1948: di assoluta rilevanza sono altresì il formante dottrinale e quello giurisprudenziale, con particolare (sebbene non esclusivo) riferimento all'interprete privilegiato della Costituzione, ossia la Corte costituzionale. Più in dettaglio, appare opportuno offrire una sintetica disamina della natura di quel diritto oggi variamente declinato come alla riservatezza o alla privacy, così da poterne apprezzare le differenze con la prerogativa oggetto della presente trattazione.

5.1. *I primi passi della dottrina italiana*

Di questa pretesa giuridica soggettiva, la cui prima teorizzazione risale alla fine del XIX secolo negli Stati Uniti d'America (v. più diffusamente *infra*, Cap. III, §3.3), la dottrina italiana comincia a discutere già prima dell'avvento della Costituzione repubblicana. In principio la riflessione si sviluppa in ambito privatistico, tentando una qualificazione di questa posizione giuridica formulata nei termini di un diritto alla illesa intimità privata[62]. Essa veniva intesa come una configurazione specifica del diritto della personalità, dal cui ampio perimetro era riuscita a rendersi autonoma.

[62] M. Ferrara Santamaria, *Il diritto alla illesa intimità privata*, in *Riv. dir. priv.*, 1937, I, 168-191.

Non si limitava a un presidio avverso le violazioni del segreto della vita privata, ma offriva altresì uno schermo avverso la pubblicità di alcun dettaglio della vita della persona a cui la stessa non fosse disposta a consentire[63].

Sempre prendendo come punto di partenza quel fascio di prerogative costituito dai diritti della personalità, vi fu chi, sottolineando l'esigenza di riconoscere alla persona, in quanto tale, "una sfera relativa ai dati più gelosi e più intimi di essa e della sua attività", ne derivò la necessaria esistenza di un diritto alla riservatezza[64]. Lo stesso termine fu utilizzato da altri autori dopo la seconda guerra mondiale e all'inizio dell'età repubblicana[65], anche in polemica con chi, traendo ispirazione dalle prime pronunce dei giudici ordinari in materia[66], contestava l'esistenza di tale diritto. All'interno della stessa dottrina privatistica, vi fu chi ritenne che il termine privatezza fosse più adeguato a descrivere la pretesa individuale in discorso[67].

Nonostante le diverse formulazioni lessicali utilizzate da differenti autori, si può ritenere che fosse uniforme l'identificazione dell'interesse sottostante, consistente in un atteggiamento negativo della persona rispetto alla conoscenza (o pubblicità) di fatti della propria sfera privata da parte di altri soggetti[68]. Si può dunque imputare il primo riconoscimento del cd. diritto alla riservatezza a due soluzioni interpretative. Una prima ne ascriveva la configurabilità all'applicazione in via analogica delle norme disposte in tema di protezione del diritto all'immagine (art. 10 c.c.), da distinguersi dal caso particolare del pregiudizio al decoro o all'onore di una persona[69]. Un secondo indirizzo interpretativo riconduceva le varie disposizioni dell'ordinamento che tutelano differenti aspetti della personalità a un più generale e unitario diritto della

---

[63] *Ibid.*, 169-170.

[64] A. Ravà, *Istituzioni di diritto privato*, Padova, CEDAM, 1938, 157. Gli studi dello stesso Ravà sui diritti della persona e sulla personalità, peraltro, datano già ad alcuni decenni prima, v. *Id.*, *I diritti sulla propria persona nella scienza e nella filosofia del diritto*, Torino, Fratelli Bocca, 1901.

[65] A. De Cupis, *Il diritto alla riservatezza esiste*, in *Foro it.*, 1954, 4, 89-97. L'A. si era già espresso in questi termini negli anni precedenti, v. *Id.*, *Il diritto all'onore e il diritto alla riservatezza*, Milano, Giuffrè, 1948, 41 ss.

[66] V., a titolo di esempio, Trib. Roma, 14 settembre 1953 (caso Caruso), in *Foro it.*, 1954, 1, 115-133.

[67] F. Carnelutti, *Diritto alla vita privata (contributo alla teoria della libertà di stampa)*, in *Riv. trim. dir. pubbl.*, 1955, 5 ss., secondo il quale "tra *riservato* e *privato* corre una differenza … la riservatezza è piuttosto una disposizione dell'animo che un modo di vivere esteriore" (corsivo nell'originale).

[68] T.M. Ubertazzi, *Il diritto alla privacy. Natura e funzioni giuridiche*, Padova, CEDAM, 2004, 50-51; in precedenza già T.A. Auletta, *Riservatezza e tutela della personalità*, Milano, Giuffrè, 1978, 28.

[69] A. De Cupis, *I diritti della personalità*, Milano, Giuffrè, 1950, 110.

personalità, da concepirsi come esorbitante la mera somma dei diritti riconosciuti espressamente dal diritto positivo[70].

5.2. Il contributo della giurisprudenza ordinaria e costituzionale

La giurisprudenza ordinaria di questi primi decenni, inizialmente relativa a casi di realizzazione di opere cinematografiche che riproducevano episodi della vita di personaggi pubblici, lungi dallo sciogliere il nodo, si mosse fra l'una e l'altra ricostruzione, senza consolidare un orientamento uniforme. L'unico dato di sistema che si possa legittimamente trarre da questa serie di pronunce è una concezione dell'interesse alla riservatezza come concernente una dimensione prettamente domestica[71].

Pochi anni dopo, la Corte di cassazione cominciò a prendere atto delle numerose obiezioni sorte in dottrina con riferimento al principio di diritto sancito dalla stessa Suprema Corte in una pronuncia risalente a pochi anni prima. Il giudice di legittimità aveva infatti precedentemente negato che un diritto alla riservatezza si potesse rintracciare nel diritto positivo e aveva parimenti escluso una sua derivabilità da diversi diritti soggettivi della personalità per il tramite dell'analogia[72]. La Corte di cassazione, pur senza spingersi a sancire l'esistenza di un diritto alla riservatezza, riconobbe l'art. 2 Cost. come fondante un diritto alla libera autodeterminazione nello svolgimento della personalità, la cui lesione sarebbe consistita nella divulgazione di notizie riguardanti la vita privata che, per loro natura, dovessero considerarsi riservate[73].

Dove non arrivò la giurisprudenza ordinaria, intervenne infine la Corte costituzionale, la quale respinse una questione di legittimità costituzionale riguardante, fra le altre disposizioni, anche l'art. 10 c.c. La Consulta affermò che esse erano finalizzate a realizzare gli scopi di cui all'art. 2 Cost., ribaditi agli artt. 3, c.2 e 13,

---

[70] Capofila di tale ricostruzione, di chiaro stampo monista, fu G. Giampiccolo, *La tutela giuridica della persona umana e il c.d. diritto alla riservatezza*, in *Riv. trim. dir. e proc. civ.*, 1958, 458-475.
[71] T.M. Ubertazzi, *op. cit.*, 56.
[72] Cass. civ., Sez. I, n. 4487/1956, 22 dicembre 1956, (ancora sul cd. caso Caruso), in *Foro It.*, 80, 1, 4-11, 1957.
[73] Cass. civ., Sez. II, 10 maggio 1963, n. 1149, in *Foro It.*, 86, 5, 1963, 874-877.

c.1 Cost., i quali riconoscono e garantiscono i diritti inviolabili dell'uomo, nel cui elenco il giudice costituzionale menzionò altresì la riservatezza, rinviando a questo proposito alle disposizioni in materia della Convenzione europea dei diritti dell'uomo[74].

Dalla precedente concezione della *privacy* intesa come protezione eminentemente domestica, la Suprema corte cominciò ad allargare la proiezione di tale prerogativa, che rimase tuttavia confinata, anche in ragione di un più ridotto avanzamento tecnologico del nostro Paese rispetto a quanto avveniva oltreoceano, alle categorie sociali più esposte per ragioni di prestigio o di incarichi ricoperti. Dopo averne illustrato la compatibilità con i principi costituzionali rilevanti in materia (artt. 2, 3, 13, 14, 15, 29 Cost.), il giudice di legittimità riconobbe infatti la consistenza di tale diritto "nella tutela di quelle situazioni e vicende strettamente personali e familiari, le quali, *anche se verificatesi fuori del domicilio domestico*, non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione e il decoro, non siano giustificate da interessi pubblici preminenti"[75].

Questa pronuncia valeva già a superare la concezione di riservatezza che il legislatore aveva appena posto alla base dell'introduzione del delitto di interferenze illecite nella vita privata (art. 615-bis c.p.)[76], che non circoscriveva la sfera di garanzia allo spazio domiciliare fisico, ma comunque non abbracciava ancora l'idea della riservatezza come pretesa attiva di controllo dell'utilizzo dei dati. Quest'ultima concezione andò diffondendosi a scapito di quella meramente individualistica e limitata al diritto a essere lasciati in pace: negli anni '70, infatti, l'attenzione tese a spostarsi dalla protezione della segretezza dell'informazione al controllo sull'uso che dell'informazione viene fatto, con una prospettiva a rilievo marcatamente collettivo[77].

Sul finire del decennio, un ulteriore indirizzo interpretativo ricostruì il diritto alla riservatezza in un'ottica strumentale rispetto alla tutela della dignità e libertà della persona. La tutela avverso la diffusione di informazioni riguardanti la vita privata di

---

[74] Corte cost., sent. n. 38/1973, Cons. dir. §2.
[75] Cass. civ., Sez. I, 27 maggio 1975, n. 2129 (cd. caso Soraya), in *Foro It.*, 99, 1, 1976, 2895-2907 (corsivo aggiunto).
[76] Art. 1, l. 8 aprile 1974, n. 98.
[77] S. Rodotà, *La "privacy" tra individuo e collettività*, in *Politica del diritto*, 5, ottobre 1974, 545-563.

un cittadino, si argomentava, deriva perciò dalla necessità di procedere a un bilanciamento degli interessi riconosciuti sotto il profilo costituzionale, ma fra loro confliggenti, della circolazione di informazioni e della protezione di dignità e libertà degli individui, da operarsi da parte del legislatore ordinario in prima istanza e dal giudice in via sussidiaria[78].

5.3. L'intervento del legislatore

Gli anni '80 furono caratterizzati da una crescente attenzione al tema in oggetto, senza che tuttavia i vari progetti di legge a tal proposito fossero effettivamente portati a compimento dal Parlamento, il quale parve, in ogni caso, sempre più propenso ad accogliere una concezione ampia del diritto alla riservatezza, che includesse anche il controllo sull'utilizzo dei dati personali[79]. La non più trascurabile espansione dell'utilizzo della rete Internet nella vita quotidiana dei cittadini e l'influenza delle fonti di rango comunitario hanno infine condotto il legislatore italiano a prendere l'iniziativa sul tema a partire dalla seconda metà degli anni '90.

Il primo atto di cui dare conto è la l. 31 dicembre 1996, n. 375 (*Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*), che si prefiggeva di garantire che il trattamento dei dati personali si svolgesse "nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla *riservatezza* e all'identità personale"[80]. Tale atto è stato poi abrogato con l'esercizio della delega legislativa attraverso la quale il governo ha predisposto il cd. "Codice in materia di protezione dei dati personali" (d.lgs. 30 giugno 2003, n. 196), esplicitamente finalizzato ad assicurare che "il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla *riservatezza*, all'identità personale e al diritto alla protezione dei dati personali"[81].

---

[78] A. Belvedere, *Riservatezza e strumenti di informazione*, in N. Irti (a cura di), *Dizionari di diritto privato*, Giuffrè, Milano, 1980, I, 750-752.
[79] T.M. Ubertazzi, *op. cit.*, 73-75.
[80] Art. 1, l. 31 dicembre 1996, n. 375 (corsivo aggiunto).
[81] Art. 2, c.1, d.lgs. 30 giugno 2003, n. 196 (versione in vigore fino 18 settembre 2018) (corsivo aggiunto).

L'ambito della tutela dei dati personali è uno di quelli nei quali l'influenza del diritto dell'Unione Europea negli ordinamenti degli Stati membri è più evidente. A questo proposito, si rinvia a quanto si dirà *infra*, Cap. III, §1.3.

5.4. Affinità e differenze

La sintetica disamina del dibattito pluridecennale alimentato dalla dottrina e dalla giurisprudenza italiana in materia di diritto alla *privacy* (come variamente declinato dai diversi interpreti) consente quindi di identificare alcuni caratteri che differenziano l'inviolabilità della segretezza delle comunicazioni e la riservatezza della vita privata. Per quanto a prima vista le due prerogative possano apparire quasi sovrapponibili, esse si differenziano infatti sotto il profilo della sfera giuridica sulla quale ciascuna prerogativa incide. D'altronde, se entrambe si connotano per un'esigenza di riservatezza in senso generico, la segretezza delle comunicazioni si distingue per il momento dinamico della trasmissione del contenuto comunicativo, configurandosi come funzionale alla comunicazione intersoggettiva[82].
Infine, la dottrina ha distinto il diritto individuale di intimità in due dimensioni, l'una personale e l'altra privata: alla prima categoria, che implica una valutazione del grado di intimità pari a quello di ciò che sia collocato sulla persona, apparterrebbe la pretesa di inviolabilità della segretezza di ogni forma di comunicazione; alla seconda, invece, apparterrebbero la tutela del domicilio e il diritto cd. alla privatezza[83].

Siffatta distinzione sul piano teorico si riflette sull'oggetto della protezione di ciascuna delle posizioni giuridiche soggettive. Mentre il diritto alla segretezza delle comunicazioni tutela le parti del rapporto comunicativo avverso l'illegittima conoscenza del contenuto del messaggio, il diritto alla riservatezza tutela il singolo avverso l'abuso della legittima conoscenza degli elementi esteriori e del contenuto di una data corrispondenza[84]. D'altronde, così configurata la distinzione, sembra potersi affermare che l'una pretesa sia la logica prosecuzione dell'altra, tramutandosi il diritto all'inviolabilità del segreto della corrispondenza, una volta che di essa abbia preso

[82] C. Caruso, *op. cit.*, 7.
[83] V. Italia, *op. cit.*, 73-74.
[84] V. Italia, *op. cit.*, 87.

conoscenza il destinatario, per estinzione, in un diritto alla riservatezza riferito tanto ai dettagli che identifichino gli estremi della comunicazione, quanto al contenuto concreto della stessa[85].

6. *I limiti alla tutela costituzionale del segreto epistolare*

All'inviolabilità di libertà e segretezza della corrispondenza il secondo comma dell'art. 15 Cost. affianca, come già premesso, un'ipotesi di deroga al principio stesso, prevedendo che una limitazione delle prerogative in oggetto possa avere luogo, ma solo ove disposta tramite atto motivato dell'autorità giudiziaria e nel rispetto delle garanzie stabilite dalla legge. Come dettato altresì in ordine alla libertà personale, il testo costituzionale presidia il diritto in questione tramite la previsione di una riserva di legge formale e una riserva di giurisdizione[86].

6.1. Natura della riserva di legge

La dottrina qualifica la riserva di legge in oggetto come assoluta, in quanto attinente all'ambito dei diritti inviolabili ex-art. 2 Cost. e poiché l'interesse alla tutela del diritto in oggetto non può essere soddisfatto da una mera disciplina di principio, la cui specificazione nel dettaglio spetterebbe al Governo nell'esercizio della propria potestà regolamentare[87]. Tuttavia, a differenza di quanto previsto dall'art. 13 Cost., l'art. 15 Cost. non richiede espressamente che la legge individui i casi di limitazione del diritto, limitandosi a sancire che la legge stabilisce le garanzie che presiedano alla limitazione – per effetto di un provvedimento giurisdizionale – della prerogativa in questione[88]. Ciò ha condotto una parte della dottrina ad affermare che la legge non sia chiamata a stabilire le modalità attraverso le quali tale compressione della pretesa giuridica del

---

[85] V. Italia, *op. cit.*, 169. A questa conclusione si perviene, peraltro, aderendo all'ipotesi secondo la quale la conoscenza del contenuto del messaggio da parte del destinatario è causa di estinzione della pretesa di segretezza, v. A. Pace, *Problematica delle libertà costituzionali*, *Parte speciale*, *op.cit.*, *supra* in nota 44, 246-247.

[86] C. Troisio, *Corrispondenza (libertà e segretezza della)*, in *Enciclopedia giuridica Treccani*, IX, 1988, 6; v. anche A. Valastro, *Libertà di comunicazione e nuove tecnologie. Inquadramento costituzionale e prospettive di tutela delle nuove forme di comunicazione interpersonale*, Milano, Giuffrè, 2001, 102.

[87] P. Giocoli Nacci, *op. cit.*, 123.

[88] V. Italia, *op. cit.*, 127-128.

soggetto può avvenire, ma che spetti al giudice soltanto valutare quando ciò sia necessario[89].

Adottandosi tale prospettiva, la riserva andrebbe considerata semplice, e non rinforzata, perché il legislatore, per quanto tenuto a dettare la disciplina nella sua interezza, sarebbe investito del solo compito di regolare discrezionalmente le accortezze che l'autorità giudiziaria deve adottare in concreto per circoscrivere quanto più possibile la compressione del diritto in parola[90]. Il legislatore non potrebbe quindi limitare l'esercizio del potere del giudice in sé e per sé, ma sarebbe intitolato ad agire sulle modalità concrete dell'esercizio di tale potere, così da garantirne una minore intrusività nel godimento del diritto. Peraltro, tale interpretazione implica la conseguenza che le limitazioni del diritto di cui all'art. 15, c.2 Cost. siano passibili di immediata applicazione, non dovendosi attendere un intervento del Parlamento volto a delineare le fattispecie in cui sia autorizzata l'interferenza con le prerogative in oggetto (come invece si ritiene valga per la libertà personale e l'inviolabilità del domicilio, salvi i casi di necessità e urgenza di cui all'art. 13, c.2 Cost.)[91].

Un diverso indirizzo interpretativo, che fa leva sulla giurisprudenza costituzionale in materia di intercettazioni telefoniche[92] (su cui v. *infra,* Cap. II.2), ritiene più corretta una lettura sistematica della disposizione. L'operazione ermeneutica richiederebbe infatti all'interprete di integrare lo scarno contenuto dell'art. 15, c.2 Cost. con il più rigoroso dettato di cui all'art. 13, c.3 Cost., così rinvigorendo la riserva di legge contenuta nella prima disposizione, altrimenti non sufficiente, di per sé, a proteggere dalle ingiustificate interferenze nel godimento del diritto[93]. Ciò significherebbe attribuire al legislatore il compito non solo di disciplinare le garanzie relative all'esercizio del potere del giudice di disporre atti limitativi della libertà o del segreto della corrispondenza, ma altresì di dettagliare i casi in cui ciò possa avvenire.

---

[89] P. Giocoli Nacci, *op. cit.*, 122.
[90] *Ibid.*, 123-4.
[91] *Ibid.*, 124-125.
[92] Sviluppatasi a partire da Corte cost., sent. 34/1973.
[93] C. Caruso, *op. cit.*, 9.

Peraltro, questa seconda lettura testimonia un tendenziale scetticismo nella capacità del giudice di determinare in concreto quando sussista la necessità di ricorrere ad atti tanto intrusivi e introduce un significativo temperamento a una discrezionalità dell'autorità giudiziaria altrimenti cospicua (su cui, in ogni caso, vale quanto detto con riferimento alla motivazione del provvedimento, v. *infra,* Cap. II, §2.4). L'identificazione di esigenze che giustifichino il sacrificio (anche parziale o temporaneo) di una situazione giuridica soggettiva individuale viene così riportato in una cornice definita dal legislatore e meno affidata al libero convincimento del giudice.

6.2. Natura della riserva di giurisdizione

Come anticipato, libertà e segretezza della corrispondenza sono altresì presidiate da una riserva di giurisdizione, che si estrinseca in due direzioni. In primo luogo, essa assicura che spetti alla autorità giudiziaria – e a essa soltanto – la decisione concreta di limitare il diritto in questione. In secondo luogo, il provvedimento giudiziale è provvisto di motivazione, così da assicurare la possibilità di sottoporlo a verifica di legittimità qualora impugnato[94].

Per quanto attiene al primo profilo, sebbene il costituente avesse in mente l'autorità giudiziaria penale nella stesura della disposizione, la dottrina non esclude che esigenze di limitazione del diritto in questione possano legittimamente sorgere con riferimento alla giurisdizione civile o alle giurisdizioni speciali previste dalla Costituzione stessa[95]. D'altronde, alcune criticità a riguardo possono configurarsi laddove la legge autorizzi un'amministrazione statale a limitare la libera circolazione della corrispondenza epistolare (o assimilata) senza il previo intervento di un provvedimento giurisdizionale. Il caso più evidente fu quello della disposizione del codice postale risalente all'epoca fascista che investiva la stessa amministrazione delle poste del potere di non recapitare la corrispondenza passibile di essere pericolosa per la sicurezza dello Stato o di cagionare danni o persone o cose o comunque contraria a leggi, buon costume od ordine pubblico[96]. La Corte costituzionale ne dichiarò la non conformità a Costituzione proprio per la violazione della riserva di giurisdizione di

[94] *Ibid*.
[95] V. Italia, *op. cit.*, 118-120; P. Giocoli Nacci, *op. cit.*, 125.
[96] Art. 13, r.d. 27 febbraio 1936, n. 645.

cui all'art. 15, c.2 Cost., affermando che "l'attribuzione all'Amministrazione postale del potere, discrezionale ed autonomo, di non dar corso alla corrispondenza" configura una norma che, esponendo la libertà di corrispondenza a possibili limitazioni e ingerenze senza la garanzia dell'intervento dell'autorità giudiziaria, viola il dettato costituzionale[97].

La disciplina subentrata in pendenza della pronuncia della Consulta (l. 20 dicembre 1966, n. 1114) fu invece, nella medesima pronuncia, dichiarata costituzionalmente legittima: la previsione di un obbligo di trasmissione tempestiva della corrispondenza fermata al pretore (il cui decreto era impugnabile dinanzi al tribunale) e la sottrazione di qualsivoglia margine di discrezionalità sull'inoltro della corrispondenza all'amministrazione postale fu considerato "sostanzialmente valido ed idoneo ad attuare la tutela del diritto del singolo all'inviolabilità della corrispondenza"[98]. Questa ricostruzione fu fatta propria anche dalla Corte di cassazione, la quale rifiutò di sollevare una questione di legittimità costituzionale relativamente al nuovo testo della disposizione sul fermo postale, adducendo le ragioni di cui alla summenzionata pronuncia della Consulta[99].

Invero, anche una tale disciplina presenta alcune problematiche, non potendosi negare come la libertà della corrispondenza subisca in ogni caso una limitazione da parte dell'autorità amministrativa preposta alle poste, per quanto parziale e temporanea. D'altronde, pare difficile prospettare una soluzione diversa che coinvolga direttamente l'autorità giudiziaria, rimanendo in capo a un'amministrazione dello Stato una prima e imprescindibile fase di filtro. Per questa ragione, si può ritenere che esista una presunzione assoluta di illegittimità degli interventi che interferiscano con il profilo della segretezza senza previo coinvolgimento dell'autorità giudiziaria, mentre opera una presunzione solo relativa con riferimento alla limitazione del profilo

[97] Corte Cost., sent. 100/1968.
[98] *Ibid.*
[99] Cass. civ., Sez. I, 30 ottobre 1969, n. 3593. Peraltro, ritiene la disposizione illegittima anche nella versione riformata, criticando l'appiattimento della Suprema Corte sulle ragioni della Consulta e l'inconfigurabilità di un limite generale di sicurezza pubblica alle libertà costituzionali, R. Zaccaria, *Il «fermo» della corrispondenza ha ancora finalità censorie?*, in *Foro It.*, 1970, 7/8, 1980-1987.

della libertà, la cui valutazione dipende dalla strumentalità della stessa al controllo di un giudice[100].

Più spinoso è il secondo profilo relativo alla riserva di giurisdizione, ovvero quello attinente all'obbligo di motivazione particolarmente rigoroso, in quanto incidente su un diritto inviolabile riconosciuto alla generalità dei soggetti sottoposti alla giurisdizione dello Stato. Per quanto la motivazione sia un requisito prescritto per tutti i provvedimenti giurisdizionali dall'art. 111, c.6 Cost., nel caso in questione la sua funzione è ancora più rilevante, in quanto è solo in conseguenza di un libero convincimento formatosi in seno all'autorità giudiziaria che l'interferenza pubblica con il godimento del diritto può verificarsi. Si tratta quindi di misure la cui attuazione dipende in ogni caso (salva la parziale eccezione di cui sopra riferita al fermo postale) da una decisione del giudice, che è dunque investito di un controllo diretto sull'operato degli organi di polizia fin dal principio.

È stata la Corte costituzionale a rendere plasticamente la centralità del ruolo dell'organo giurisdizionale, con particolare riferimento al caso delle intercettazioni telefoniche. La Consulta ha infatti prescritto "cautela scrupolosa" nell'emanazione di provvedimenti di tal fatta e ha invitato il giudice a contemperare gli interessi divergenti della tutela del segreto delle comunicazioni e della repressione dei reati. Il giudice deve dare conto dell'accertamento di effettive esigenze dell'amministrazione della giustizia e della sussistenza di fondati motivi di ritenere che tramite tale iniziativa siano acquisiti risultati utili alle indagini, stendendo un'adeguata e specifica motivazione[101].

Appare evidente come l'identificazione del *quantum* di motivazione che sia conforme ai criteri della giurisprudenza costituzionale in materia è la chiave di volta per poter valorizzare la riserva di giurisdizione al meglio senza snaturarne l'originaria funzione di garanzia nei confronti di ciascun individuo. Peraltro, si deve interpretare il potere attribuito al giudice come limitato, per ambito, al contesto del procedimento in atto e per soggetto, poiché solo le parti in causa possono conoscere il contenuto della corrispondenza o comunicazione in parola in quanto acquisita al fascicolo processuale.

---

[100] C. Caruso, *op. cit.*, 10.
[101] Corte cost., sent. 34/1973.

Tale precisazione consente di apprezzare come, pur in un'ipotesi di interferenza con il godimento del diritto, viene esperito un tentativo di non svuotare del tutto il principio costituzionale di contenuto[102]. L'ampio tema dei confini del potere di limitazione della libertà e della segretezza di comunicazione e corrispondenza a fini processual-penalistici verrà trattato più approfonditamente nel cap. II con riferimento alla corrispondenza epistolare e alla comunicazione telefonica e nel cap. IV con riferimento alle tecnologie di più recente introduzione.

6.3. Le limitazioni disposte dalla legge

La limitazione della libertà e segretezza della corrispondenza non è però circoscritta all'ambito delle indagini penali, in quanto la normativa in vigore consente altresì delle deroghe all'inviolabilità sancita dall'art. 15, c.2 Cost. sulla base di specifiche circostanze di fatto (diverse, come ovvio, da esigenze processuali) o della posizione soggettiva del mittente o del destinatario della comunicazione.

6.3.1. Limitazioni in tempo di guerra

Con riferimento alla prima delle due categorie, giova ricordare come, nel progetto redatto e approvato dalla I sottocommissione della Commissione dei 75 in Assemblea Costituente, la disposizione relativa alla garanzia della libertà e segretezza della corrispondenza fosse corredata da un terzo comma, che autorizzava la legge a introdurre delle forme di censura ove fosse deliberato lo Stato di guerra (v. *supra*, §2). La decisione del Comitato di coordinamento di eliminare questa parte della disposizione si fa risalire alla (malriposta) convinzione dei membri dello stesso che un articolo *ad hoc* relativo alla sospensione dei diritti fondamentali dei cittadini sarebbe stato incluso nella Parte II della Costituzione, all'interno del titolo dedicato al Parlamento[103].

Se è pur vero che il testo della Costituzione non contiene, nella sua versione licenziata in via definitiva dall'Assemblea costituente, una tale disposizione, si ritiene che il dettato dell'art. 78 Cost. offra un appiglio sicuro ai sostenitori della tesi secondo

[102] P. Giocoli Nacci, *op. cit.*, 132.
[103] P. Barile-E. Cheli, *op. cit.*, 751.

la quale lo Stato di guerra legittima l'adozione di misure che incidano anche sulle libertà inviolabili (fra cui quella riconosciuta dall'art. 15 Cost.). D'altronde, la deliberazione dello Stato di guerra da parte delle Camere si accompagna al contestuale conferimento al Governo dei poteri necessari. Nell'ambito di tali poteri, argomenta la dottrina, rientrano anche quelli volti a limitare il godimento di diritti o libertà garantite dalla Costituzione. È sulla base di tale argomentazione che è stata a posteriori ritenuta conforme al dettato costituzionale la previsione contenuta nella cd. legge di guerra (r.d. 8 luglio 1938, n. 1415) che autorizza il Governo (tramite decreto presidenziale) a sottoporre a censura o controllo la corrispondenza epistolare e ogni tipo di comunicazione e a sospendere, limitare o modificare i servizi di comunicazione operanti all'interno o all'esterno del territorio dello Stato[104].

6.3.2. Limitazioni in tempo di pace

Diversa sorte hanno avuto le disposizioni del Tulps relative alla sospensione dei diritti costituzionali di libertà in tempo di pace, ove si verifichino circostanze tali da determinare uno stato di pericolo pubblico o di guerra interna (anche noto come "stato d'assedio")[105]. Infatti, con l'entrata in vigore della Costituzione repubblicana è da escludersi che le autorità governative (prefetto o ministro dell'Interno) possano ritenersi legittimate a sospendere il godimento dei diritti costituzionalmente garantiti. L'unica eccezione, con riferimento alle circostanze in oggetto, si potrebbe delineare con l'adozione di un decreto-legge del Governo, che almeno coinvolga il Parlamento nel procedimento di convalida delle decisioni degli organi esecutivi[106].

Per quanto invece riguarda la condizione personale di una delle parti del rapporto comunicativo, il primo gruppo di soggetti su cui è opportuno riflettere è quello costituito dai detenuti. Il regolamento per gli istituti di prevenzione e di pena (r.d. 18 giugno 1931, n. 787), risalente all'epoca fascista, prevedeva che costoro non potessero ricevere o inviare lettere senza che le stesse fossero prima state lette e vistate dalle autorità preposte alla loro custodia. Inoltre, l'autorità giudiziaria poteva disporre la necessità di un proprio visto anche con riferimento alla corrispondenza di soggetti

[104] Art. 19, c.1, n. 2 e Art. 20, n. 1.
[105] Artt. 214-217, Testo Unico delle Leggi di Pubblica Sicurezza (r.d. 18 giugno 1931, n. 773).
[106] P. Barile-E. Cheli, *op. cit.*, 751.

meramente imputati. Infine, si prevedevano limiti quantitativi e preclusioni alla corrispondenza con altri detenuti[107].

Tale severa impostazione originaria, invero giustificata (almeno con riferimento a chi fosse in stato di detenzione a seguito di sentenze passate in giudicato) da alcune autorevoli voci come conseguenza della generale restrizione della libertà personale discendente dalla pronuncia di una sentenza penale di condanna[108], fu in un primo tempo temperata con l'entrata in vigore della legge sull'ordinamento penitenziario, che sancì la necessità di un provvedimento motivato *ad hoc* della magistratura di sorveglianza per sottoporre a visto preventivo la corrispondenza dei detenuti[109]. Dopo una serie di modifiche dell'art. 18 o.p., relativo a colloqui, corrispondenza e informazione dei detenuti, il Parlamento si è infine risolto a eliminare dal testo la possibilità di sottoporre a visto la corrispondenza dei detenuti[110]. Peraltro, la spettanza del diritto ai detenuti è stata ribadita di recente dalla Corte costituzionale in un giudizio sulla legittimità costituzionale dello stesso art. 18 della legge sull'ordinamento penitenziario[111].

Risolta nei termini di cui sopra la risalente limitazione della libertà nei confronti dei detenuti, occorre occuparsi di altre categorie soggette a limitazioni a opera di fonti primarie. Ben più controversa, infatti, risulta la disciplina dettata dalla cd. legge fallimentare (r.d. 16 marzo 1942, n. 267), a norma della quale la corrispondenza destinata al fallito deve essere consegnata al curatore, che trattiene quella riguardante interessi patrimoniali, sempre salvo il diritto del fallito di prenderne visione e sotto obbligo, per il curatore, di non rivelare a terzi il contenuto estraneo agli interessi patrimoniali[112].

Se anche l'autorità giudiziaria è indirettamente coinvolta nella vicenda, avendo pronunciato una sentenza dichiarativa del fallimento che incide sullo status del

---

[107] Artt. 103, 104 e 105, r.d. 18 giugno 1931, n. 787.
[108] P. Barile-E. Cheli, *op. cit.*, 752.
[109] Art. 18, c.5, l. 26 luglio 1975, n. 354; il principio fu conservato anche all'esito della riforma della disposizione a opera dell'Art. 2, l. 12 gennaio 1977, n. 1 (la disposizione divenne l'art. 18, c.7 o.p.).
[110] Art. 3, c.2, l. 8 aprile 2004, n. 95.
[111] Corte cost., sent. 20/2017; a proposito, si veda D. Coduti, *Libertà e segretezza della corrispondenza dei detenuti nella sentenza n. 20 del 2017 della Corte costituzionale*, in *federalismi.it*, Focus Human Rights N.2, 28 luglio 2017.
[112] Art. 48 legge fallimentare (regio decreto 16 marzo 1942, n. 267).

destinatario della detta corrispondenza[113], sembra difficile poter conciliare la severità dell'interferenza con la segretezza epistolare autorizzata dalla legge in questa circostanza con la tutela della stessa garantita dalla Costituzione. D'altronde, l'intervento del giudice nelle vicende di cui sopra è relativo al mero accertamento della sussistenza dei requisiti della dichiarazione di fallimento, non essendo contemplato alcun onere di motivazione nei confronti della limitazione delle libertà costituzionalmente riconosciute al fallito[114]. È stato sostenuto che più conforme al dettato costituzionale sarebbe una modifica della disposizione nel senso di consentire al fallito di attendere egli stesso allo spoglio della corrispondenza a lui indirizzata (almeno nella parte non esteriormente riconducibile ad attività commerciali), salvo l'obbligo di consegnare immediatamente al curatore le missive relative a interessi patrimoniali (sanzionando penalmente l'inosservanza)[115].

A una simile compressione della libertà in parola soggiacciono coloro che, in conseguenza del riconoscimento di uno stato di infermità mentale, siano stati dichiarati interdetti da un giudice[116]. L'art. 34, lett. b) del risalente regolamento di esecuzione del codice postale (All. A, r.d. 18 giugno 1940, n. 689) prevedeva infatti che la corrispondenza destinata a persone in stato di demenza dovesse essere consegnata ai tutori degli stessi oppure essere trattenuta dall'autorità preposta su richiesta di chi potesse avervi interesse, fino a che l'autorità giudiziaria avesse preso una decisione a riguardo. La disposizione è stata abrogata con l'entrata in vigore del successivo analogo regolamento, che invero riproduce il testo precedente se non per il riferimento alle persone in stato di infermità mentale (art. 35, d.P.R. 29 maggio 1982, n. 655).

Se si ritiene che la *ratio* sottostante alla limitazione in parola sia in buona sostanza affine a quella addotta per giustificare la limitazione della prerogativa a danno di detenuti e falliti, è stato sostenuto che, in questo caso, la disposizione si estenda anche alle missive di cui l'interdetto sia mittente[117] (anche se una interpretazione fedele al dato letterale sembrerebbe escludere l'applicabilità della

---

[113] Grado di coinvolgimento ritenuto sufficiente da P. Barile-E. Cheli, *op. cit.*, 752.
[114] P. Giocoli Nacci, *op. cit.*, 129-130.
[115] A. Pace, *Problematica delle libertà costituzionali*, *Parte speciale*, *op. cit.*, 261.
[116] Art. 34, c.1, b), r.d. 18 aprile 1940, n. 689, poi modificato dall'art. 35 d.P.R. 29 maggio 1982, n. 655. Esclude dal novero dei destinatari della norma coloro che siano meramente inabilitati A. Pace, *ibid*.
[117] P. Barile-E. Cheli, *op. cit.*, 752.

regola a una fattispecie che, nei fatti, è diversa). Peraltro, è stato argomentato che un ruolo preponderante riveste in materia l'art. 32 Cost., a norma del quale l'esercizio dei diritti di libertà può essere limitato allorché esso sia passibile di arrecare un danno alla salute del titolare: è questo il caso di una persona inferma di mente, il cui già fragile equilibrio psichico è più facilmente soggetto a turbamento a fronte di determinate comunicazioni[118]. Ancor più controversa è la legittimità della previsione secondo la quale sarebbe sufficiente addurre lo stato di infermità mentale di un soggetto affinché l'amministrazione preposta debba sospendere la consegna della corrispondenza, in quanto l'unica fonte il cui pronunciamento sullo status delle persone sia vincolante è l'autorità giudiziaria[119].

La medesima disposizione di cui al regolamento di esecuzione del codice postale prevede altresì che la corrispondenza destinata a coloro che servano nell'esercito o in altre forze armate assimilate sia consegnata a persone appositamente indicate a riceverla da parte dei comandanti competenti. Si tratta di norma meramente volta a consentire di individuare il soggetto autorizzato a ricevere materialmente le missive, senza per ciò stesso significare che costoro possono limitare il corso di tale corrispondenza o prendere visione del contenuto della stessa[120]. Quanto appena detto vale anche per le comunicazioni epistolari dirette ai detenuti (a differenza della disciplina previgente, v. *supra*), a coloro che siano ricoverati in istituti di beneficenza o agli alunni di istituti educativi.

6.3.3. Come muta la natura delle limitazioni

La rassegna dei limiti desumibili dal testo costituzionale alla compressione delle garanzie di cui all'art. 15 Cost. consente pertanto di focalizzare l'interesse dell'analisi sulla natura e la disciplina degli strumenti tecnici e delle misure attraverso le quali la forza pubblica ha storicamente interferito con il diritto di ciascun individuo di poter mantenere riservato il contenuto delle proprie comunicazioni. Seguendo un approccio di natura diacronica, si procederà ad occuparsi delle comunicazioni postali, su cui già in parte si sono svolte considerazioni *supra*, per poi occuparsi delle tecnologie

[118] A. Pace, *Problematica delle libertà costituzionali, Parte speciale, op. cit.*, 261-262.
[119] P. Giocoli Nacci, *op. cit.*, 131.
[120] A. Pace, *Problematica delle libertà costituzionali, Parte speciale, op. cit.*, 263.

attraverso le quali, a partire dal XX secolo, è possibile captare le conversazioni orali fra persone lontane (tramite intercettazione telefonica) o fra compresenti (intercettazione ambientale).

La verifica dell'influenza che il diritto europeo (inteso tanto come fonti dell'Unione Europea quanto come CEDU) ha esercitato sull'ordinamento nazionale e il confronto sull'impostazione tradizionale adottata sul tema da ordinamenti continentali di *Civil Law*, affiancati alla ricostruzione del diverso assetto della materia nel contesto di *Common Law* d'oltreoceano, consentono di tracciare un quadro complessivo della tutela costituzionale di questa prerogativa al tramonto dell'era analogica e aprono la strada a riflessioni di natura teorica e pratica sulle implicazioni che il crescente ricorso a strumenti digitali a fini comunicativi generano sul non facile bilanciamento di interessi fra diritti individuali dei soggetti interessati e diritti a rilievo collettivo della società nel suo complesso.

II. I tradizionali strumenti di intrusione e indagine del potere pubblico

Sommario: 1. Il controllo sulle comunicazioni postali. – 1.1. Il segreto postale nell'Italia liberale - 1.2. Dalla riforma di epoca fascista all'età repubblicana – 1.3. L'eco della Consulta: dal nuovo codice postale alla disciplina del Codice Vassalli. - 2. Le intercettazioni telefoniche. – 2.1. I presupposti nel codice del 1930 e l'adeguamento al quadro costituzionale. – 2.2. La nuova disciplina del codice del 1989. – 2.3. La riforma promessa (ma in parte tradita) del decreto Orlando. - 2.4. La funzione della motivazione. – 3. Le intercettazioni cd. ambientali. – 3.1. La disciplina generale. – 3.2. L'intercettazione domiciliare. – 4. Le intercettazioni telematiche.

1. Il controllo sulle comunicazioni postali

1.1. Il segreto postale nell'Italia liberale

Coerentemente con l'impostazione descritta nel Cap. I, il legislatore italiano fu a lungo orientato più a tutelare la segretezza delle comunicazioni dei cittadini e dei singoli dall'intrusione di terzi privati che non a garantire che essa fosse protetta dall'intrusione dei pubblici poteri. La prima disposizione a questo riguardo che seguì l'unificazione del Paese fu l'art. 27, l. 5 maggio 1862, n. 604, a norma del quale "*il segreto delle lettere è inviolabile. Il Governo ed i funzionari da lui dipendenti ne sono responsabili e vigilano rigorosamente perché non siano aperte da alcuno né venga presa in alcun modo cognizione del loro contenuto*"[121]. Le disposizioni seguenti (che, non a caso, erano ricomprese entro il capo rubricato "*Lettere che possono aprirsi*"), tuttavia, riconoscevano ai medesimi funzionari la facoltà di aprire quella corrispondenza con indirizzo mancante o illeggibile o quella che venisse rifiutata dal destinatario, frustrando l'affermazione di principio di cui all'art. 27 (in un contesto in cui, è d'uopo ricordare, non vi era un riconoscimento costituzionale espresso della tutela del segreto epistolare).

[121] Tale disposizione fu poi confermata, dall'art. 9, regio decreto 20 giugno 1889, n. 6151, che approvava il cd. T.U. delle leggi sul servizio postale, recependo in larga misura il contenuto dell'atto precedente, e, in seguito, dall'art. 9, regio decreto 24 dicembre 1899, n. 501. Idem dicasi per le successive disposizioni relative ai casi in cui la corrispondenza che poteva essere aperta.

Analoga attenzione rivolta alla violazione del segreto della corrispondenza da parte dei privati si può rintracciare nelle disposizioni del primo codice penale post-unitario[122]. Nel capo rubricato "*Dei delitti contro l'inviolabilità dei segreti*", infatti, trovava spazio l'art. 159, a norma del quale chi avesse aperto o si fosse impossessato indebitamente di una lettera, telegramma o piego postale non a esso diretto, per conoscerne il contenuto, soggiaceva a una pena detentiva fino a quindici giorni e a una pena pecuniaria compresa fra cinquanta e millecinquecento lire. Più severamente, a norma dell'art. 160, veniva punita la soppressione di una corrispondenza epistolare o telegrafica, anche senza che fosse presa cognizione del contenuto. Chi rendesse pubblico il contenuto di una corrispondenza epistolare, laddove da tale pubblicità potesse essere cagionato un danno, era punito con una mera sanzione pecuniaria (art. 161). In tutti i casi di cui sopra, tuttavia, in assenza di un danno alla collettività, la procedibilità era a querela di parte (art. 164). Diversamente, i reati propri dei funzionari dell'amministrazione postale che avessero violato il segreto epistolare o avessero soppresso lettere o altre corrispondenze, erano procedibili d'ufficio e prevedevano pene detentive più afflittive (art. 162).

Il successivo codice di procedura penale di epoca liberale[123], che sostituì quello post-unitario[124] che si limitava a rinviare, laddove si dovesse procedere a sequestri di lettere o pieghi negli uffici postali, alle disposizioni rilevanti di leggi e regolamenti sull'amministrazione delle poste[125], divaricava il regime di tutela della segretezza del contenuto della corrispondenza da quello relativo alla libertà della medesima[126]. Infatti, sotto il primo profilo, esso prevedeva che potessero essere sequestrati, su ordine del giudice, una serie di oggetti o forme di corrispondenza spediti a un imputato o ritenuti attinenti al reato perseguito (art. 238, c.1); al sequestro potevano essere delegati ufficiali e agenti di polizia giudiziaria, pur restando permesso al solo giudice di procedere all'apertura della corrispondenza (art. 238, c.2); inoltre, la

[122] Cd. Codice Zanardelli, regio decreto 30 giugno 1889, n. 6133.
[123] Regio decreto 27 febbraio 1913, n. 127.
[124] Si tratta, in buona sostanza, del Codice di procedura penale del Regno di Sardegna, che data al 20 novembre 1859; esso fu poi esteso a tutto il Regno d'Italia per effetto del regio decreto 26 novembre 1865, n. 2598.
[125] Art. 150.
[126] Così C. Caruso, *La libertà e la segretezza delle comunicazioni nell'ordinamento costituzionale*, *op. cit.*, 3.

disposizione consentiva altresì al giudice di accedere agli uffici telefonici per intercettare o impedire comunicazioni o per raccogliere informazioni rilevanti (art. 238, c.3).

Sotto il secondo profilo, il codice di rito disponeva che gli ufficiali di polizia giudiziaria dovessero astenersi dall'apertura dei plichi di corrispondenza, dovendo limitarsi a trasmetterli all'autorità giudiziaria (art. 170, c.1), ben potendo chiedere, nei casi in cui la legge prevedesse il sequestro, che essi fossero trattenuti fino alla pronuncia del provvedimento giurisdizionale che disponesse il sequestro (art. 170, c.2); inoltre, anche a costoro era consentito l'accesso agli uffici telefonici ai medesimi fini per i quali era autorizzato per i giudici (art. 170, c.3).

1.2. Dalla riforma di epoca fascista all'età repubblicana

Nel 1930, il legislatore introdusse una nuova versione tanto del codice penale[127] (il cd. Codice Rocco, ancora oggi in vigore – pur sensibilmente modificato) quanto del codice di procedura penale[128]. Sotto il profilo del diritto penale sostanziale, le disposizioni inserite nella sezione rubricata "Dei delitti contro l'inviolabilità del segreto" punivano (e puniscono tutt'oggi) tanto l'interferenza da parte di terzi privati, che prendessero conoscenza del contenuto di una corrispondenza, sia essa epistolare, telegrafica o telefonica, non indirizzata a loro, ne sopprimessero il corso o ne rivelassero senza giusta causa il contenuto (artt. 616-617-618 c.p.), sia il reato proprio commesso dal pubblico dipendente o funzionario delle poste, dei telegrafi o del telefono, che soggiace a un trattamento sanzionatorio aggravato (artt. 619-620 c.p.). La tutela sotto il profilo penalistico è dunque diretta alla protezione della corrispondenza in sé, indipendentemente dal contenuto della medesima, dal carattere di confidenzialità o dall'interesse a essa ricollegato dalle parti del rapporto comunicativo[129].

Per quanto concerne il profilo processualistico, il codice di rito approvato nel 1930 prevedeva il potere del giudice, in fase istruttoria, di disporre il sequestro di lettere, pieghi, pacchi, valori e altri oggetti di corrispondenza presso uffici postali o

---

[127] Regio decreto 19 ottobre 1930, n. 1398, *Approvazione del testo definitivo del Codice Penale*.
[128] Regio decreto 19 ottobre 1930, n. 1399, *Approvazione del testo definitivo del Codice di Procedura Penale*.
[129] P. Barile-E. Cheli, *Corrispondenza (libertà di)*, in *Enc. del dir.*, X, Milano, 1962, 747.

telegrafici, laddove vi fossero ragioni per ritenere i medesimi spediti dall'imputato o a esso indirizzati o che potessero avere una qualche forma di relazione con il reato perseguito; nel caso fosse un ufficiale di polizia giudiziaria a procedere al sequestro, si prescriveva che gli oggetti di corrispondenza dovessero essere rimessi al giudice senza procedere all'apertura o prenderne in ogni caso cognizione (art. 338 c.p.p.).

Se tale disposizione non pareva sollevare particolari problematiche sotto il profilo della compatibilità con il dettato costituzionale entrato successivamente in vigore, di ben altro tenore è l'interferenza che veniva autorizzata ai sensi dell'art. 226, c.2 c.p.p. Quest'ultimo introduceva una fattispecie che riconosceva agli ufficiali di polizia giudiziaria il potere di ordinare di trattenere la corrispondenza in casi di urgenza fino all'emanazione di un provvedimento giurisdizionale. Tale ipotesi, non prevedendo un termine entro il quale l'autorità giudiziaria dovesse pronunciarsi, introduceva una limitazione della libertà di corrispondenza affine a quella preventiva prevista all'art. 13 Cost. (e valida anche per l'art. 14), ma in apparente contraddizione con il requisito stringente della riserva di giurisdizione, che a norma dell'art. 15 Cost. appare non derogabile[130].

La debolezza della garanzia statutaria emerse con chiarezza all'entrata in vigore del Codice postale e delle telecomunicazioni fascista[131]. L'art. 12 sanciva sì che nessuno potesse prendere visione o fare copia di telegrammi o altre forme di corrispondenza, all'infuori di mittente, destinatario e loro eredi o legali rappresentanti (c.1), ma attribuiva altresì alla pubblica amministrazione la facoltà di prendere visione, fare copia e sequestrare la corrispondenza nei modi e casi stabiliti dalla legge (c.2). Il successivo art. 13 imponeva che non si desse corso alla corrispondenza suscettibile di costituire pericolo per la sicurezza dello Stato o di essere dannosa per le persone o di essere contraria a leggi, ordine pubblico e buon costume.

Si comprende facilmente come, per poter porre in essere tale funzione di filtro, l'amministrazione pubblica fosse investita della facoltà di apertura della corrispondenza e di presa di cognizione del contenuto della stessa. D'altronde, la riserva di legge di cui all'art. 12, c.2 era ben poco significativa in un ordinamento a

[130] P. Barile-E. Cheli, *op. cit.*, 750.
[131] Regio decreto 27 febbraio 1936, n. 645.

costituzione flessibile, in cui la discrezionalità del legislatore ordinario non era vincolata in senso gerarchico da disposizioni costituzionali (di cui, peraltro, lo Statuto difettava nello specifico); in ogni caso la riserva di legge era contenuta meramente in una fonte primaria, quindi derogabile da una fonte di pari rango. Questo quadro consente perciò di ritenere poco significativa l'enunciazione dell'inviolabilità del segreto epistolare, che pure il codice postale riprendeva (art. 38, c.1), investendo funzionari e agenti dell'amministrazione delle poste della responsabilità e vigilanza sulla sua osservanza (c.2).

1.3. L'eco della Consulta: dal nuovo codice postale alla disciplina del Codice Vassalli

L'entrata in vigore della Costituzione, che contempla la specifica tutela di cui all'art. 15, non ebbe effetti immediati, poiché non fu che dopo due decenni che la Corte costituzionale si pronunciò su tali disposizioni, dettando il principio da seguire in materia e riconoscendo la legittimità costituzionale della modifica introdotta in pendenza del giudizio a opera della l. 20 dicembre 1966, n. 1114. Investita della questione in un procedimento in via incidentale originato da un procedimento penale a carico di un soggetto accusato del reato di pubblicazioni oscene, la Consulta aveva ritenuto che la disposizione che aveva consentito l'acquisizione delle prove, ossia l'art. 13 del Codice postale fascista, violasse l'art. 15, c.2 Cost., in quanto esso attribuiva all'Amministrazione postale il "*potere, discrezionale ed autonomo, di non dar corso alla corrispondenza e non prevede l'intervento dell'autorità giudiziaria e neppure l'obbligo di fare ad essa immediato rapporto in ordine alla corrispondenza fermata*"[132].

Poiché la norma esponeva la libertà di corrispondenza a possibili limitazioni e ingerenze in assenza della garanzia dell'intervento dell'autorità giudiziaria, proseguiva la Corte, essa era costituzionalmente illegittima. Con ciò, tuttavia, il giudice delle leggi non intendeva dire che la libertà riconosciuta fosse assoluta, ben potendo la stessa essere suscettibile all'apposizione di limiti con riferimento ad altri interessi, individuali o collettivi, di rilevanza costituzionale, a patto che tali limitazioni

[132] Corte Cost., sent. 100/1968, Cons. dir. §3.

fossero previste dalla legge e disposte per ciascuna occasione con atto motivato dall'autorità giudiziaria.

La Corte costituzionale salvò, invece, il contenuto dell'art. 12, c.2 del Codice postale, in quanto la disposizione si limitava ad attribuire a determinati soggetti la facoltà di procedere alla presa visione, copiatura e sequestro di corrispondenze o telegrammi nei casi stabiliti da altre disposizioni, le quali appunto erano suscettibili di scrutinio dell'autorità giudiziaria (come dimostra il caso dell'art. 13 del Codice postale).

La nuova versione dell'art. 13 del Codice postale, introdotta con un atto legislativo *ad hoc* dopo che era già stata sollevata la prima questione di legittimità costituzionale, fu invece ritenuta compatibile con il dettato costituzionale. Il meccanismo che poneva in essere, infatti, prevedeva che la corrispondenza fermata da dipendenti delle Poste, che agivano in quelle circostanze come ufficiali di polizia giudiziaria, dovesse essere trasmessa tempestivamente al pretore, il quale entro ventiquattro ore doveva disporre, con decreto motivato, se la stessa dovesse avere corso. Tale decreto andava poi notificato nello stesso giorno dell'emanazione al mittente e all'amministrazione delle poste, i quali potevano, entro le ventiquattro ore successive alla notifica, proporre reclamo al tribunale.

Una tale configurazione della procedura, argomentò il giudice costituzionale, sottrae all'amministrazione postale il potere autonomo di arrestare il corso della corrispondenza, investendo l'autorità giudiziaria della decisione sulla limitazione del diritto individuale inviolabile. L'attività del funzionario sarebbe dunque meramente strumentale alla sollecitazione dell'intervento del giudice, che è il soggetto titolato a esercitare il potere di fermo, sempre potendo il mittente chiedere che si pronunci il tribunale.

Nemmeno furono ritenute rilevanti le supposte lacune relative alla mancanza di un termine per la trasmissione della corrispondenza fermata al pretore e di un'indicazione di quale fosse l'ufficio titolato a effettuare il fermo. Entrambe, affermò la Corte, potrebbero essere colmate per via di interpretazione logica, desumendo che la trasmissione al pretore debba essere quanto più tempestiva, in ragione del breve lasso di tempo a esso disponibile per la decisione, e che una volta che sia intervenuta

una pronuncia favorevole a che si dia corso alla corrispondenza, non sia possibile un successivo ulteriore fermo da parte di altro ufficio postale.

Fu soltanto cinque anni dopo la pronuncia della Consulta che il legislatore ordinario mise mano alla legislazione di settore, emanando un nuovo testo unico dedicato alla materia postale[133]. In particolare, il nuovo testo sanciva esplicitamente la libertà di corrispondenza e l'inviolabilità del segreto epistolare, consentendone la limitazione soltanto per atto motivato dell'autorità giudiziaria (art. 10, c.1), così recependo il dettato costituzionale e la giurisprudenza della Consulta.

Furono in ogni caso confermate la funzione di responsabilità e vigilanza dei funzionari dell'amministrazione postale sul rispetto di tale principio (c.2) e il divieto per chiunque di prendere cognizione del contenuto ed estrarne copia, salvo che per il mittente, destinatario e i loro eredi o legali rappresentanti, nonché le altre persone indicate dalla legge (c.4). Parimenti confermati furono le limitazioni all'inoltro della corrispondenza postale o telegrafica nociva per lo Stato o i singoli cittadini o che costituisse essa stessa reato, nonché quella contraria al buon costume o contenente espressioni scurrili, ingiuriose o denigratorie (art. 11, cc.1-2). Tale accertamento, peraltro, fu consentito soltanto per quella corrispondenza soggetta a verifica a norma di legge o quella dal cui involucro si possa riscontrare il suddetto contenuto (c.3). Il procedimento per la convalida del fermo postale rimaneva quella introdotto nel 1966, che prevedeva la decisione del pretore, avverso la quale era ammesso reclamo dinanzi al tribunale (cc.4-6).

Da sottolineare come, in ogni caso, il regolamento di esecuzione di tale fonte legislativa[134], all'art. 11, c.2 disponga che i funzionari postali o delle dogane e gli agenti di pubblica sicurezza, laddove sospettino che il contenuto di corrispondenze o pacchi sia di provenienza furtiva o spedito in contravvenzione a disposizioni legislative o regolamentari, possono procedere, d'intesa con gli impiegati postali, all'apertura di tali plichi, con eccezione di quelli epistolari. Il testo qualifica come corrispondenze epistolari tutto gli invii chiusi, a eccezione dei pacchi, nonché gli invii aperti che abbiano contenuto di carattere attuale e personale (art. 24).

---

[133] D.P.R. 29 marzo 1973, n. 156.

[134] D.P.R. 29 maggio 1982, n. 655, *Approvazione del regolamento di esecuzione dei libri I e II del codice postale e delle telecomunicazioni (norme generali e servizi delle corrispondenze e dei pacchi).*

Tale esclusione dei pacchi dalla nozione di corrispondenza ai fini dell'esecuzione del codice postale presta il fianco a critiche[135], poiché, per esempio, l'art. 181 del regolamento prevede che i pacchi postali possano essere aperti in qualunque ufficio dietro richiesta di funzionari o agenti finanziari se costoro sospettano una violazione delle leggi sulle dogane, i monopoli o qualsiasi altra disposizione normativa che essi debbano applicare (c.1). Anche l'ufficio di destinazione può procedere all'apertura del pacco in costanza di un fondato sospetto che contenga merci non dichiarate o il cui trasporto sia vietato (c.2), ma deve avvertire il destinatario che ha facoltà di assistere all'apertura personalmente o tramite rappresentante (c.3). In questo caso, pertanto, la garanzia dell'art. 15 Cost. viene surrettiziamente circoscritta a una parte dell'ampio novero di oggetti che condividono la natura di corrispondenza, e ciò avviene per via regolamentare, in apparente violazione della riserva di legge prevista dalla disposizione costituzionale in discorso.

Lo scenario si è modificato una volta di più con l'approvazione del più recente fra i codici in vigore nell'ordinamento italiano, il cd. Codice Vassalli[136]. In particolare, il testo contiene un'apposita disposizione che disciplina il sequestro di corrispondenza, che riproduce quasi *verbatim* il contenuto dell'art. 338 del vecchio Codice di procedura penale[137]. Diversamente, il legislatore sembra aver preso coscienza dei limiti dell'art. 226 del codice abrogato, tanto da aver novellato la disciplina prevedendo che l'ufficiale di polizia giudiziaria debba trasmettere pacchi o plichi di corrispondenza da acquisire a fini probatori o di indagine intatti al pubblico ministero. Quest'ultimo potrà autorizzarlo all'apertura immediata e all'accertamento del contenuto in casi di urgenza, ma vige un termine di quarantotto entro il quale il sequestro deve essere convalidato dall'autorità giudiziaria, trascorso inutilmente il quale gli oggetti di corrispondenza devono essere inoltrati al destinatario (art. 353 c.p.p.).

---

[135] V. P. Barile, *Diritti dell'uomo e libertà fondamentali*, Bologna, Il Mulino, 1984, 165.
[136] D.P.R. 22 settembre 1988, n. 447, *Approvazione del codice di procedura penale*.
[137] Art. 254 c.p.p., come modificato dall'art. 8, c.4, l. 18 marzo 2008, n. 48, *Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*.

Il quadro dell'evoluzione della regolamentazione dell'interferenza privata e pubblica nell'esercizio della libertà di corrispondenza postale e telegrafica dimostra come lo stato attuale della disciplina si riveli senz'altro più adeguato a garantire le prerogative sancite dalla Costituzione ai singoli a tutela della libera e segreta corrispondenza con i terzi rispetto al quadro normativo rimasto in vigore per quattro decenni dopo l'entrata in vigore della costituzione repubblicana. Se ciò si palesa in particolare sotto il profilo dell'adeguamento delle disposizioni del codice di procedura penale al contenuto dell'art. 15 Cost., purtuttavia rimane controversa la legittimità del potere riconosciuto agli ufficiali di polizia giudiziaria a norma dell'art. 181 del regolamento di esecuzione del codice postale. Sulla compatibilità della disposizione con il quadro costituzionale, in ogni caso, non può essere la Consulta a esprimersi, poiché come noto l'art. 134 della Costituzione sancisce che la Corte costituzionale giudica sulla legittimità costituzionale della legge e degli atti aventi forza di legge, senza menzionare le fonti regolamentari, sulla cui legittimità la sola a potersi pronunciare con effetti ablatori è la giurisdizione amministrativa.

2. *Le intercettazioni telefoniche*

2.1. I presupposti nel codice del 1930 e l'adeguamento al quadro costituzionale

La trattazione della regolamentazione delle intercettazioni telefoniche come mezzo di ricerca della prova in ambito penale non può prescindere dal riconoscimento della molto più giovane esistenza dell'invenzione del telefono rispetto alla corrispondenza per iscritto. Per questa ragione, il primo codice di procedura penale dell'Italia unita non poteva dettare una qualsiasi disciplina su una modalità di comunicazione la cui invenzione risale, al netto delle dispute sulla paternità della stessa, grossomodo al decennio successivo all'unificazione.

Fu dunque soltanto con il codice di procedura penale di epoca giolittiana che l'intercettazione telefonica fece il suo esordio fra i mezzi a disposizione della polizia giudiziaria (art. 170) e del giudice (art. 238) per la ricerca di indizi e prove di reato. Tuttavia, soltanto al termine della prima guerra mondiale il telefono cominciò lentamente a diffondersi in Italia anche a scopi non commerciali. Il codice di procedura

penale di era fascista recepiva l'impostazione del precedente codice sul potere di ufficiali di polizia giudiziaria e giudici di accedere a uffici e impianti telefonici per trasmettere, intercettare o impedire comunicazioni o per prenderne cognizione (rispettivamente, art. 226, c.3 e art. 339).

Un primo intervento del legislatore per ricondurre alla legittimità costituzionale la disciplina delle intercettazioni telefoniche si ebbe nell'ambito di un ampio intervento emendativo del codice di procedura penale nel 1955. L'art. 226 c.p.p. venne integralmente sostituito e, in particolare, fu aggiunto un quarto comma che prevedeva che, per intercettare o impedire comunicazioni telefoniche o per prenderne cognizione, gli ufficiali di polizia giudiziaria dovessero ottenere un'autorizzazione dall'autorità giudiziaria contenuta in un decreto motivato[138]. Nel medesimo senso fu altresì modificato l'art. 339 c.p.p., così che prevedesse che il giudice potesse accedere per i fini di cui sopra agli uffici e impianti telefonici o potesse delegarvi con decreto motivato un ufficiale di polizia giudiziaria[139].

L'intervento del legislatore fu senz'altro meritorio per lo sforzo di adeguare la disciplina di questo mezzo di ricerca della prova alle garanzie costituzionali entrate in vigore, in particolare in ossequio alla riserva di giurisdizione sancita all'art. 15 Cost. Tuttavia, un tale entusiasmo non si poteva condividere sotto il profilo del rispetto della riserva di legge di cui alla medesima disposizione, essendosi il legislatore limitato a un intervento superficiale e non organico della materia[140].

La Corte costituzionale fu investita in un giudizio in via incidentale dello scrutinio sulla legittimità costituzionale dell'art. 226, c.4 c.p.p., come da ultimo modificato dal legislatore nel 1955[141]. Nel dichiarare la questione di legittimità costituzionale infondata, la Consulta ricordò come l'art. 15 Cost. non si limiti a sancire l'inviolabilità della libertà e segretezza della corrispondenza, ma enunci espressamente anche la possibilità di limitare tale prerogativa per atto dell'autorità giudiziaria con le garanzie stabilite dalla legge. Tale formulazione, argomentò il collegio, dimostra come la disposizione tuteli due interessi distinti e potenzialmente

---

[138] Art. 7, c.1, l. 18 giugno 1955, n. 517.
[139] Art. 19, c.1, l. 18 giugno 1955, n. 517.
[140] P.G. Gosso, *Intercettazioni telefoniche*, in *Enc. dir.*, XXI, 1971, 891-892.
[141] Corte cost., sent. n. 34/1973.

in competizione l'uno con l'altro. Da un lato, vi era il profilo inerente libertà e segretezza delle comunicazioni, strettamente connesso alla dichiarazione di inviolabilità dei diritti della persona di cui all'art. 2 Cost., dall'altro l'interesse connesso all'esigenza di prevenzione e repressione delle condotte di reato. Il giudice costituzionale riconobbe che le modifiche alla disposizione di quasi venti anni prima fossero preordinate a riportare sotto il quadro costituzionale la disciplina della materia, che era fuoriuscita da tale alveo con l'entrata in vigore della Costituzione repubblicana, più garantista di quanto non fosse lo Statuto.

La Corte si spese nel sottolineare come nell'ordinamento costituzionale italiano la compressione del diritto costituzionalmente sancito alla riservatezza delle comunicazioni possa avvenire soltanto sotto il controllo dell'autorità giudiziaria, venendo così sottratta all'attuazione discrezionale e autonoma dell'organo di polizia giudiziaria. È il giudice che, per mezzo di un apposito decreto, autorizza il dispiegamento delle operazioni di intercettazione e deve valutare ciascuna richiesta con particolare attenzione e cautela, tenendo presente le gravi lesioni del diritto alla riservatezza delle comunicazioni che l'esperimento di questo mezzo di ricerca della prova comporta.

Il giudice si trova perciò a svolgere un contemperamento dei due interessi protetti dallo stesso art. 15 Cost. e il suo compito è quello di assicurarsi che l'interesse al mantenimento della segretezza delle comunicazioni non sia sacrificato in maniera sproporzionata sull'altare delle esigenze di efficace persecuzione delle condotte penalmente rilevanti. All'autorità giudiziaria spetta pertanto la verifica della sussistenza di effettive esigenze di procedere ad attività di intercettazione telefonica e la formulazione di un giudizio prognostico sulla possibilità di acquisire riscontri favorevoli per lo svolgimento delle attività di indagine. Tale percorso argomentativo deve riflettersi nella motivazione del provvedimento con cui viene autorizzato l'esperimento dell'intercettazione telefonica, ben dovendo il giudice altresì premurarsi di indicare il lasso temporale per il quale l'operazione è autorizzata e motivare eventuali proroghe di tale termine[142].

[142] La pronuncia è stato oggetto di un celebre commento da parte di V. Grevi, *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche*, in *Giur. Cost.*, 1973, 317-342.

La Corte costituzionale proseguì dettando ulteriori principi in merito alla conformità a Costituzione della disciplina dedotta in giudizio, in particolare con riferimento alla predisposizione in concreto delle attrezzature tecniche per svolgere l'operazione di intercettazione, così che l'autorità giudiziaria possa esercitare il controllo sul rispetto dei limiti dell'autorizzazione contenuta nel decreto. Inoltre, essa si premunì di pronunciarsi sul controllo sulla legittimità del decreto che autorizza l'intercettazione e sull'utilizzabilità in sede processuale del materiale probatorio raccolto. Soprattutto con riferimento al primo dei due aspetti suindicati, la Consulta riconobbe l'ampia discrezionalità di cui gode il legislatore, ma ne sollecitò un puntale intervento in concreto sul piano legislativo.

Sulla base di quanto premesso, la Corte costituzionale sancì che il decreto autorizzativo, per quanto non impugnabile, è ben sindacabile e la sua illegittimità può essere rilevata nel corso del giudizio. Inoltre, gli ufficiali di polizia giudiziaria sono tenuti al segreto e nel processo possono essere utilizzate soltanto le risultanze probatorie utili all'imputazione formulata dalla pubblica accusa. La Corte sottolineò la centralità del rigoroso rispetto del divieto di pubblica divulgazione del contenuto di comunicazioni non pertinenti al processo. La Corte rigettò dunque la questione di legittimità costituzionale con riferimento all'art. 15 Cost., argomentando che esso sarebbe violato, con grave nocumento del diritto costituzionalmente sancito a favore dell'individuo, laddove fossero in giudizio come indizi o prove risultanze di intercettazioni predisposte senza la preventiva autorizzazione dell'autorità giudiziaria[143].

La Corte respinse altresì la doglianza relativa alla violazione del diritto di difesa di cui all'art. 24 Cost., specificando come il collegamento svolto nell'ordinanza di rimessione del Tribunale di Bolzano con il diritto al silenzio dell'imputato sottoposto a interrogatorio non fosse risolutivo, poiché le due situazioni sono ontologicamente diverse, in quanto nella prima l'indagato comunica liberamente e senza pressioni psicologiche di alcuna sorta con un terzo (consapevole o meno dell'intercettazione in

[143] Sia consentito sottolineare come, nonostante la Corte non si diffonda sul punto, sia da ritenersi che la lesione del diritto costituzionale alla libera e segreta comunicazione con i terzi si compia già nel momento dell'apprensione non autorizzata del contenuto della comunicazione, indipendentemente dall'effettivo utilizzo delle medesime in giudizio.

corso, questo non fa differenza), mentre nella seconda può essere sottoposto a pressioni di natura psicologica che impongono il riconoscimento di un diritto al silenzio e a non rispondere alle domande poste dagli ufficiali di polizia giudiziaria o direttamente dall'autorità giudiziaria.

La decisione della Corte, che si configura come una pronuncia interpretativa di rigetto, fu uno sprone al legislatore a intervenire per rendere più organica la disciplina delle intercettazioni telefoniche. L'anno seguente, con un provvedimento legislativo la cui rubrica esemplare recitava "*Tutela della riservatezza e della libertà e segretezza delle comunicazioni*"[144], l'ultimo comma dell'art. 226 fu dunque abrogato e furono inserite quattro nuove disposizioni in materia, oltre a sostituire integralmente l'art. 336 con un testo novellato.

L'art. 226-bis provvedeva alla storica carenza della disciplina sulle intercettazioni fornendo un elenco tassativo ("*soltanto in caso di indagini relative ai seguenti reati*") delle fattispecie di reato per la cui persecuzione era consentito il ricorso da parte della polizia giudiziaria, su autorizzazione dell'autorità giudiziaria, alle intercettazioni telefoniche[145]. La disposizione escludeva esplicitamente dal novero delle comunicazioni intercettabili quelle di difensori e consulenti tecnici che avessero per oggetto i procedimenti giudiziari nei quali essi prestassero la propria opera[146].

Il successivo articolo 226-ter prevedeva che l'autorizzazione fosse disposta con un decreto motivato da parte del competente procuratore della Repubblica o giudice istruttore in presenza di seri e concreti indizi di reato, di cui il decreto doveva dare conto, oppure laddove vi fosse necessità di limitare la libertà di comunicazione dell'indiziato ai fini della raccolta di elementi di prova per il fatto perseguito non altrimenti ottenibili. Il provvedimento doveva contenere indicazioni circa modalità e durata delle operazioni, prevedendo un termine non superiore a quindici giorni,

---

[144] L. 8 aprile 1974, n. 98.

[145] Delitti dolosi puniti con una pena superiore nel massimo a cinque anni, reati in materia di stupefacenti, di armi e sostanze esplosive, di contrabbando, nonché i reati di ingiurie, minacce, molestia e disturbo alla persona con il mezzo del telefono.

[146] Gli artt. 226-bis, 226-ter, 226-quater e 226-quinquies sono stati introdotti dall'art. 5, l. 98/1974. Sulle innovazioni introdotte dalla legge 98/1974 e, in particolare, sull'art. 226-bis, v. R. Cantagalli, *Riservatezza della vita privata e intercettazioni delle comunicazioni*, Firenze, Edizioni Laurus, 1977, in particolare §§46 ss., 188 ss.

prorogabile tramite ordinanza per ulteriori quindici giorni per due sole volte, in costanza dei requisiti di cui sopra e con motivazione non meramente *per relationem*.

L'art. 226-quater prescriveva le modalità tecniche di svolgimento delle operazioni di intercettazione, disponendo che le stesse dovessero tenersi soltanto pressi appositi locali installati presso le Procure della Repubblica o, in pendenza della predisposizione degli stessi, presso gli impianti di pubblico servizio. Delle operazioni di registrazione andava redatto apposito processo verbale, da trasmettersi immediatamente al procuratore della Repubblica o al giudice istruttore che avesse autorizzato l'operazione, e le registrazioni medesime andavano conservate in custodie sigillate *ad hoc*. L'articolo disponeva altresì in merito al deposito in cancelleria dei verbali delle operazioni, così come delle comunicazioni ai legali delle parti interessate, ai fini di dare a essi la possibilità di estrarre copia delle suddette registrazioni. La disposizione in questione regolava altresì la selezione del materiale rilevante a fini processuali da parte del magistrato, disponendo che si procedesse alla distruzione di registrazioni e trascrizioni viziate da nullità o estranee ai fini processuali.

L'art. 226-quinquies, infine, prevedeva che fossero colpite da nullità insanabile e rilevabile d'ufficio in ogni stato e grado del processo le intercettazioni telefoniche eseguite fuori dai casi stabiliti dalla legge o in difformità dai procedimenti prescritti, nonché quelle ottenute per mezzo di condotte che integrassero la fattispecie di interferenze illecite nella vita privata (indebito ottenimento di notizie o immagini attinenti alla vita privata tramite ripresa audio-visiva di comportamenti che si tengano nei luoghi di domicilio)[147].

L'art. 339 fu modificato inserendo gli appositi riferimenti alle nuove disposizioni in tema di intercettazioni di cui agli artt. 226-bis e seguenti[148]. Di rilievo fu anche il riconoscimento esplicito della retroattività della disposizione in tema di insanabilità delle intercettazioni illecitamente ottenute, in contraddizione con il tradizionale principio processuale *tempus regit actum*, per evitare di mantenere in essere situazioni processuali altrimenti contrarie allo spirito della Costituzione[149].

---

[147] Art. 619-bis c.p.
[148] Art. 6, l. 98/1974.
[149] Art. 8, l. 98/1974.

La Consulta ritornò sul tema l'anno dopo, richiamando la decisione presa nella sentenza 34/1973 e argomentando che non integra fattispecie costituzionalmente illegittima la previsione dell'art. 338 c.p.p., secondo la quale l'ufficiale di polizia giudiziaria prende cognizione diretta del contenuto delle comunicazioni telefoniche prima di trasmetterle al pubblico ministero, laddove con riferimento alla corrispondenza epistolare e postale il segreto è protetto dall'inoltro del pacco o plico sigillato[150]. Non sarebbe violato, argomenta la Corte costituzionale, il principio di ragionevolezza, poiché le due situazioni sarebbero diverse, non essendo necessaria la presa di cognizione del contenuto della lettera nel caso della corrispondenza epistolare, mentre la previa audizione dell'ufficiale di polizia giudiziaria ben può essere indispensabile, pur sempre presidiata dall'obbligo di mantenere il segreto sul contenuto delle conversazioni sottoposte a intercettazione (obbligo che, ricorda la Corte, sussiste anche in forza degli artt. 230 e 307 c.p.p. e a tutela dei terzi parti del rapporto comunicativo intercettato). Pure nel senso del rigetto la Corte si espresse sulla presunta illegittimità delle disposizioni sul deposito del verbale di esecuzione delle intercettazioni, permanendo in capo alla discrezionalità politica del legislatore la decisione su tempi e modi in cui esso debba avvenire, purché la difesa ne sia prontamente messa al corrente.

Parimenti infondata, secondo il giudice delle leggi, era la questione di legittimità costituzionale concernente l'art. 226-quinquies, che avrebbe violato l'obbligo di esercitare l'azione penale e avrebbe ingenerato un'ingiustificata disparità di trattamento fra diversi imputati, in spregio al principio di ragionevolezza. Il principio introdotto dalla disposizione, argomenta la Corte, determina l'equiparazione delle prove raccolte illegittimamente a prove inesistenti, per tanto prive di alcun valore probatorio in giudizio.

Tale interpretazione della Corte costituzionale valeva a superare l'orientamento giurisprudenziale e dottrinale che deponeva a favore della prevalenza del libero convincimento del giudice nella valutazione delle prove assunte al di fuori delle procedure previste dalla legge. Ciò, tuttavia, spiegava effetti retroattivi solo nei confronti di quelle prove che fossero state raccolte in spregio alle procedure al tempo

[150] Corte Cost., sent. n. 120/1975.

applicabili (pur nel senso della più garantistica interpretazione di cui alla sentenza 34/1973), senza depauperare di valenza probatoria anche quegli elementi di prova raccolti in ossequio alle regole al tempo vigenti. In forza di tale interpretazione, la Corte costituzionale rigettò dunque la censura che deduceva una violazione del principio generale in materia processuale *tempus regit actum* (che, diversamente, sarebbe stato violato, insieme al principio di eguaglianza, laddove l'interpretazione suggerita dal giudice remittente fosse stata accolta).

Il legislatore intervenne nuovamente, in via di urgenza, a modificare in parte la disciplina[151], eliminando il limite di due proroghe alle operazioni di intercettazione precedentemente contemplato dall'art. 226-ter c.p.p., limitandosi a richiedere che la motivazione per ciascun rinnovo dell'autorizzazione fosse specifica (e non anche dettagliata) e disponendo in favore di una concessione dell'autorizzazione anche in forma orale, fermo restando l'obbligo di formalizzazione per iscritto non appena possibile e dando conto di data e ora dell'autorizzazione concessa in forma orale[152].

L'atto adottato dal Governo e convertito dalle Camere prevedeva poi la possibilità di svolgimento delle operazioni di intercettazione altresì presso impianti in dotazione alla polizia giudiziaria, dietro autorizzazione del Procuratore della Repubblica o del giudice istruttore e nei soli casi di urgenza ove non fosse possibile procedere alle operazioni negli impianti installati presso la Procura. La disposizione ordinava altresì la trasmissione immediata dei verbali delle operazioni al giudice che avesse autorizzato l'esperimento di tale mezzo di ricerca della prova. Fu previsto, inoltre, che le prove raccolte tramite tale strumento di indagine potessero essere utilizzate anche in altri procedimenti, se riferite a reati per i quali il mandato di cattura fosse obbligatorio anche per uno soltanto degli imputati[153].

La novella legislativa conteneva infine la previsione di un'ipotesi eccezionale di intercettazione delle comunicazioni, che potevano essere disposte dal Procuratore della Repubblica competente su richiesta del Ministro dell'Interno, del questore o di ufficiali o comandanti di servizio o di reparto operativo delle forze di pubblica sicurezza per i casi in cui il ricorso all'intercettazione telefonica fosse necessaria per la

[151] Decreto-legge 21 marzo 1978, n. 59, convertito con modificazioni dalla l. 18 maggio 1978, n. 191.
[152] Artt. 6-7, d.l. 59/1978.
[153] Art. 8, d.l. 59/1978.

prosecuzione delle indagini in ordine ai reati indicati dall'art. 165-ter c.p.p. (anch'esso introdotto dal medesimo atto)[154]. Lo svolgimento di tali operazioni poteva derogare ad alcuni dei passaggi procedurali di cui all'art. 226-quater novellato, ma gli elementi così acquisiti potevano essere utilizzati solo ai fini della prosecuzione delle indagini e non avevano alcuna valenza probatoria in giudizio.

La nuova disciplina è sopravvissuta per una decina d'anni, prima del complessivo intervento di riordino nella materia sfociato nell'approvazione ed entrata in vigore del codice Vassalli al termine degli anni '80, che ha ridisegnato la disciplina delle intercettazioni telefoniche disponendo una disciplina specifica di tale strumento.

2.2. La nuova disciplina del codice del 1989

La crescente popolarità e diffusione dei sistemi di telefonia (prima fissa, ma progressivamente anche mobile, in specie in Italia dalla fine degli anni '90 in avanti) si deduce dalla scelta del riformatore del 1988 di dedicare alle intercettazioni di conversazioni o comunicazioni un apposito Capo (il IV) del Titolo III (dedicato ai mezzi di ricerca della prova) del Libro III (che contiene la disciplina delle prove) del nuovo codice di procedura penale.

Il testo si apriva con una disposizione dedicata ai limiti all'ammissibilità del ricorso alle intercettazioni telefoniche, che riproduceva in larga parte il contenuto del vecchio art. 226-bis, aggiungendo però che esse potessero essere disposte per tutti i delitti contro la pubblica amministrazione per i quali la pena non fosse inferiore nel massimo a cinque anni di reclusione[155]. La disposizione prevedeva altresì la possibilità

---

[154] Art. 9, d.l. 59/1978. I reati per i quali era consentita tale deroga alle ordinarie norme sulle intercettazioni telefoniche erano la banda armata (art. 306 c.p.), la strage (art. 422 c.p.), l'incendio (art. 423 c.p.), l'inondazione, frana o valanga (art. 426 c.p.), il naufragio, sommersione o disastro aviatorio (art. 428 c.p.), l'attentato alla sicurezza dei trasporti (art. 432, c.1 c.p.), l'attentato alla sicurezza degli impianti di energia elettrica e del gas, ovvero delle pubbliche comunicazioni (art. 433 c.p.), epidemia (art. 438 c.p.), avvelenamento di acque o sostanze alimentari (art. 439 c.p.), omicidio (art. 575 c.p.), rapina aggravata (art. 628, c.3 c.p.), estorsione aggravata (art. 629, c.2 c.p.), sequestro di persona a scopo di estorsione (art. 630 c.p.), riorganizzazione del partito fascista (art. 1-2, c.1, l. 645/1952), associazione per delinquere finalizzata al traffico di sostanze stupefacenti (art. 75, l. 685/1975) e in alcune ipotesi di infrazioni valutarie (art. 1, c.4-5, d.l. 31/1976).

[155] Art. 266 c.p.p., D.P.R. 22 settembre 1988, n. 447.

di disporre intercettazioni tra presenti (cd. intercettazioni ambientali), per un'analisi delle quali si rinvia *infra* §3.

Con la soppressione della figura del giudice istruttore e la modifica dell'architettura del processo penale, mutò necessariamente anche il procedimento di autorizzazione all'esperimento delle intercettazioni telefoniche, concesso dal giudice per le indagini preliminari su richiesta del pubblico ministero tramite un decreto motivato e accertata la presenza di gravi indizi di reato e nei casi in cui esse siano assolutamente indispensabili per la prosecuzione delle indagini.

La disposizione confermava l'obbligo per il pubblico ministero di indicare nel decreto che dispone l'intercettazione le modalità e la durata dell'operazione, che non può superare i quindici giorni ma può essere prorogata per la medesima durata senza limiti massimi, previo accertamento del permanere dei requisiti suindicati. Il testo indicava inoltre che il pubblico ministero potesse procedere personalmente alle operazioni o avvalersi di funzionari di polizia giudiziaria, aggiungendo l'obbligo di tenere un registro per l'annotazione di autorizzazione, convalida e proroga di ciascuna operazione di intercettazione, di cui vanno annotate data di inizio e fine[156].

Il quadro finora tratteggiato, pertanto, alterava la disciplina precedente soprattutto con riferimento alla natura degli indizi di reato che devono pre-esistere, che non basta più siano seri e concreti, ma devono essere qualificabili come gravi. Si tratta, quindi, di un aggravamento dell'onore probatorio a carico del pubblico ministero affinché il GIP possa concedere l'autorizzazione all'attività di captazione.

La nuova disciplina prevedeva inoltre un'ipotesi di intercettazioni disposte d'urgenza, laddove il ritardo possa arrecare nocumento alla prosecuzione delle indagini. In questi casi le operazioni sono disposte dal pubblico ministero per decreto, il quale tuttavia deve essere trasmesso al GIP entro le successive ventiquattro ore, così che entro le quarantotto ore dalla ricezione il decreto possa essere convalidato, a pena di decadenza, che implica l'obbligo di interrompere le intercettazioni e il divieto di utilizzo degli elementi di prova raccolti.

È pur vero che, per effetto dell'abrogazione implicita derivante dalla nuova disciplina dell'intera materia per mezzo di un codice di rito, la previsione legislativa

[156] Art. 267 c.p.p., D.P.R. 22 settembre 1988, n. 447.

riformulava il contenuto dell'art. 226-sexies come introdotto dal d.l. 59/1978, rimuovendo il rinvio ad altra disposizione per l'identificazione di specifiche fattispecie di reato per le quali è possibile disporre intercettazioni d'urgenza. Essa dettava però limiti temporali specifici entro i quali il decreto d'urgenza dovesse essere trasmesso al GIP ed egli dovesse procedere alla convalida, colpendo con la sanzione dell'inutilizzabilità tutto il materiale raccolto in forza di un decreto autorizzativo non tempestivamente convalidato. Inoltre, la previsione della concessione orale dell'autorizzazione da formalizzarsi non appena possibile in un decreto per iscritto veniva soppressa dopo soli dieci anni dalla sua introduzione.

La nuova disciplina dettava anche modifiche in ordine all'esecuzione in concreto delle operazioni di intercettazione, disponendo che nel verbale che viene redatto fosse trascritto anche in forma sommaria il contenuto delle comunicazioni intercettate (i cd. 'brogliacci'). Veniva confermato l'obbligo di procedere alle operazioni tramite gli impianti installati presso le procure, ma si disponeva che, laddove essi fossero insufficienti o se sussistessero eccezionali ragioni di urgenza, si potesse procedere tramite gli impianti di pubblico servizio o quelli in dotazione alla polizia giudiziaria, previa emanazione di un decreto motivato da parte del pubblico ministero.

Venivano confermate la trasmissione immediata dei verbali e il deposito in cancelleria, salvo che il GIP autorizzasse il pubblico ministero a ritardare quest'ultimo, in caso da esso potesse derivare un grave pregiudizio alle indagini. In ogni caso, al più tardi al termine delle indagini, i verbali devono essere depositati. La disposizione consentiva altresì ai difensori delle parti di esaminare gli atti e ascoltare le registrazioni entro dati termini, potendone estrarre copia. Si disponeva fossero acquisite le conversazioni non manifestamente irrilevanti, stralciando d'ufficio quelle inutilizzabili. Alle operazioni di stralcio possono partecipare pubblico ministero e legali delle parti, che vengono avvertiti almeno ventiquattro ore prima dell'operazione. Le conversazioni non irrilevanti sono dunque trascritte e vengono acquisite al fascicolo per il dibattimento[157].

[157] Art. 268, c.p.p., D.P.R. 22 settembre 1988, n. 447.

Il codice si preoccupava altresì della conservazione del materiale oggetto di intercettazione, disponendo che verbali e registrazioni fossero conservati presso il pubblico ministero che avesse disposto l'esperimento del mezzo di ricerca della prova, fino a che fosse pronunciata una sentenza non più soggetta a impugnazione. Gli interessati potevano in ogni caso chiedere la distruzione della documentazione non necessaria al procedimento al giudice che avesse autorizzato l'intercettazione, il quale, se la disponeva, assicurava che dell'operazione fosse redatto verbale[158].

Veniva confermata anche l'inutilizzabilità delle conversazioni nei procedimenti diversi da quelli per i quali le intercettazioni fossero state disposte, salvo che fossero indispensabili per l'accertamento di delitti per i quali è previsto l'arresto obbligatorio in flagranza[159]. Venivano infine colpiti da inutilizzabilità i risultati di quelle intercettazioni che fossero state eseguite fuori dai casi previsti dalla legge o in violazione delle disposizioni procedimentali, estendendo la categoria dell'inutilizzabilità anche alle intercettazioni di comunicazioni di persone che fossero ministri di culto, legali rappresentanti, periti incaricati, medici, chirurghi o comunque appartenenti a categorie professionali che devono serbare un segreto professionale, salvo che essi stessi le avessero divulgate in altro modo[160].

Le disposizioni del nuovo codice hanno subito negli anni successivi una serie impressionante di modifiche, dovute tanto all'azione del legislatore quanto alla giurisprudenza costituzionale, che hanno plasmato il quadro delle intercettazioni delle comunicazioni come conosciuto oggi. Tuttavia, tali troppo frequenti mutamenti di disciplina ne hanno indebolito la legittimità, con evidente sacrificio della certezza degli operatori del diritto e dei potenziali soggetti nei cui confronti tali mezzi di ricerca della prova siano esperiti.

Già nel 1991, con un provvedimento d'urgenza, il Governo predispose una modifica significativa dell'art. 267 c.p.p., che prevedeva la concessione dell'autorizzazione all'intercettazione al solo sussistere di sufficienti indizi di reato e un prolungamento del termine massimo della prima autorizzazione a quaranta giorni e delle successive proroghe, che potevano essere disposte dal pubblico ministero stesso

[158] Art. 269, c.p.p., D.P.R. 22 settembre 1988, n. 447.
[159] Art. 270, c.p.p., D.P.R. 22 settembre 1988, n. 447.
[160] Art. 271, c.p.p., D.P.R. 22 settembre 1988, n. 447.

in casi di urgenza, a venti giorni ciascuna[161]. In sede di conversione, le Camere mitigarono la portata della novella legislativa, prevedendo che le modifiche della disciplina originaria del codice si applicassero soltanto con riferimento ai delitti di criminalità organizzata e di minaccia con l'uso del telefono, mantenendo per tutti gli altri reati la soglia della sussistenza della gravità degli indizi e i termini temporali di quindici giorni per la prima autorizzazione e i successivi rinnovi[162]. Una tale modifica del testo del decreto, se da un lato dimostra la volontà del Parlamento di mantenere una soglia di tutela più elevata della riservatezza dei singoli, è spia del momento storico di aperto contrasto dello Stato con la criminalità organizzata, che viene sottoposta a una disciplina probatoria particolarmente penalizzante.

La riforma del codice proseguì negli anni seguenti con la previsione di un regime meno garantistico per le intercettazioni ambientali nei luoghi di domicilio nell'ambito delle indagini sui reati di criminalità organizzata (v. *infra*, §3) e con l'introduzione della fattispecie delle intercettazioni di comunicazioni telematiche e informatiche (v. *infra*, §4). Fu inoltre ampliato il novero dei reati per i quali è prevista la possibilità di ricorrere alle intercettazioni telefoniche, inserendo l'usura e l'abusiva attività finanziaria[163], l'abuso di informazioni privilegiate e la manipolazione del mercato[164], i delitti previsti dall'art. 600-ter, c.3 c.p.[165], anche se relativi al materiale pornografico virtuale (art. 600-quater 1 c.p.)[166], e dall'art. 609-undecies[167], i delitti di commercio di sostanze alimentari nocive (art. 444 c.p.), contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.), introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.), frode nell'esercizio del commercio (art. 515 c.p.), vendita di sostanze alimentari non genuine

---

[161] Art. 13, decreto-legge 13 maggio 1991, n. 152.
[162] L. 12 luglio 1991, n. 203.
[163] Art. 8, l. 7 marzo 1996, n. 108.
[164] Art. 9, c.5, l. 18 aprile 2005, n. 62.
[165] Art. 12, l. 3 agosto 1998, n. 269. Si tratta dei reati di distribuzione, divulgazione, diffusione o pubblicizzazione di materiale pedo-pornografico o distribuzione o divulgazione di notizie o informazioni finalizzate ad adescamento o sfruttamento sessuale di minori.
[166] Art. 13, l. 6 febbraio 2006, n. 38.
[167] Art. 4, d. lgs. 4 marzo 2014, n. 39. Si tratta del reato di adescamento di minore di sedici anni al fine di commettere i reati di riduzione o mantenimento in schiavitù o in servitù, prostituzione o pornografia minorile, detenzione di materiale pedo-pornografico, iniziative turistiche volte allo sfruttamento della prostituzione minorile, violenza sessuale, atti sessuali con minorenne, corruzione di minorenne e violenza sessuale di gruppo.

come genuine (art. 516 c.p.), contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-quater c.p.) e invasione di terreni o edifici (art. 633 c.p.)[168], atti persecutori (cd. stalking, art. 612-bis c.p.)[169] e, infine, delitti commessi avvalendosi del vincolo sodalizio dell'associazione mafiosa o al fine di agevolarne le attività[170].

In parallelo alla riforma costituzionale dell'art. 111 Cost., che iscrisse il principio del giusto processo in Costituzione[171], l'art. 267 c.p.p. fu integrato dall'aggiunta di un comma 1-bis, che disponeva che nella valutazione dei gravi indizi di reato si applicasse l'art. 203 c.p.p., che prevede che il magistrato non possa obbligare agenti, ufficiali di polizia giudiziaria o dipendenti dei servizi segreti a rivelare l'identità di propri informatori. Tuttavia, la mancata escussione dei medesimi come testi rendeva le informazioni da essi rese non acquisibili né utilizzabili. Quindi queste ultime non potevano considerarsi al fine della determinazione della sussistenza dei gravi indizi di reato per autorizzare l'esperimento di intercettazioni telefoniche[172].

Il legislatore si è altresì preoccupato di introdurre una disposizione normativa *ad hoc* per disciplinare il caso in cui nell'esperimento dell'attività di intercettazione, l'autorità procedente si imbatta in comunicazioni di soggetti impiegati dai servizi segreti. In questo caso, il giudice deve disporre la secretazione dei verbali e delle registrazioni e la trasmissione di copia della documentazione di cui ci si voglia avvalere in giudizio al Presidente del Consiglio dei ministri, ai fini dell'accertamento dell'eventuale copertura di taluna delle informazioni contenute da parte di segreto di Stato. La disciplina prevede altresì la possibilità di utilizzare le informazioni prima del termine entro il quale il segreto di Stato debba essere opposto (60 giorni) solo in ipotesi di pericolo di inquinamento delle prove, pericolo di fuga o laddove sia necessario intervenire per la prevenzione o l'interruzione della commissione di un delitto con pena massima prevista di almeno quattro anni. La legittima opposizione del segreto

---

[168] Art. 14, l. 14 gennaio 2013, n. 9.
[169] Art. 2, c.1, lett. 0b), d.l. 14 agosto 2013, n. 93, come modificato in sede di conversione dalla l. 15 ottobre 2013, n. 119.
[170] Art. 2, c.1, let. b-bis), d.l. 30 dicembre 2019, n. 161.
[171] Legge costituzionale 23 novembre 1999, n. 2, *Inserimento dei principi del giusto processo nell'articolo 111 della Costituzione.*
[172] Art. 10, l. 1 marzo 2001, n. 63.

impedisce all'autorità giudiziaria l'utilizzo delle informazioni coperte dal segreto nel procedimento[173].

La disciplina delle intercettazioni telefoniche è stata altresì oggetto di scrutinio della Consulta, che nel 2008 ha accolto una questione di legittimità costituzionale sollevata dal GIP del Tribunale di Catanzaro con riferimento alla possibilità, prevista nell'art. 268 c.p.p., di poter rinviare il deposito delle registrazioni qualora da esso possa derivare un grave pregiudizio per le indagini[174]. Tale deroga al regime tradizionale del deposito di registrazioni e verbali, combinata con l'orientamento della giurisprudenza di legittimità secondo il quale la richiesta di misure cautelari (in particolare personali) può essere formulata dal pubblico ministero anche sulla base dei soli 'brogliacci'[175], lederebbe il diritto alla piena difesa del destinatario della misura cautelare (art. 24 Cost.) e il principio della parità delle parti nel processo, essendo inibito al legale l'esame diretto della registrazione.

La Corte condivide la prospettazione del giudice remittente, sottolineando come la lettura delle trascrizioni di polizia giudiziaria, che non avviene con le garanzie di una trascrizione peritale, non può sostituirsi efficacemente all'ascolto diretto delle conversazioni registrate senza per ciò stesso cagionare un sacrificio ingiustificato del diritto di difesa in giudizio (non controbilanciato da un interesse alla riservatezza del contenuto della registrazione, che viene meno dato l'avvenuto deposito della trascrizione). Per tali ragioni, la Corte ha ritenuto che la soluzione più conforme al dettato costituzionale fosse quella di consentire al difensore dell'imputato o dell'indagato di poter accedere direttamente alle registrazioni e di poterne estrarre copia, senza per questo costringere il pubblico ministero obbligatoriamente al deposito delle registrazioni insieme ai brogliacci.

Peraltro, la pronuncia del giudice delle leggi non ha sgombrato del tutto il campo dai dubbi, poiché le modalità di tale diritto d'accesso del difensore sono state lasciate all'elaborazione giurisprudenziale, la quale, pur prevedendo una sorta di *vademecum* che soddisfacesse tale interesse della difesa del soggetto sottoposto a

---

[173] Art. 270-bis c.p.p., l. 3 agosto 2007, n. 124.
[174] Corte cost., sent. 336/2008.
[175] La stessa sentenza della Corte costituzionale menziona Cass. pen., sent. n. 36439/2004 e sent. n. 39469/2004.

misura cautelare[176], ha visto accendersi un vivace dibattito sul diritto del difensore a ottenere certificazione di conformità della copia alla registrazione originale (la giurisprudenza si è orientata nel senso di negare la sussistenza di tale ulteriore diritto)[177]. Più di recente, la giurisprudenza di legittimità ha altresì affermato che l'accesso alle registrazioni sia garantito alla difesa anche in caso di impugnazione da parte del pubblico ministero del rigetto della misura cautelare proposta[178].

2.3. La riforma promessa (ma in parte tradita) del decreto Orlando

La disciplina delle intercettazioni di comunicazioni è stata da ultimo oggetto di una revisione significativa, contenuta in un decreto legislativo approvato dal Governo al termine del 2017 in esecuzione di una legge di delega parlamentare e i cui effetti non si sono ancora del tutto spiegati nell'ordinamento[179]. La materia è stata però magmatica nei tre anni successivi e in più occasioni disposizioni normative introdotte dal suddetto decreto non sono sopravvissute ai successivi interventi, spiegando dunque i propri effetti per un arco temporale molto limitato.

In particolare, l'atto normativo in questione disponeva l'integrazione dell'art. 267 c.p.p. prevedendo che l'ufficiale di polizia giudiziaria incaricato procedesse all'esperimento dell'operazione curando che nel verbale non fossero presenti espressioni lesive della reputazione delle persone o riguardanti dati personali definiti sensibili dalla legge, salva la rilevanza degli stessi ai fini dell'indagine[180]. Il decreto legislativo integrava altresì la disposizione seguente, inserendo un c.2-bis all'art. 268

---

[176] Cass. pen. SS.UU., sent. n. 20300/2010, 22 aprile 2010 (Lasala).

[177] L. Pistorelli, *Accesso difensivo alle registrazioni delle intercettazioni, tra limiti normativi ed evoluzione tecnologica*, 15 gennaio 2012, nota a Cass. pen., sez. VI, 9 novembre 2011 (dep. 24 novembre 2011), n. 43654, Pres. De Roberto, Rel. Petruzzellis, ric. Aga e a Tribunale di Trani, ord. 16 giugno 2011, Pres. Carone, Est. Gadaleta, disponibile all'url: https://archiviodpc.dirittopenaleuomo.org/d/1172-accesso-difensivo-alle-registrazioni-delle-intercettazioni-tra-limiti-normativi-ed-evoluzione-tecno (ultimo accesso: 25 novembre 2020).

[178] Cass. pen., sez. VI, sent. n. 33046/2018, 25 gennaio 2018.

[179] D. lgs. 29 dicembre 2017, n. 216, in attuazione della delega di cui all'art. 1, cc. 82, 83 e 84, lett. a), b), c), d) ed e) l. 23 giugno 2017, n. 103. Sul contenuto della legge di delega si veda S. Lonati, *I criteri direttivi contenuti nella delega in materia di intercettazioni di conversazioni e comunicazioni*, in O. Mazza (a cura di), *Le nuove intercettazioni*, Torino, Giappichelli, 2018, 1-26.

[180] Art. 2, c.1, lett. c), d. lgs. 216/2017. Il periodo è stato abrogato a opera dell'art. 2, c.1, lett. d), n. 3, d.l. 30 dicembre 2019, n. 161. Tuttavia, l'art. 2, c.1, lett. e), n. 1 ne dispone l'introduzione come c.2-bis dell'art. 268 c.p.p.

c.p.p., a norme del quale si vietava la trascrizione, anche sommaria, di comunicazioni e conversazioni irrilevanti ai fini delle indagini, sia sotto un profilo soggettivo che oggettivo, o riguardanti dati personali sensibili pure non rilevanti per l'indagine. Tuttavia, il pubblico ministero avrebbe potuto richiederne la trascrizione nel verbale tramite decreto motivato, laddove le ritenesse rilevanti per i fatti oggetto di prova, ivi comprese quelle riguardanti dati personali sensibili (c.2-ter)[181]. Inoltre, il testo del decreto disponeva la trasmissione al pubblico ministero di verbali e registrazioni immediatamente dopo la scadenza del termine per l'esperimento delle intercettazioni, con facoltà dello stesso PM di differire la trasmissione in casi di complesse indagini che richiedessero una consultazione delle risultanze acquisite. Infine, veniva disposta l'abrogazione dei successivi commi 5, 6, 7 e 8[182].

Lo stesso atto normativo introduceva tre nuove disposizioni riguardanti le modalità di esecuzione delle intercettazioni, prevedendo che entro cinque giorni dalla conclusione dell'operazione il pubblico ministero procedesse al deposito di tutti i materiali raccolti e i decreti di autorizzazione, convalida o proroga, selezionando quelli rilevanti a fini probatori. Ciò per consentire ai difensori delle parti in causa di esaminare gli atti e prendere visione dei mezzi di prova selezionati e cognizione delle conversazioni o comunicazioni intercettate. In caso di grave pregiudizio per le indagini che potesse derivare dal deposito di tali documenti, si disponeva la facoltà del giudice di autorizzare il pubblico ministero a differire il rinvio fino al momento della chiusura delle indagini[183].

Inoltre, si prescriveva che il pubblico ministero disponesse l'acquisizione delle comunicazioni o conversazioni utilizzate nel corso delle indagini preliminari a supporto dell'adozione di una misura cautelare, avendo cura di inserire verbali e atti relativi nell'apposito fascicolo presso il pubblico ministero in cui sono conservati l'atto contenente la notizia di reato e la documentazione relativa alle indagini. In tutti gli altri casi, il PM doveva presentare richiesta di acquisizione al giudice entro cinque

[181] Questa previsione non è più possibile oggi a seguito dell'abrogazione del c. 2-ter da parte dell'art. 2, c.1, lett. e), n. 2, d.l. 30 dicembre 2019, n. 161.
[182] Art. 2, c.1, lett. d), e) d. lgs. 216/2017. Il c. 4 è stato poi sostituito dall'art. 2, c.1, lett. e), n. 3, d.l. 30 dicembre 2019, n. 161, che ha altresì disposto la reintroduzione dei commi 5, 6, 7 e 8.
[183] Art. 268-bis c.p.p., introdotto dall'art. 3, c.1, lett. b), d. lgs. 216/2017.

giorni dal deposito dei materiali di cui alla disposizione precedente. I difensori, entro dieci giorni (prorogabili di altri dieci per indagini complesse) dalla ricezione dell'avviso di cui all'art. 268-bis, c.1, avevano facoltà di richiedere l'acquisizione di materiali rilevanti a fini probatori e non inclusi nell'elenco formato dal PM, oppure l'eliminazione di quelli compresi ma inutilizzabili o dei quali fosse vietata la trascrizione. La richiesta di eliminazione dei materiali originariamente inseriti nell'elenco era consentita entro i medesimi termini anche allo stesso pubblico ministero, laddove essi fossero divenuti irrilevanti sulla base di elementi sopravvenuti[184].

La terza disposizione introdotta dal decreto sul tema delle modalità di esecuzione delle operazioni di intercettazione prevedeva che il GIP disponesse, dopo cinque giorni dalla presentazione delle richieste, con ordinanza emessa in camera di consiglio, l'acquisizione delle conversazioni e comunicazioni indicate dalle parti, a meno che fossero manifestamente irrilevanti, e ordinasse lo stralcio di quelle di cui fosse vietato l'utilizzo. L'ordinanza valeva a sollevare il segreto su atti e verbali delle comunicazioni in questione e il giudice doveva ordinare la trascrizione sommaria di quelle acquisite su richiesta dei difensori, i quali potevano anche ottenere copia in forma digitale delle registrazioni e dei verbali delle comunicazioni acquisite[185].

L'atto interveniva altresì a modificare l'articolo 269 c.p.p., disponendo la sostituzione del c. 1 così da prevedere che verbali e registrazioni fossero conservati in un apposito archivio riservato presso l'ufficio del PM che avesse richiesto ed eseguito le operazioni di intercettazione e che su di esse vigesse il segreto[186]. L'accesso all'archivio e l'ascolto delle registrazioni era comunque consentito al GIP e ai difensori dell'imputato. Non erano invece coperti da segreto verbali e registrazioni depositate nel fascicolo formato presso il PM, in cui sono conservati l'atto contenente la notizia di reato e la documentazione delle indagini. Inoltre, la possibilità di chiedere la

[184] Art. 268-ter c.p.p., introdotto dall'art. 3, c.1, lett. b), d. lgs. 216/2017.
[185] Art. 268-quater c.p.p., introdotto dall'art. 3, c.1, lett. b), d. lgs. 216/2017.
[186] La custodia di verbali e supporti delle registrazioni entro un archivio riservato del pubblico ministero era già stata ipotizzata dal progetto Alfano nel corso della XV legislatura (C 1415), v. C. Fiorio, *Intercettazioni telefoniche e diritti costituzionalmente garantiti fra frammenti di storia parlamentare e prospettive* de iure condendo, in A. Gaito (a cura di), *Riservatezza e intercettazioni tra norma e prassi*, Roma, Aracne, 2011, 283-297.

distruzione di registrazioni e verbali a fini di tutela della riservatezza veniva specificamente circoscritta alle registrazioni non acquisite[187].

L'ulteriore grande novità introdotta dal decreto legislativo in commento è stata la disciplina espressa dell'intercettazione fra presenti che si serva dello strumento del captatore informatico inoculato su un dispositivo elettronico portatile (Art. 266, c.2 c.p.p.), per la cui trattazione specifica si rinvia al Cap. IV, §4. L'intervento legislativo disponeva che essa fosse sempre possibile nel caso dei procedimenti per i delitti di cui all'art. 51, c.3-bis e 3-quater c.p.p[188]. La nuova forma di intercettazione è caratterizzata anche da un contenuto specifico del decreto di autorizzazione (art. 267, c.1) e dalla possibilità di agire nelle situazioni di urgenza senza attendere l'autorizzazione del giudice solo per quei reati di cui sopra (art. 267, c.2-bis)[189]. Essa contempla altresì la facoltà della polizia giudiziaria di avvalersi di persone idonee alle operazioni tecniche da eseguire, come peraltro dispone anche l'art. 348, c.4 c.p.p. in generale[190].

Per quanto riguarda le preclusioni all'utilizzo dei risultati di tali intercettazioni, è disposto che esse non possano essere utilizzate per la prova di reati diversi da quelli per il cui perseguimento siano state esperite, salvo che siano indispensabili per l'accertamento di delitti soggetti all'arresto obbligatorio in flagranza (art. 270, c.1-bis c.p.p.), peraltro così riproducendo il contenuto del c. 1[191]. Infine, anche l'art. 271 è stato oggetto di modifica, così che non siano mai utilizzabili dati che siano stati acquisiti tramite operazioni preliminari all'inoculazione del captatore informatico sul dispositivo *target*, nonché quelli ottenuti al di fuori dei limiti del decreto autorizzativo (art. 271, c.1-bis)[192].

Vi è però da precisare che l'art. 9 prevedeva il differimento dell'entrata in vigore di gran parte delle disposizioni del decreto legislativo (centottanta giorni per gli artt. 2, 3, 4, 5 e 7), e che con provvedimenti successivi il legislatore ha rinviato il momento di entrata in vigore fino al 31 agosto 2020[193].

---

[187] Art. 3, c.1, lett. c), d. lgs. 216/2017.
[188] Art. 4, c.1, lett. a), d. lgs. 216/2017.
[189] Art. 4, c.1, lett. b), d. lgs. 216/2017.
[190] Art. 4, c.1, lett. c), d. lgs. 216/2017.
[191] Art. 4, c.1, lett. d), d. lgs. 216/2017.
[192] Art. 4, c.1, lett. e), d. lgs. 216/2017.
[193] In ordine cronologico: d.l. 25 luglio 2018, n. 91; l. 30 dicembre 2018, n. 145; d.l. 14 giugno 2019, n. 53; d.l. 30 dicembre 2019, n. 161; l. 20 febbraio 2020, n. 7; d.l. 30 aprile 2020, n. 28.

La riforma del 2017, pur perseguendo astrattamente il lodevole fine di introdurre disposizioni volte a garantire la riservatezza delle comunicazioni in ossequio al principio sancito dall'art. 15 Cost., non è stata immune da censure significative, che possono aver pesato sul parziale ripensamento di alcune disposizioni da parte del legislatore poco più di due anni dopo, come si vedrà di seguito. In particolare, è stato messo in luce come l'autonomia del legislatore sia stata scarsa e la spina dorsale della delega sia stata oggetto non tanto di una riflessione sistematica in sede politica, bensì piuttosto di un coacervo raccogliticcio di regole pratiche desunte dalla giurisprudenza da un lato e dalle circolari emesse da alcune fra le più importanti procure della repubblica. Ciò ha condotto, in concreto, alla previsione di un meccanismo che poteva apparire farraginoso già a uno sguardo preventivo[194], che richiedeva alla polizia giudiziaria di astenersi dalla trascrizione delle comunicazioni non rilevanti, dovendo indicarne soltanto data, orario e dispositivo, per poi comunque darne contezza al pubblico ministero che potesse rettificare la valutazione della p.g. e, in conseguenza di tale passaggio, dover formalmente notificare le annotazioni sulle intercettazioni scartate ai difensori dei soggetti indagati. In ogni caso, sull'acquisizione o eliminazione delle intercettazioni (ir)rilevanti o (in)utilizzabili decide in ultima istanza il giudice[195].

All'inizio del 2019 il legislatore, nell'ambito di una più ampia iniziativa normativa volto al contrasto dei reati contro la pubblica amministrazione, ha modificato ulteriormente l'art. 266, c.2-bis c.p.p., aggiungendo anche i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con una pena pari nel

---

[194] Una ricostruzione problematizzante della nuova disciplina è offerta da C. Gabrielli, *Dall'esecuzione di operazioni di ascolto all'acquisizione delle captazioni rilevanti*, in G. Giostra-R. Orlandi (a cura di), *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, Torino, Giappichelli, 2018, 3-30. Sulle sfide che si potevano ragionevolmente prevedere sotto il profilo pratico laddove la disciplina fosse entrata in vigore, si rinvia a P. Rivello, *Il procedimento acquisitivo delle intercettazioni e l'archivio riservato presso il pubblico ministero*, in O. Mazza (a cura di), *Le nuove intercettazioni*, Torino, Giappichelli, 2018, 55-100.

[195] Sull'infelicità dell'idea madre di limitare la trascrizione della p.g. alle sole conversazioni rilevanti e sul malriuscito *drafting* legislativo della legge di delegazione, che si risolverebbe in un complicato arabesco, v. G. Giostra, *Il segreto estende i suoi confini e la sua durata*, in G. Giostra-R. Orlandi (a cura di), *op. cit.*, 115-135, in particolare 116-118. L'A. affronta altresì il nodo spinoso della segretezza degli atti non di indagine e, in quanto tali, pubblicabili, dando conto del tentativo del legislatore di estendere la sfera di applicazione della segretezza anche ad altri atti, in particolare quelli attinenti al procedimento cautelare, per tutelare la riservatezza delle conversazioni dell'indagato da un'eventuale diffusione e pubblicazione a mezzo stampa.

massimo ad almeno cinque anni di reclusione fra quelli per i quali l'intercettazione tra presenti per mezzo del captatore è sempre consentita, adattando a questo proposito anche il primo comma dell'art. 267 c.p.p[196].

L'ultimo intervento in ordine di tempo sulla disciplina delle intercettazioni risale al decreto-legge adottato il penultimo giorno del 2019 che, oltre a prorogare il termine di entrata in vigore delle disposizioni novellate, è intervenuto a modificare nuovamente alcune di esse. In particolare, la previsione dell'esperibilità in ogni caso delle intercettazioni per mezzo di captatore nei confronti dei delitti dei pubblici ufficiali o incaricati di pubblico servizio contro la pubblica amministrazione di cui sopra viene vincolata alla previa indicazione delle ragioni che ne giustifichino l'utilizzo anche nei luoghi di privata dimora, peraltro modificando così per la seconda volta in meno di un anno solare la medesima disposizione (idem dicasi per l'art. 267, cc.1 e 2-bis, che vengono modificati per adeguarli alla nuova formulazione dell'art. 266, c.2-bis)[197].

Se delle nuove modifiche all'art. 268 c.p.p., che hanno riorganizzato la struttura della disposizione, si è già detto *supra*, si deve infine dar conto delle modifiche all'art. 269 c.p.p. Viene infatti introdotto un nuovo c.1, a norma del quale verbali e registrazioni sono conservati integralmente in un apposito archivio gestito, diretto e sorvegliato dal Procuratore della Repubblica e non sono coperti da segreto solo i materiali nel fascicolo che raccoglie la documentazione delle indagini o quelli utilizzati nel corso delle indagini preliminari. È consentito in ogni caso l'accesso alle registrazioni e ai verbali a giudice e difensori delle parti a seguito del deposito. L'atto abroga il c.1-bis dell'art. 269 e introduce una nuova versione del c.2, che prevede la conservazione delle registrazioni fino alla pronuncia di sentenza non più impugnabile, salve quelle inutilizzabili, pur potendo gli interessati chiederne la distruzione al

[196] Art. 1, c.4, lett. a) e b), l. 9 gennaio 2019, n. 3. Il tema della speciale disciplina applicabile alle due categorie di reati di cui all'art. 266, c.2-bis c.p.p. è affrontato, per quanto prima dell'intervento della fonte sopracitata e sulla base dei soli contenuti della legge di delegazione, da G. Varraso, *Le intercettazioni e i regimi processuali differenziati per i reati di "grande criminalità" e per i delitti dei pubblici ufficiali contro la pubblica amministrazione,* in O. Mazza (a cura di), *op. cit.*, 139-161.
[197] Art. 2, c.1, lett. c) e d), d.l. 30 dicembre 2019, n. 161.

giudice per tutelare la propria riservatezza laddove le stesse non siano necessarie per il procedimento[198].

L'ultimo intervento emendativo riguarda l'articolo 270 c.p.p., che dispone oggi, come già in precedenza, che i risultati delle intercettazioni non possano essere utilizzati in procedimenti diversi tranne per i casi in cui essi siano rilevanti e indispensabili per l'accertamento di delitti per i quali sia previsto l'arresto obbligatorio in flagranza, ma anche per l'accertamento dei reati di cui all'art. 266, c.1 c.p.p. (vale a dire tutti quelli per i quali possano essere autorizzate operazioni di intercettazione telefonica). Viene inoltre precisato che i risultati delle intercettazioni disposte con captatore informatico possano essere utilizzati anche per la prova di reati diversi da quelli perseguiti tramite il loro esperimento, laddove siano indispensabili per l'accertamento di delitti di cui all'art. 266, c.2-bis (vale a dire quelli di cui all'art. 51, commi 3-bis e 3-quater c.p.p. e quelli dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione puniti con pena non inferiore nel massimo a cinque anni)[199]. Infine, forse anche sulla scorta delle critiche delle quali si è dato succintamente conto *supra*, la fonte ha abrogato gli artt. 268-bis, -ter e -quater, eliminando quel complicato meccanismo introdotto dal d. lgs. 216/2017 che prevedeva la trascrizione delle sole intercettazioni rilevanti da parte della p.g., limitandosi ad annotare solo data, ora e dispositivo di quelle considerate irrilevanti[200].

Come si può desumere dalla trattazione di cui sopra, la materia è stata dunque oggetto di numerosi interventi legislativi nel corso del trentennio di vigenza del Codice Vassalli e si trova in questo momento in una fase particolarmente dinamica, che ha visto una riforma significativa della disciplina, anche per tener conto dell'evoluzione tecnologica, che ancora deve dare prova di sé in concreto, anche se il mutamento tanto rapido e continuo delle disposizioni normative non può che ingenerare qualche perplessità nell'interprete sulla visione d'insieme e il coordinamento del legislatore stesso (per quanto ci sia stato un passaggio da una legislatura e un'altra nel frattempo).

---

[198] Art. 2, c.1, lett. f), d.l. 161/2019.
[199] Art. 2, c.1, lett. g), d.l. 161/2019.
[200] Art. 2, c.1, lett. q), d.l. 161/2019.

2.4. La funzione della motivazione

La trattazione dell'evoluzione della disciplina normativa delle intercettazioni telefoniche fa emergere la centralità che la motivazione del decreto che autorizza l'esperimento di questo mezzo di prova ricopre nell'assicurazione delle garanzie costituzionalmente sancite per i singoli. Invero, sarebbe certamente frustrato lo scopo della riserva di giurisdizione non derogabile di cui all'art. 15 Cost., alla quale è vincolata qualsiasi interferenza con la libertà e la segretezza della corrispondenza, qualora si consentisse al giudice di disporre l'operazione di intercettazioni con un provvedimento non motivato oppure laddove il medesimo atto si risolvesse in un mero esercizio di stile *pro forma*. La rilevanza della motivazione ai fini della determinazione della legittimità del ricorso all'intercettazione e, di conseguenza, della utilizzabilità delle prove raccolte era stata sottolineata con chiarezza già nella storica sentenza 34/1973 della Corte costituzionale, il cui portato dovrebbe orientare ancor'oggi l'interpretazione delle disposizioni in materia.

La giurisprudenza di legittimità ha senz'altro contribuito al tentativo di delineare in concreto quali siano i connotati di una legittima motivazione del decreto di autorizzazione, pur con qualche oscillazione fra le decisioni delle diverse sezioni. In particolare, il requisito della sussistenza dei gravi indizi di reato è stato ritenuto validamente integrato laddove il provvedimento contenga un'esposizione, pur sommaria, degli elementi sulla base dei quali sia possibile formulare un giudizio probabilistico sull'avvenimento della condotta di reato[201]. Diversamente, sono state ritenute idonee all'integrazione del requisito della sufficienza degli indizi di reato nelle indagini su reati associativi anche le sole informazioni raccolte dagli organi di p.g. e trasmesse al PM, il quale le abbia poste a fondamento della richiesta di autorizzazione[202].

[201] Cass. pen., Sez. II, sent. n. 2873/1997, 10 ottobre 1997; conforme Cass. pen., Sez. V, sent. n. 776/2000, 9 marzo 2000.
[202] Cass. pen., SS.UU., sent. n. 17/2000, 21 settembre 2000; Cass. pen., Sez. VI, sent. n. 1625/2003, 15 gennaio 2003.

Altra questione dibattuta è il grado di autonomia del decreto del GIP rispetto al contenuto della richiesta del PM. Se un indirizzo interpretativo minoritario ha di fatto avallato la recezione in toto in motivazione delle ragioni che secondo il pubblico ministero fondano la richiesta[203], la giurisprudenza maggioritaria ritiene che dal provvedimento debba emergere in ogni caso un'avvenuta valutazione critica degli elementi addotti dal PM a supporto della richiesta[204] ed esclude che la motivazione si possa risolvere in una mera perifrasi del contenuto del dettato legislativo in materia[205]. Minori sarebbero invece gli oneri con riferimento alla proroga di un'autorizzazione in precedenza già concessa[206], ben potendosi procedere a motivare *per relationem*, senza che in ogni caso ciò consenta di riprodurre in toto il contenuto del decreto precedente[207]. La sanzione prevista in caso di motivazione apparente, vale a dire del tutto incongrua a supportare il provvedimento, sarebbe l'inutilizzabilità a fini processuali delle conversazioni captate[208], mentre si avrebbe difetto sanabile in sede di impugnazione della legittimità del ricorso al mezzo di prova se la motivazione fosse soltanto incompleta, insufficiente o inadeguata[209].

Un altro ambito entro il quale l'intervento della Suprema Corte è servito da guida interpretativa è quello della deroga all'ordine logico e procedurale prescritto, a norma del quale il pubblico ministero deve richiedere al giudice l'autorizzazione all'esperimento di tale mezzo di ricerca della prova tramite gli impianti installati presso la Procura della repubblica. Questo meccanismo viene spesso disatteso nella prassi, dandosi sovente il caso di operazioni condotte tramite impianti esterni privati

---

[203] Cass. pen., Sez. I, sent. n. 22/1998, 4 aprile 1998.
[204] Cass. pen., Sez. I, sent. n. 1495/1998, 4 maggio 1998; Cass. pen., Sez. I, sent. n. 2505/1999, 17 giugno 1999; Cass. pen., Sez. III, sent. n. 2780/1999, 13 ottobre 1999; Cass. pen., Sez. VI, sent. n. 46056/2008, 12 dicembre 2008.
[205] Cass. pen., Sez. VI, sent. n. 4057/1999, 6 ottobre 1999.
[206] Cass. pen., Sez. VI, sent. n. 8645/1999, 7 luglio 1999.
[207] Cass. pen., Sez. I, sent. n. 1495/1998, 4 maggio 1998.
[208] Cass. pen., Sez. IV, sent. n. 48543/2018, 24 ottobre 2018.
[209] Cass. pen., SS.UU., sent. n. 17/2000, 21 settembre 2000; le Sezioni Unite illustrano altresì quando la motivazione *per relationem* si possa dire legittima: essa deve fare riferimento a un legittimo atto del procedimento, la cui motivazione risulti congrua rispetto all'esigenza di giustificazione propria del provvedimento di destinazione; deve fornire la dimostrazione che il giudice abbia preso cognizione del contenuto sostanziale delle ragioni del provvedimento di riferimento, le abbia analizzate e infine ritenute coerenti con la sua decisione; inoltre, l'atto di riferimento, quando non allegato o trascritto nel provvedimento da motivare, deve essere conosciuto o conoscibile dall'interessato ai fini dell'esercizio del diritto di impugnazione. V. anche Cass. pen., Sez. IV, sent. n. 32667/2002, 1 ottobre 2002.

o in dotazione alla polizia giudiziaria[210]. La giurisprudenza di legittimità ha dapprima riconosciuto al PM una certa discrezionalità nella determinazione degli strumenti ai quali fare ricorso per esperire l'operazione di intercettazione, laddove sia stata adeguatamente motivata l'impossibilità di procedere efficacemente per mezzo degli impianti installati presso la Procura della Repubblica[211], senza che sia necessario indicare la ragione di tale carenza[212]. Addirittura, nemmeno sarebbe necessario un ulteriore provvedimento *ad hoc* per la proroga di un'autorizzazione a svolgere intercettazioni tramite impianti diversi da quelli della Procura[213].

Il tema si è posto anche con riferimento alla possibilità di ricorrere alla motivazione postuma dei decreti autorizzativi da parte del PM, con riferimento alla quale la giurisprudenza di legittimità ha sancito un obbligo di intervento, anche eventualmente con un'integrazione in un secondo momento, che deve sussistere prima dell'inizio dell'esecuzione delle operazioni, a pena di inutilizzabilità delle prove raccolte[214]. La Suprema Corte ha altresì censurato la motivazione dei decreti del PM di cui si è detto sopra quando si risolvano in mere clausole di stile e siano insuscettibili di comprendere le reali cause di indisponibilità degli impianti della Procura[215]. Essa ha anche aggiunto che non spetta al giudice integrare la motivazione eventualmente carente o tardiva del pubblico ministero, poiché è su quest'ultimo che grava l'onere di dimostrare l'esistenza delle motivazioni del ricorso a impianti esterni, non residuando al giudice alcun compito all'infuori della valutazione dell'iter argomentativo contemplato dal decreto autorizzativo[216].

Più di recente, la giurisprudenza di legittimità si è anche espressa sul tema dell'acquisizione dei tabulati relativi al traffico telefonico, che tuttavia pertengono più all'ambito delle informazioni riservate riguardo alla persona che non al segreto del

---

[210] L'argomento dell'esternalizzazione dell'esecuzione fuori dalle mura della procura, ricorrendo alla deroga prevista dal codice stesso, è sviscerato da N.E. La Rocca, *L'utilizzo di impianti esterni alla Procura e l'ascolto "remotizzato"*, in A. Gaito (a cura di), *Riservatezza ed intercettazioni tra norma e prassi*, *op. cit.*, 149-163.
[211] Cass. pen., Sez. VI, sent. n. 7/1997, 4 marzo 1997.
[212] Cass. pen., Sez. II, sent. n. 2539/2000, 25 maggio 2000.
[213] Cass. pen., SS.UU., sent. n. 42792/2001, 28 novembre 2001.
[214] Cass., SS. UU. pen., sent. n. 2737/2006, 29 novembre 2005 (Campenni).
[215] Cass., SS. UU. pen., sent. n. 30347/2007, 12 luglio 2007 (Aguneche).
[216] F. Giunchedi, *La motivazione dei decreti autorizzativi nell'interpretazione delle Sezioni Unite*, in A. Gaito (a cura di), *Riservatezza e intercettazioni tra norma e prassi*, *op. cit.*, 141-147.

contenuto delle comunicazioni. Proprio la differente natura dell'interesse sottostante e, correlativamente, un livello inferiore di intrusione nella sfera di riservatezza delle persone fondano un obbligo di motivazione meno severo in questo ambito, persino limitato all'assoluta necessità di procedere alle operazioni in questione ai fini della prosecuzione delle indagini[217].

Infine, il tema della motivazione dei decreti che autorizzano l'esperimento del mezzo di prova delle intercettazioni è stato nuovamente affrontato più di recente dalla Suprema Corte, la quale ha sancito come debba emergere dal percorso argomentativo il collegamento tra l'indagine in corso e la persona la cui utenza sia sottoposta a captazione occulta, così che si possa accertare l'adeguatezza del provvedimento ad assolvere alla funzione di garanzia di cui alla riserva di giurisdizione assoluta ex-art. 15, c.2 Cost.[218].

3. *Le intercettazioni cd. ambientali*

3.1. La disciplina generale

Il codice Vassalli del 1989 prevedeva sin dal principio una seconda ipotesi di intercettazione, che si affiancava a quella telefonica. Il comma 2 dell'art. 266 c.p.p., infatti, disponeva che negli stessi casi in cui si potesse effettuare un'intercettazione del tipo di cui al comma 1, fosse possibile richiedere l'autorizzazione a esperire un'intercettazione di una comunicazione tra presenti. Si tratta, cioè, di operazioni che non richiedono di catturare un flusso comunicativo fra strumenti tecnologici o digitali, ma vengono effettuate per mezzo del collocamento di dispositivi di registrazione e trasmissione fissi in un determinato luogo, in grado di far pervenire all'autorità investigativa il contenuto delle conversazioni che in quel tal luogo si tengano fra coloro che sono presenti in un dato momento. Per questa ragione, tradizionalmente l'intercettazione tra presenti è nota altresì come intercettazione cd. ambientale[219].

---

[217] Cass. pen., Sez. I, sent. n. 37212/2014, 5 settembre 2014.
[218] Cass. pen., Sez. V, sent. n. 1407/2017, 12 gennaio 2017.
[219] Es. P. Tonini, *Manuale di procedura penale*, XX ed., Milano, Giuffrè, 2020, 391.

La stessa disposizione, tuttavia, al periodo successivo sanciva come questo tipo di operazione non potesse essere esperita indiscriminatamente, poiché per quanto concerne i luoghi di domicilio (da intendersi nell'accezione penalistica dell'art. 614 c.p.), dovevano sussistere fondati motivi di ritenere che vi si stesse svolgendo attività criminosa. Diversamente, l'insussistenza di tali requisiti si traduceva in un divieto di poter procedere all'intercettazione delle comunicazioni che in tale ambiente avessero luogo (v. *infra*, §3.2).

Con riferimento a questa ipotesi, ancor più che nel caso delle intercettazioni telefoniche, lo sviluppo della disciplina è avvenuto per via pretoria. La giurisprudenza di legittimità ha ricostruito come, data la finalità del mezzo di ricerca della prova sia quella di captare scambi comunicativi fra i presenti, non si potrebbe utilizzare a fini di prova, o ulteriori e diversi, qualsiasi altra condotta o gesto captato (es. tramite una registrazione audiovisiva) a contenuto non comunicativo[220]. Inoltre, rientrerebbe nella disciplina in esame anche il caso della registrazione da parte di uno dei soggetti del rapporto comunicativo, laddove la polizia giudiziaria sia in grado di ascoltare la registrazione in tempo reale[221].

Interessante è altresì la distinzione che la giurisprudenza ha ritenuto di rinvenire fra intercettazioni telefoniche o telematiche, che si servono necessariamente di una strumentazione tecnica (es. utenza telefonica) i cui dettagli devono essere specificati nello specifico nel decreto di autorizzazione, e intercettazioni tra presenti, per le quali tale dipendenza dallo strumento tecnologico non sussiste e, pertanto, la variazione del mezzo specifico attraverso il quale l'operazione di intercettazione viene posta in essere non è rilevante fintanto che la natura dell'ambiente per il quale sia stata disposta la captazione sia analoga a quella in cui essa sia effettivamente esperita (es. un'automobile anziché un'altra, nella disponibilità di un medesimo soggetto)[222]. L'indicazione dell'ambiente dove si tenga la conversazione captata è necessaria parte integrante della motivazione solo se si tratti di luogo tutelato ai sensi dell'art. 614 c.p.,

[220] Cass. pen., Sez. VI, sent. n. 4397/1998, 21 gennaio 1998.
[221] Cass. pen., Sez. I, sent. n. 3458/1999, 17 marzo 1999.
[222] Cass. pen., Sez. I, sent. n. 4561/1999, 27 luglio 1999; analogamente, Cass. pen., Sez. V, sent. n. 5956/2012, 15 febbraio 2012.

non essendo diversamente tale indicazione prescritta dalla legge[223]. Né il dettato normativo impone alcun obbligo di indicare in motivazione chi sia deputato a intervenire nella fase di esecuzione dell'operazione, poiché le uniche informazioni necessarie ai fini della legittimità del decreto sono modalità e durata delle operazioni[224].

Anche con riguardo alle intercettazioni ambientali, la questione dell'utilizzo di strutture diversi dagli impianti installati presso gli uffici del pubblico ministero è stata oggetto di un certo numero di pronunce, che hanno tendenzialmente assunto un'interpretazione meno rigorosa del requisito del codice di rito, anche in ragione della natura specifica dell'intercettazione fra presenti. In particolare, tale ricorso a impianti in uso alla polizia giudiziaria è non solo qualificato come legittimo, ma addirittura funzionale a sopperire alle difficoltà tecniche che nascerebbero dall'applicazione a un genere diverso di captazione di disposizioni originariamente costruite per calzare alla fattispecie delle intercettazioni telefoniche[225].

Ciononostante, tale deroga alla regola generale dettata in tema di captazione occulta di comunicazione deve essere oggetto di specifica motivazione da parte del pubblico ministero[226]. Se dal provvedimento emergono chiaramente le ragioni per cui l'utilizzo delle strutture in dotazione alla Procura della Repubblica non assicura l'efficace esperimento dell'operazione, non è necessario argomentare il merito all'opportunità di ricorrere a impianti esterni[227], ben potendo utilizzare microspie data la particolare natura, rispetto al *genus* dell'intercettazione delle comunicazioni per via telefonica, dell'intercettazione ambientale, la quale richiede di portare le strumentazioni vicino a coloro che comunicano[228].

Peraltro, l'utilizzo delle microspie è da ritenersi lecito anche nei luoghi di privata dimora a norma delle disposizioni del codice, le quali riflettono il bilanciamento di interessi a opera del legislatore che, nell'esercizio della sua

---

[223] Cass. pen., Sez. I, sent. n. 3541/1999, 2 dicembre 1999.
[224] Cass. pen., Sez. IV, sent. n. 40790/2002, 4 dicembre 2002.
[225] Cass. pen., Sez. I, sent. n. 9370/1994, 31 agosto 1994; Cass. pen., Sez. VI, sent. n. 5156/1998, 21 gennaio 1998.
[226] Cass. pen., Sez. I, sent. n. 5239/1999, 4 novembre 1999; Cass. pen., Sez. I, sent. n. 3732/2000, 26 giugno 2000.
[227] Cass. pen., Sez. II, sent. n. 8025/2004, 24 febbraio 2004.
[228] Cass. pen., Sez. I, sent. n. 7671/2001, 23 febbraio 2001.

discrezionalità, detta i limiti ai diritti sanciti agli artt. 14 e 15 Cost. al fine di garantire un'adeguata tutela dell'interesse pubblico alla sicurezza e alla persecuzione delle condotte di reato[229]. Nei casi di urgenza, è stato altresì riconosciuto come legittimo il ricorso a strumenti tecnici di privati, a patto che l'operazione sia condotta sotto il diretto controllo della polizia giudiziaria[230].

La giurisprudenza si è infine preoccupata anche di fornire linee interpretative in tema di proroga dei decreti che autorizzano l'esperimento di intercettazioni tra presenti. In particolare, al decreto del GIP che disponga la proroga non è necessario che segua un nuovo provvedimento del PM che dia conto delle ragioni sottostanti al ricorso a strumentazioni esterne a quelle della Procura della Repubblica. Inoltre, quanto dettato in tema di motivazione *per relationem* con riferimento alle intercettazioni telefoniche va considerato applicabile anche alle intercettazioni tra presenti[231].

3.2. L'intercettazione domiciliare

Accanto all'intercettazione ambientale disciplinata come illustrato sopra, il legislatore si era preoccupato di prevedere altresì un'ipotesi di intercettazione di conversazioni tra presenti che si svolgesse in uno dei luoghi che sono tutelati dalla sanzione penale avverso l'intrusione non autorizzata (art. 614 c.p.). In questi casi, la captazione di comunicazioni sarebbe potuta avvenire soltanto in presenza di fondati motivi che facessero ritenere che in quei luoghi si stesse consumando una condotta di reato.

Anche su questa fattispecie eccezionale la giurisprudenza di legittimità si è pronunciata in più occasioni, tentando di esercitare dosi di equilibrio e bilanciando fra le esigenze di persecuzione dei reati e quelle di tutela dello spazio domiciliare. In particolare, tale ambito è stato interpretato come quello riservato allo svolgimento di attività libere e legittime di ciascuno senza l'interferenza di terzi (ivi compresi locali delle attività commerciali), al cui esclusivo godimento si possono prevedere limitazioni a norma di quanto previsto dall'art. 15 per la libertà e segretezza delle

[229] Cass. pen., Sez. VI, sent. n. 4397/1998, 21 gennaio 1998.
[230] Cass. pen., Sez. II, sent. n. 1595/2006, 16 gennaio 2006.
[231] Cass. pen., SS.UU., sent. n. 42792/2001, 28 novembre 2001.

comunicazioni[232]. Tuttavia, tale natura non è stata ritenuta propria di altri spazi non atti, secondo la Suprema Corte, a configurarsi come luoghi di privata dimora, quali ad esempio l'abitacolo dell'autovettura di cui disponga un soggetto[233] oppure luoghi che, per quanto utilizzati per fini di comunicazione personale, sono pertinenze di luoghi pubblici (quali la sala colloqui di un istituto di reclusione)[234].

Per quanto riguarda la fondatezza dei motivi che possano far ritenere che in un luogo di privata dimora si stia svolgendo un'attività criminosa, che è alla base della richiesta di procedere all'intercettazione domiciliare, è stato affermato che non è necessario l'accertamento che la condotta si stia effettivamente compiendo in quei luoghi, ben potendo bastare un esito ragionevolmente favorevole del giudizio prognostico formulato in sede di autorizzazione dell'operazione[235]. Sull'utilizzo di adeguata strumentazione tecnica che consenta un efficace esperimento dell'operazione, quale l'installazione di microspie presso un luogo di privata dimora, si rinvia a quanto detto *supra*.

Sul quadro normativo delineato dal Codice del 1988 si è ben presto innestata un'ipotesi speciale che deroga alla disciplina generale in materia di intercettazioni tra presenti. Difatti, per far fronte all'offensiva della criminalità organizzata nei confronti dello Stato, pochi anni dopo l'entrata in vigore del nuovo codice di rito fu inserito un nuovo periodo all'art. 13 del d.l. 152/1991, che originariamente richiedeva la sussistenza di soli sufficienti indizi di reato per poter disporre un'operazione di intercettazione (ipotesi limitata ai reati di criminalità organizzata e di minaccia con l'uso del telefono in sede di conversione, v. *supra*). La novità introdotta consistette in un regime speciale per i reati associativi, che permetteva, in presenza di sufficienti indizi di reato, di procedere alle intercettazioni ambientali anche in luoghi che ricadessero entro il perimetro di cui all'art. 614 c.p. senza che vi dovesse essere ragione

[232] Cass. pen., Sez. I, sent. n. 4141/1992, 2 dicembre 1992.
[233] Cass. pen., Sez. I, sent. n. 1904/1996, 17 febbraio 1996; Cass. pen., Sez. II, sent. n. 1831/1998, 10 giugno 1998.
[234] Cass. pen., Sez. I, sent. n. 3901/1997, 28 aprile 1997.
[235] Cass. pen., Sez. I, sent. n. 1367/1995, 10 febbraio 1995.

di pensare che in quei luoghi si stesse consumando l'attività di natura penalmente rilevante[236].

4. *Le intercettazioni telematiche*

In ragione della rivoluzione tecnologica montante e della crescente diffusione di personal computer per una serie di attività professionali e lavorative, ma non solo, il legislatore pochi anni dopo l'entrata in vigore del nuovo codice ha voluto fornire le autorità investigative di un nuovo mezzo di ricerca della prova, introducendo una disposizione ulteriore (art. 266-bis c.p.p.) e correlativamente coordinando la disciplina del codice in materia (modifica art. 268 c.p.p.)[237]. In particolare, nelle fattispecie previste dall'art. 266 c.p.p. e con riferimento ai reati commessi tramite sistemi informatici o telematici viene consentito altresì l'esperimento di intercettazioni di comunicazioni o flussi telematici o informatici, eventualmente servendosi di impianti appartenenti a privati.

Uno dei temi che più ha impegnato l'interprete è stato quello della definizione del concetto di sistema informatico o telematico ai fini della disposizione di cui sopra. In particolare, è stato riconosciuto come un esempio del primo caso qualsiasi complesso di apparecchiature che svolgono funzioni attraverso le tecnologie informatiche, caratterizzate da registrazione e memorizzazione, per mezzo di impulsi elettronici, di dati su supporti e dall'elaborazione degli stessi sotto forma di informazioni[238].

Sulla scorta di tale definizione e dell'evoluzione dei metodi di comunicazione anche telefonica, è stato sostenuto dalla giurisprudenza di legittimità che al giorno d'oggi quasi tutte le comunicazioni fra persone non presenti sarebbero sussumibili sotto la categoria generale di comunicazioni telematiche[239] e, pertanto, ad esse si applicherebbe la disciplina dell'art. 266-bis c.p.p. Non è del tutto chiaro, peraltro, se

---

[236] Legge 7 agosto 1992, n. 356. L'allegato dispone l'inserimento di un art. 3-bis al decreto-legge 8 giugno 1992, n. 306, che modifica appunto l'art. 13, c.1 d.l. 152/1991 (come modificato dalla l. 203/1991).
[237] Artt. 11-12, l. 23 dicembre 1993, n. 547.
[238] Cass. pen., Sez. VI, sent. n. 3067/1999, 14 dicembre 1999; Cass. pen., Sez. V, sent. n. 31135/2007, 6 luglio 2007.
[239] Cass. pen., SS.UU., sent. n. 36359/2008, 26 giugno 2008.

l'ipotesi che consente di sottoporre a intercettazione telefonica meramente sulla base di sufficienti indizi di reato coloro che siano sospettati di porre in essere una condotta associativa finalizzata a scopi criminali possa essere estesa analogicamente anche alle intercettazioni telematiche e informatiche[240].

Peraltro, una delle questioni controverse relative all'art. 266-bis c.p.p. riguarda l'estensione particolarmente ampia del suo ambito di applicazione. Infatti, se il ricorso all'intercettazione tradizionale ex-art. 266 c.p.p. rimane confinata a quelle fattispecie di reato che superano una certa soglia di offensività, si è visto che così non è per l'intercettazione telematica, che può essere disposta per qualsivoglia reato a patto che sia stato commesso per mezzo di un sistema informatico. In questo modo, viene spostata l'attenzione dalla natura del reato allo strumento utilizzato per porre in essere la condotta, in un certo senso discriminando sotto il profilo dell'equità processuale fra i reati comuni e quelli commessi con l'ausilio di infrastrutture informatiche[241].

L'intercettazione di flussi di informazioni fra sistemi informatici può avvenire secondo due modalità principali, che consistono nell'utilizzo di un captatore informatico, vale a dire un *software* che viene inoculato nel dispositivo di una delle parti del rapporto comunicativo a sua insaputa, o nella tecnica del reindirizzamento. Rinviando al Cap. IV per la trattazione in dettaglio del funzionamento dei cd. *software* spia e dei tentativi legislativi e giurisprudenziali di ricondurne l'utilizzo sotto il dettato costituzionale, è opportuno tratteggiare sinteticamente l'altra categoria di intercettazioni telematiche.

Il reindirizzamento si caratterizza per la trasmissione dei contenuti della comunicazione all'autorità inquirente prima che essi pervengano al destinatario. Nel caso delle comunicazioni telematiche tramite la rete Internet, che sono in buona sostanza immediate, ciò implica che nel brevissimo lasso di tempo che intercorre fra l'invio della comunicazione da parte del mittente e la ricezione da parte del

---

[240] A. Bonomo, *I nuovi strumenti di comunicazione telematica ed informatica: aspetti tecnici e questioni giuridiche*, in *Le investigazioni con l'impiego di intercettazioni di comunicazioni e di flussi informatici o telematici*, Gruppo di studio del 6 luglio 2011 ore 15,00, Incontro di studi sul tema: *Tecniche di indagine e rapporti tra p.m., polizia giudiziaria, consulenti tecnici e difensori*, Roma, 4-8 luglio 2011, Consiglio Superiore della Magistratura.

[241] S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, Giappichelli, 2018, 233 ss.

destinatario, che si sostanzia nel passaggio del messaggio sul server del *provider* del servizio di comunicazione, avvenga la trasmissione a chi abbia disposto la misura investigativa.

Questo aspetto della simultaneità e della precedenza della trasmissione all'autorità che conduce le indagini rispetto alla ricezione al destinatario è cruciale affinché di intercettazione si possa parlare, diversamente ricadendo nell'alveo di differenti mezzi di ricerca della prova. Inoltre, si segnala che questo strumento investigativo si applica non soltanto a qualsiasi scambio comunicativo che non avvenga in forma orale e simultanea (vale a dire anche ai messaggi audio registrati), bensì anche alle conversazioni orali che utilizzino quale infrastruttura di supporto la rete Internet, quindi anche le cd. 'chiamate vocali' effettuate tramite applicazioni installate sui dispositivi informatici[242].

Per quanto invece concerne il captatore informatico, si segnala in questo passaggio soltanto come la giurisprudenza di legittimità, a seguito delle precisazioni sui limiti di utilizzo dello stesso ai fini delle intercettazioni tra presenti nei luoghi di privata dimora effettuate per mezzo di un dispositivo portatile (v. sentenza Scurato *infra*, Cap. IV, §4.3), ha sancito altresì la legittimità delle intercettazioni di comunicazioni informatiche o telematiche ex-art. 266-bis c.p.p. che siano esperite per mezzo dell'inoculazione di un captatore informatico su un sistema informatico fisso che sia collocato in un luogo di privata dimora[243].

[242] *Ibid.*, 249 ss.
[243] Cass. pen., Sez. V, sent. n. 48370/2017, 20 ottobre 2017.

III. La segretezza delle comunicazioni e della corrispondenza sul piano internazionale e comparato

Sommario: 1. Profili di tutela nel diritto internazionale e sovranazionale. - 1.1. Il segreto delle comunicazioni nelle Carte dei diritti del II dopoguerra. - 1.2. Le garanzie nel sistema del Consiglio d'Europa. - 1.3. L'armonizzazione delle fonti dell'Unione Europea. - 2. La disciplina nell'ordinamento tedesco. - 2.1. La tutela costituzionale nelle Carte di epoca liberale. - 2.2. Il laboratorio di Weimar. - 2.3. Aspettando la Costituzione federale … – 2.4. La disciplina costituzionale nella Grundgesetz. *– 2.5. Le limitazioni ordinarie contenute nel codice di procedura penale - 2.6. La disciplina della G 10 - 3. L'esperienza statunitense. - 3.1. La tutela delle comunicazioni private prima del* bill of rights. *- 3.2. L'interpretazione originaria del IV Emendamento. - 3.3. Le prime avvisaglie di un'evoluzione dell'interpretazione del IV Emendamento - 3.4. La tutela del segreto delle comunicazioni telefoniche come paradigma del conflitto fra le diverse concezioni di privacy. - 3.5. La prima regolazione del* wiretapping *negli USA: il* Federal Communications Act *(1934). - 3.6. Il dado è tratto: l'avvento della* reasonable expectation of privacy *e i suoi limiti - 3.7. Il quadro normativo dopo* Katz.

1. Profili di tutela nel diritto internazionale e sovranazionale

1.1. Il segreto delle comunicazioni nelle Carte dei diritti del II dopoguerra

Se la tutela della segretezza delle comunicazioni fra privati avverso l'interferenza dei pubblici poteri non è stata oggetto di particolare regolazione da parte delle Carte liberali ottriate d'epoca liberale (v. *supra*, Cap. I), lo stesso non si può dire con riferimento ai testi costituzionali approvati nel secondo dopoguerra, a partire dalla Costituzione repubblicana italiana del 1948, della quale si è già detto *supra*, e dalla Legge Fondamentale della Repubblica federale tedesca del 1949 (su cui v. *infra*, §2.4). Una tale attenzione a questo interesse individuale si può d'altronde ravvisare anche nei documenti approvati in sedi sovranazionali nella seconda metà del cd. "Secolo breve"[244]. Peraltro, le disposizioni in essi contenute tendono nel corso del tempo ad assumere un aspetto standard e conformarsi a una formulazione comune, che si struttura secondo un generale riconoscimento della prerogativa in parola in capo a

[244] Così è stato tradotto il titolo dell'iconica opera di E. Hobsbawm, *Age of Extremes. The Short Twentieth Century 1914-1991*, Londra, Michael Joseph, 1994 (trad. it. a cura di B. Lotti, Milano, BUR, 1994).

ciascun individuo, al quale fa seguito una specificazione del diritto a ottenere forme di tutela sotto il profilo giuridico contro quelle attività che minaccino il godimento di tale posizione giuridica soggettiva.

Il suddetto approccio si rintraccia già all'art. 12 della *Dichiarazione Universale dei Diritti dell'Uomo* approvata dall'Assemblea Generale della neonata Organizzazione delle Nazioni Unite nel dicembre 1948[245]. La disposizione recita infatti che "*Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni*"[246]. Un altro esempio di tale attenzione alla tutela del segreto delle comunicazioni è senz'altro costituito dal riconoscimento esplicito dato al diritto al rispetto della [riservatezza della] corrispondenza nell'art. 8 della *Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà Fondamentali*[247]. La disposizione, come interpretata dalla Corte di Strasburgo, costituisce un riferimento assai significativo per il continente europeo ed è suscettibile di incidere in maniera penetrante sulla disciplina della materia negli ordinamenti delle parti contraenti, pur con le dovute differenze determinate dal grado di apertura di ciascuno alla penetrazione del diritto internazionale (v. *infra*, §1.2).

Diversamente, un approccio da un lato più sintetico e limitato alla proclamazione del principio generale, dall'altro più particolaristico poiché al diritto in oggetto aveva dedicato una disposizione apposita, caratterizza la *Dichiarazione Americana dei Diritti e Doveri dell'Uomo*, la quale all'art. X sancisce che "*ciascuna persona ha diritto all'inviolabilità e alla [libertà di] trasmissione della propria corrispondenza*"[248]. Peraltro, una formulazione in parte differente da quelle dei testi coevi e anche di quelli

---

[245] Risoluzione 217/A, 183esima adunanza plenaria, 10 dicembre 1948.

[246] La traduzione in italiano è tratta dal sito Internet istituzionale dell'Ufficio per l'Alto Commissariato per i Diritti Umani delle Nazioni Unite, disponibile all'url: https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/itn.pdf (ultimo accesso 3 gennaio 2021). Il testo della disposizione nella versione ufficiale in lingua inglese recita "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks*".

[247] Firmata a Roma il 4 novembre 1950.

[248] La Dichiarazione è stata adottata dalla Nona Conferenza degli Stati Americani riunitasi a Bogotá fra il 30 marzo e il 4 maggio 1948 (sede in cui nacque anche l'Organizzazione degli Stati Americani). Il testo originale della disposizione recita "*Every person has the right to the inviolability and transmission of his correspondence*".

successivi non dovrebbe sorprendere del tutto, poiché la cd. *Dichiarazione di Bogotá* è stato invero cronologicamente la prima Carta dei diritti umani approvata sul piano internazionale dopo la conclusione del secondo conflitto mondiale, precedendo di qualche mese quella approvata dall'ONU.

Sulla scorta della formulazione delle disposizioni nella Dichiarazione Universale delle Nazioni Unite del 1948 e nella Convenzione EDU del 1950, anche le proclamazioni dei diritti dei decenni successivi hanno contemplato una tutela di questa prerogativa articolata su due livelli, quello del riconoscimento in astratto del diritto e quello della sua garanzia in concreto. È questo il caso dell'art. 17 del *Patto Internazionale sui Diritti Civili e Politici*, a norma del quale "*Nessuno può essere sottoposto ad interferenze arbitrarie o illegittime nella sua vita privata, nella sua famiglia, nella sua casa o nella sua corrispondenza, né a illegittime offese al suo onore e alla sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze od offese*"[249]. Sulla stessa scia si pone altresì la *Convenzione Americana sui Diritti dell'Uomo*[250], in ciò evolvendo dalla limitata attenzione riservata a tale prerogativa dalla *Dichiarazione di Bogotà* e finendo, nei fatti, per sovrapporsi in termini di formulazione alle disposizioni contenute in altre Carte adottate negli ultimi decenni, quali quelle contemplate nell'ambito della *Carta araba sui diritti dell'uomo*[251] e della *Dichiarazione ASEAN sui diritti*

---

[249] L'ICCPR è stato adottato dall'Assemblea Generale delle Nazioni Unite con Risoluzione 2200/A (XXI) del 16 dicembre 1966. Il testo originale della disposizione recita "*No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks*".
La traduzione in italiano è tratta dal sito Internet del Centro per i Diritti Umani "Antonio Papisca" dell'Università degli studi di Padova, accessibile all'url:
https://unipd-centrodirittiumani.it/it/strumenti_internazionali/Patto-internazionale-sui-diritti-civili-e-politici-1966/15 (ultimo accesso 3 gennaio 2021).

[250] La Convenzione è stata adottata il 22 Novembre 1969 dalla Conferenza Inter-Americana Speciale sui Diritti dell'Uomo presso la sede della Commissione Inter-Americana per i Diritti dell'Uomo di San José. L'art. 11 (*Right to Privacy*) recita "*Everyone has the right to have his honor respected and his dignity recognized. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation. Everyone has the right to the protection of the law against such interference or attacks*".

[251] L'*Arab Charter on Human Rights* è stata adottata il 22 maggio 2004 durante il sedicesimo summit ordinario della Lega Araba tenutosi a Tunisi. L'art. 21 dispone che "*No one shall be subjected to arbitrary or unlawful interference with regard to his privacy, family, home or correspondence, nor to unlawful attacks on his honour or his reputation. Everyone has the right to the protection of the law against such interference or attacks*". Peraltro, in una precedente versione della Carta (approvata nel 1994 ma 'congelata' fino all'adozione della versione del 2004) la formulazione della disposizione riconduceva esplicitamente la tutela della segretezza della corrispondenza sotto la categoria generale della vita privata, qualificata come consacrata (art. 17: "*Private life is sacred, and violation of that sanctity is a crime. Private life includes*

dell'uomo[252]. Diversamente, sono assenti del tutto riferimenti a questo proposito nel documento più rilevante in tema di protezione dei diritti umani nel continente africano, vale a dire la *Carta africana sui diritti dell'uomo e dei popoli*[253].

Una formulazione sintetica, che riproduce per intero il primo comma dell'art. 8 della Convenzione EDU, omettendo però la previsione della tutela concreta avverso l'interferenza pubblica nel godimento del diritto, è contenuta nell'art. 7 della *Carta dei diritti fondamentali dell'Unione Europea*[254], sul cui contenuto v. più diffusamente *infra*, §1.3.

Al di fuori delle Carte dei diritti caratterizzate da ambito di applicazione regionale, è d'uopo fare altresì riferimento a un trattato internazionale sulla materia che, per quanto formalmente promosso dal Consiglio d'Europa, è aperto alla firma anche di Stati extra-europei. La *Convenzione sulla criminalità informatica*, che raccoglie 65 adesioni su scala globale, prevede infatti all'art. 21 che ciascuna parte contraente faccia in modo di fornire alle competenti autorità nazionali gli strumenti giuridici per raccogliere, registrare od obbligare un fornitore di servizi di rete a cooperare alla raccolta del contenuto di comunicazioni che si svolgano per mezzo di sistemi informatici, con riferimento a gravi fattispecie di reato che siano determinate per legge dallo Stato. In particolare, le operazioni in questione non interferiscono con la trasmissione delle comunicazioni e, quindi, con la ricezione del messaggio da parte del destinatario, ma sacrificano la segretezza riposta dalle parti del rapporto comunicativo nel mezzo utilizzato, consentendo di ottenere copia tanto dei dati 'esteriori' della comunicazione quanto del suo contenuto.

La differenza fra le due operazioni risiede proprio nel più intenso interesse alla riservatezza che, in molti ordinamenti, è riconosciuto al contenuto delle comunicazioni

---

family privacy, the sanctity of the home, and the secrecy of correspondence and other forms of private communication").

[252] L'*ASEAN Human Rights Declaration* è stata adottata il 18 novembre 2012 in occasione del ventunesimo summit ASEAN tenutosi a Phnom Penh. A norma dell'art. 21 "*every person has the right to be free from arbitrary interference with his or her privacy, family, home or correspondence including personal data, or to attacks upon that person's honour and reputation. Every person has the right to the protection of the law against such interference or attacks*".

[253] La cd. *Carta di Banjul* (*African Charter on Human and Peoples' Rights*) è stata adottata il 27 giugno 1981 in occasione della diciottesima assemblea dei Capi di Stato e di Governo dell'*Organization of the African Unity* tenutasi a Nairobi.

[254] Proclamata a Nizza il 7 dicembre 2000.

rispetto ai meri dati esteriori delle medesime, tanto che la stessa convenzione riconosce, in linea di principio, un'applicabilità a qualsiasi presunta condotta di reato della disposizione sulla raccolta in tempo reale di dati delle comunicazioni (art. 20), mentre limita l'intercettazione del contenuto ai reati che, nella valutazione discrezionale del legislatore di ciascuna parte contraente, superino una certa soglia di gravità, eccedendo cioè un limite prestabilito nel massimo di pena[255].

1.2. Le garanzie nel sistema del Consiglio d'Europa

Come anticipato nel paragrafo precedente, ai fini dell'analisi dei confini del diritto alla segretezza del contenuto delle comunicazioni nel continente europeo non si può prescindere da un riferimento al quadro regolatorio predisposto nell'ambito del Consiglio d'Europa dal testo della Convenzione EDU come interpretato dalla giurisprudenza della Corte di stanza a Strasburgo. L'art. 8 della Convenzione (rubricato "Diritto al rispetto della vita privata e familiare"), infatti, recita che "*Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui*"[256].

Come già fatto notare, la struttura della disposizione si articola in un primo generale riconoscimento di principio della prerogativa in oggetto, al quale segue il divieto di interferenza da parte dei pubblici poteri se non nel rispetto del requisito

---

[255] Explanatory Report to the Convention on Cybercrime, Budapest, 23.XI.2001, Title V, §§ 205-231, disponibile all'url: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b (ultimo accesso: 23 gennaio 2021).

[256] La traduzione in lingua italiana è consultabile al seguente url: https://www.echr.coe.int/documents/convention_ita.pdf (ultimo accesso: 23 gennaio 2021). Il testo originale della disposizione in lingua inglese recita "*Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*".

della riserva di legge e in osservanza di un criterio di necessità oggettiva, pur nella cornice di una società democratica. Si noti altresì come la tutela della corrispondenza sia in questa sede strettamente associata a quella della vita privata e familiare e del domicilio, sì da creare quasi un unico fascio di diritti che fruisce del medesimo meccanismo di protezione. È interessante notare come la disposizione sia stata letta non solo nel senso di far sorgere una libertà negativa in capo ai cittadini degli Stati contraenti, bensì anche come orientata a esigere dagli stessi poteri pubblici prestazioni positive consistenti nella predisposizione di meccanismi che garantiscano la tutela degli interessi in parola anche avverso l'ingerenza degli altri privati cittadini[257].

Il requisito di previsione della forma di interferenza in una fonte legislativa della Parte contraente non è soddisfatto dal solo e mero rispetto delle disposizioni di diritto domestico, poiché lo stesso quadro regolatorio nazionale deve essere sufficientemente chiaro, accessibile e prevedibile in termini di chi possa essere destinatario delle misure previste[258]. Inoltre, il riferimento alla legge andrebbe opportunamente inteso non come soltanto circoscritto agli atti normativi statali, bensì in un'ottica sostanziale che includa altresì eventuali regole sviluppate dalla giurisprudenza domestica in via di prassi, se sufficientemente conosciute e prevedibili dai destinatari della misura in questione[259].

Lo scrutinio dei giudici di Strasburgo sul perseguimento di uno dei fini contemplati dalla disposizione non si è dimostrato particolarmente rigoroso, pur gravando sullo Stato convenuto in giudizio l'onore di giustificare l'interferenza premurandosi di indicare il perseguimento di un fine legittimo[260]. Ben più penetrante appare invece la verifica del requisito della necessità in una società democratica, che è

---

[257] *Bărbulescu c. Romania*, no. 61496/08, Corte EDU, Grande Camera, 5 settembre 2017. Si veda anche *Craxi c. Italia (No. 2)*, no. 25337/94, Corte EDU, I Sez., 17 luglio 2003, ove la Corte ha dichiarato la violazione dell'art. 8 Conv. EDU da parte dell'Italia per non avere tutelato in maniera efficace la sfera della vita privata di un soggetto sottoposto a procedimento penale in ragione della pubblicazione da parte di mezzi di informazione privati di stralci di conversazioni dello stesso non attinenti ai procedimenti in corso. A questo proposito v. altresì *Guide on Article 8 of the European Convention on Human Rights*, § I.B, disponibile all'url: https://www.echr.coe.int/documents/guide_art_8_eng.pdf (ultimo accesso: 23 gennaio 2021).

[258] *Lebois c. Bulgaria*, no. 67482/14, Corte EDU, V sez., 19 ottobre 2017; *Fernández Martínez c. Spagna*, no. 56030/07, Corte EDU, Grande Camera, 12 giugno 2014.

[259] C. Rossi, *Il rispetto della corrispondenza nella Convenzione europea dei diritti dell'uomo. Le intercettazioni nella legislazione italiana*, in *Riv. int. dir. uomo*, 1994, 64-71, in particolare 66.

[260] *Guide on Article 8 of the European Convention on Human Rights*, *cit.*, § I.D.

stato ritenuto soddisfatto laddove le ragioni che giustificassero l'intervento restrittivo fossero rilevanti e sufficienti e le misure adottate proporzionate ai fini perseguiti[261], con la precisazione che dovesse sussistere un bisogno sociale impellente di tale intervento da parte dello Stato[262].

Con specifico riferimento alla protezione del segreto della corrispondenza, il primo elemento da chiarire è l'ambito di applicazione della disposizione, che la Corte EDU ha ritenuto riguardare comunicazioni di natura personale o professionale[263], contenuto di plichi postali[264], conversazioni telefoniche con familiari e non[265], effettuate da luoghi privati o sede di attività commerciali[266], nonché da istituti di pena e da detenuti[267]; inoltre, le forme di comunicazione elettronica o digitale nonché su supporti esterni o periferiche sono stati considerati sussumibili sotto la definizione di corrispondenza[268]. Non è quindi rilevante il contenuto né la forma della corrispondenza affinché si ricada in un'ipotesi di interferenza ai sensi dell'art. 8[269], né è prevista una soglia di gravità della condotta ai fini della violazione del diritto in questione[270]. Se la forma di interferenza più grave è quella che impedisce del tutto il perfezionarsi della comunicazione[271], possono essere qualificati come tale anche un semplice screening della stessa[272], l'estrazione di copie[273], la cancellazione di determinati passaggi di un testo[274], l'utilizzo di strumenti di captazione telefonica[275] e la sottoposizione a misure di sorveglianza segreta[276]. Gli Stati contraenti godono in

---

[261] *Z. c. Finlandia*, no. 22009/93, Corte EDU, Camera, 25 febbraio 1997.
[262] *Piechowicz c. Polonia*, no. 20071/07, Corte EDU, IV sez., 17 aprile 2012.
[263] *Niemietz c. Germania*, no. 13710/88, Corte EDU, Camera, 16 dicembre 1992.
[264] *Silver c. Regno Unito*, no. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75, Corte EDU, Camera, 25 marzo 1983.
[265] *Margareta and Roger Andersson c. Svezia*, no. 12963/87, Corte EDU, Camera, 25 febbraio 1992; *Lüdi c. Svizzera*, no. 12433/86, Corte EDU, Camera, 15 giugno 1992.
[266] *Amann c. Svizzera*, no. 27798/95, Corte EDU, Grande Camera, 16 febbraio 2000.
[267] *Petrov c. Bulgaria*, no. 15197/02, Corte EDU, V sez., 22 maggio 2008; *X c. Regno Unito*, no. 7308/75, Commissione EDU, 12 ottobre 1978.
[268] *Copland c. Regno Unito*, no. 62617/00, Corte EDU, IV sez., 3 aprile 2007; *Petri Sallinen c. Finlandia*, no. 50882/99, Corte EDU, IV sez., 25 settembre 2005.
[269] *A. c. Francia*, no. 14838/89, Corte EDU, Camera, 23 novembre 1993.
[270] *Narinen c. Finlandia*, no. 45027/98, IV sez., 1 giugno 2004.
[271] *Golder c. Regno Unito*, no. 4451/70, Corte EDU, Camera, 21 febbraio 1975.
[272] *Campbell c. Regno Unito*, no. 13590/88, Corte EDU, Camera, 25 marzo 1992.
[273] *Foxley c. Regno Unito*, no. 33274/96, Corte EDU, III sez., 20 giugno 2000.
[274] *Pfeifer e Plankl c. Austria*, no. 10802/84, Corte EDU, Camera, 25 febbraio 1992.
[275] *Malone c. Regno Unito*, no. 8691/79, Corte EDU, Sez. plenaria, 2 agosto 1984.
[276] *Kennedy c. Regno Unito*, no. 26839/05, Corte EDU, IV sez., 18 maggio 2010.

ogni caso di un margine di apprezzamento in questo ambito, che tuttavia la Corte si riserva di valutare sotto il profilo del rispetto della Convenzione[277].

Nell'esercizio di tale scrutinio, la Corte EDU, in un caso riguardante il diverso tema del prelievo di impronte digitali e DNA da parte di un'autorità investigativa, ha preso una posizione netta, segnalando i rischi associati a un uso spregiudicato del progresso tecnologico in spregio al diritto sancito all'art. 8 della Convenzione. Infatti, la protezione riconosciuta dalla disposizione sarebbe indebolita in modo inequivocabile se l'uso delle moderne tecniche scientifiche nell'ambito dei procedimenti penali fosse ammesso a ogni costo e senza un previo cauto bilanciamento dei potenziali benefici di un utilizzo su larga scala, tale da incidere su interessi di riservatezza dei singoli. L'ampio consenso che unisce gli Stati aderenti al Consiglio d'Europa su questo tema ridurrebbe quindi il margine di apprezzamento di ciascun ordinamento nazionale e farebbe gravare particolari responsabilità su quei Paesi all'avanguardia che, utilizzando per primi queste tecniche, devono operare un equo bilanciamento di interessi[278].

Tralasciando in questa sede quanto statuito dai giudici di Strasburgo con riferimento alla prerogativa in oggetto per quanto concerne detenuti e legali rappresentanti, sembra opportuno soffermarsi invece sull'elaborazione giurisprudenziale della Corte in tema di sorveglianza delle telecomunicazioni in ambito di repressione dei fenomeni criminosi.

In questo ambito il requisito della riserva di legge è particolarmente stringente, poiché le disposizioni che regolino l'interferenza statale devono essere quanto più precise possibile[279], nonché chiare e prevedibili nella loro applicazione, così che ciascun potenziale destinatario possa valutare preventivamente le conseguenze sulla propria sfera di comunicazione privata[280]. Data la sottrazione delle decisioni su tali ambiti allo scrutinio dei singoli e della pubblica opinione, è necessario che la legge che autorizzi tali operazioni delimiti il perimetro della discrezionalità in capo all'autorità

[277] *Szuluk c. Regno Unito*, no. 36936/05 Corte EDU, IV sez., 2 giugno 2009.
[278] *S. e Marper c. Regno Unito*, no. 30562/04 e 30566/04, Corte EDU, Grande Camera, 4 dicembre 2008, §112.
[279] *Huvig c. Francia*, no. 11105/84, Corte EDU, Camera, 24 aprile 1990.
[280] *Valenzuela Contreras c. Spagna*, 58/1997/842/1048, 30 luglio 1998.

procedente[281], così da evitare esercizi arbitrari di tali poteri[282], ben dovendo dar conto delle ragioni cogenti che fondino il ricorso a strumenti tanto intrusivi[283].

La Corte di Strasburgo non ha lesinato indicazioni con riferimento allo scrutinio da effettuare sulle misure in questione, argomentando che debbano sussistere sufficienti e adeguate garanzie procedurali che tengano in considerazione tutti gli elementi del caso concreto (es. natura delle misure e degli interessi perseguiti, ambito di applicazione e durata delle misure, rimedi previsti dal diritto nazionale). Essa ha inoltre indicato come tale supervisione sia riferibile a tre distinti momenti: l'autorizzazione del dispiegamento degli strumenti di interferenza, l'operazione di interferenza stessa e il momento successivo a essa. In particolare nelle prime due fasi, che sono per definizione celate alla conoscenza del destinatario, devono sussistere salvaguardie procedurali che consentano un controllo sulla correttezza e legittimità delle attività dei pubblici poteri, che sono considerate effettivamente necessarie in una società democratica laddove finalizzate a preservarne le istituzioni e ad assicurare la sopravvivenza dell'ordinamento[284].

La giurisprudenza convenzionale si è pronunciata a più riprese sull'utilizzo di intercettazioni di conversazioni telefoniche, autorizzando il ricorso a esse nel contesto di attività di indagine penale se in osservanza della legge e necessarie in una società democratica per garantire la sicurezza pubblica e la prevenzione dei reati, precisando, tuttavia, l'obbligo degli Stati parte della Convenzione di assicurarsi che la messa in atto di tali misure non dia luogo ad abusi o condotte arbitrarie[285]. Con riferimento alla sorveglianza segreta da remoto, la Corte di Strasburgo ha riconosciuto che essa può essere necessaria per far fronte a sofisticate e complesse minacce che incombono sulle società democratiche contemporanee, ragion per cui sono tollerabili nella cornice della Convenzione misure legislative che accordino forme di sorveglianza sulla corrispondenza e le telecomunicazioni, seppur in circostanze straordinarie[286]. Il

---

[281] *Karabeyoğlu c. Turchia*, no. 30083/10, Corte EDU, II sez., 7 giugno 2016; *Roman Zakharov c. Russia,* no. 47143/06, Corte EDU, Grande Camera, 4 dicembre 2015.
[282] *Bykov c. Russia*, no. 4378/02, Corte EDU, Grande Camera, 10 marzo 2009.
[283] *Dragojević c. Croazia*, no. 68955/11, Corte EDU, I sez., 15 gennaio 2015.
[284] *Roman Zakharov c. Russia*, *cit.*
[285] *Dumitru Popescu c. Romania (No 2)*, no. 71525/01, Corte EDU, III sez., 26 aprile 2007.
[286] *Klass c. Germania*, no. 5029/71, Corte EDU, Grande Camera, 6 settembre 1978.

requisito della necessità, peraltro, è stato interpretato in senso particolarmente rigoroso, sì da essere limitato a una valutazione individuale caso per caso, che si risolva in un giudizio prognostico favorevole sull'ottenimento di informazioni vitali alla prevenzione di condotte di reato nel caso concreto[287].

È interessante notare come in questo ambito la giurisprudenza convenzionale abbia dimostrato una certa elasticità nell'interpretazione dei criteri di ammissibilità dei ricorsi, sottoponendo al vaglio sul merito altresì doglianze sollevate da soggetti che non ricadessero entro la definizione standard di 'vittima' (*rectius*, soggetto leso) ai fini dell'attivazione dello scrutinio della Corte. Infatti, data la straordinaria pervasività degli strumenti adoperati, è stato consentito l'accesso alla trattazione sul merito anche a casi laddove il ricorrente non fosse stato necessariamente inciso dalla misura in questione nella propria sfera personale, bastando a tal proposito che egli fosse suscettibile di applicazione della disciplina in parola o che appartenesse a una categoria alla quale essa fosse già stata applicata, in assenza di ulteriori rimedi a disposizione[288]. Tale approdo risponde all'esigenza di non accordare alcun 'porto franco' a condotte statali tanto pervasive, facendole soggiacere allo scrutinio sia delle giurisdizioni nazionali che dello stesso giudice di Strasburgo.

La Corte ha dettato con dovizia di particolari il contenuto obbligatorio di una fonte legislativa che disponga il dispiegamento di misure di sorveglianza occulta del tipo in parola. Essa deve indicare le fattispecie di reato e le persone suscettibili di intercettazione, contemplare un limite temporale alle operazioni, delineare una procedura da seguire per l'esame, utilizzo e la conservazione dei dati, prevedere cautele da adottare per la comunicazione dei dati a terze parti, nonché le circostanze nelle quali le registrazioni possano essere cancellate o distrutte[289].

La revisione e supervisione della messa in atto di tali attività può venire in rilievo, come già ricordato, in tre diverse fasi: nel momento in cui esse vengono disposte, in quello dello svolgimento o dopo che si siano concluse. Per evitare di prestare il fianco ad abusi, le prime due devono essere presidiate da garanzie adeguate quali l'istituzione di un controllo giurisdizionale, sì da preservarne l'indipendenza e

---

[287] *Szabó e Vissy c. Ungheria*, no. 37138/14, Corte EDU, IV sez., 12 gennaio 2016.
[288] *Roman Zakharov c. Russia*, *cit.*
[289] *Ibid.*

imparzialità. Per quanto concerne la fase successiva, le garanzie risiedono nella tempestiva notificazione al soggetto interessato, senza la quale esso molto difficilmente potrebbe agire in giudizio per tutelarsi avverso tali interferenze entro la propria sfera riservata[290].

La giurisprudenza della Corte EDU ha sottolineato altresì la rilevanza della previsione di tutele nei confronti di quei soggetti che siano oggetto di interferenza nelle comunicazioni 'fortuitamente', poiché entrano in contatto con le persone sottoposte a intercettazione per ragioni non connesse all'indagine[291]. Il giudice di Strasburgo ha inoltre ritenuto che sussista un certo margine di discrezionalità in capo alle autorità alle quali sia conferito il potere di autorizzazione delle operazioni di intercettazione, consistente nella determinazione in merito alla durata delle attività in parola, a patto che la legislazione nazionale contempli un termine di decadenza del mandato di autorizzazione e i requisiti per un rinnovo dello stesso, nonché le circostanze che ne importino la revoca[292].

Nonostante la preferibilità del conferimento del potere di supervisione a un'autorità giurisdizionale, per le ragioni illustrate *supra*, non è ragione di violazione della Convenzione l'attribuzione di tale funzione a istituzioni di diversa natura, sempre che sia garantita l'indipendenza da coloro che dispongono in concreto l'attività di intercettazione e che il soggetto incaricato della supervisione sia dotato di mezzi sufficienti per fornire un controllo efficace e continuativo[293]. Per ciò che invece concerne la notifica, non è ragione di illegittimità della disciplina nazionale la mancata previsione di un'immediata comunicazione al soggetto non appena l'attività cessi, ben potendo bastare una notificazione nel momento in cui essa non metta a repentaglio il perseguimento dello scopo al quale l'operazione miri[294].

Peraltro, non sarà sufficiente alla disciplina nazionale regolare nel dettaglio le fattispecie che legittimino l'esperimento di attività d'intercettazione e indicare le modalità concrete di attuazione delle stesse. Infatti, essa dovrà necessariamente

---

[290] *Ibid.*
[291] *Iordachi v. Moldavia*, no. 25198/02, Corte EDU, IV sez., 10 febbraio 2009; *Amann c. Svizzera*, no. 27798/95, Corte EDU, Grande Camera, 16 febbraio 2000.
[292] *Roman Zakharov c. Russia*, *cit.*; *Kennedy c. Regno Unito*, *cit.*; *Iordachi c. Moldavia*, *cit.*
[293] *Klass c. Germania*, *cit.*
[294] *Cevat Özel c. Turchia*, 19602/06, Corte EDU, II sez., 7 giugno 2016.

contemplare anche la previsione delle modalità effettive tramite le quali il soggetto, le cui conversazioni siano state oggetto di intercettazione, possa verificare la legittimità e la regolarità dell'autorizzazione e del compimento in concreto dell'attività[295].

In ragione delle forme assunte dalle consorterie criminali al giorno d'oggi, in specie quelle volte a commettere azioni terroristiche, la Corte di Strasburgo ha riconosciuto la legittimità del ricorso statale a forme di sorveglianza di massa a fini preventivi, pur sottolineando la necessità della previsione di adeguate garanzie procedurali ed efficaci rimedi per le lesioni ingiustificate. I giudici si sono persino spinti a consentire a una deroga all'autorizzazione giurisdizionale in casi di estrema urgenza, laddove l'ottenimento del mandato rischierebbe di far perdere tempo prezioso per poter evitare che si compia la condotta che si vuole prevenire. In quest'ultimo caso, il controllo di un giudice si sposterà da monte a valle dell'operazione, non potendo quest'ultima in ogni caso prescindere da una qualche forma di controllo in chiave giurisdizionale sulla sussistenza di legittimi presupposti[296].

In ogni caso, il tema del controllo esercitato sul ricorso a tali misure da parte di autorità indipendenti e la sottoposizione delle scelte in questione anche allo scrutinio della popolazione in una fase successiva è un precipitato di quel requisito della necessità delle limitazioni in una società democratica, che tale non potrebbe qualificarsi se questo controllo mancasse, cioè se queste attività fossero semplicemente ricondotte nell'alveo di attività di polizia sottratte al controllo sui requisiti da parte di un'apposita autorità e della pubblica opinione[297].

1.3. L'armonizzazione delle fonti dell'Unione Europea

Relativamente recente rispetto alle Carte dei diritti menzionate nel §1.1, la Carta dei diritti fondamentali dell'Unione Europea ha investito la Corte di Giustizia con sede a Lussemburgo della tutela di interessi ben più ampi di quelli originariamente previsti

[295] A. Bargi-S. Fùrfaro, *La prova per intercettazioni tra diritto interno e diritto sovranazionale*, in A. Gaito (a cura di), *Riservatezza ed intercettazioni tra norma e prassi*, *op. cit.*, 67.
[296] *Szabó e Vissy c. Ungheria*, *cit.*
[297] M. Griffo, *Il captatore informatico e la filosofia del doppio binario*, Napoli, ESI, 2019, 295-296.

nel Trattato di Roma e attinenti alla sfera delle libertà economiche. Tuttavia, la proclamazione della Carta prima[298] e la sua effettiva vincolatività poi[299] non marcano una discontinuità netta con la giurisprudenza comunitaria precedente, poiché già da decenni la stessa Corte di Giustizia aveva preso a considerare parametri di giudizio ulteriori – non contemplati nei Trattati – per decidere le controversie a essa devolute. La cd. Carta di Nizza costituisce dunque un tassello ulteriore di quel 'costituzionalismo multi-livello'[300] che si è affermato in Europa nella seconda metà del Novecento, offrendo a ciascun individuo più sedi presso le quali esigere la tutela dei propri diritti avverso le condotte dello Stato.

In particolare, l'art. 7 della Carta recita "*ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni*", adottando una formulazione essenziale e che riproduce quell'accostamento che si è ravvisato anche nella formulazione della disposizione della Convenzione EDU, che pure precede di mezzo secolo il documento comunitario. È interessante notare che, tuttavia, la Carta dei diritti fondamentali non si arresta a questo stadio, spingendosi a proclamare il diritto alla protezione dei dati personali (art. 8). Questa affermazione sembra sancire un diritto alla riservatezza e al controllo dei propri dati come delineato nel Cap. I e, in quei termini, distinto da quello alla segretezza della propria corrispondenza e delle comunicazioni. Peraltro, è opportuno notare come l'art. 8 della Carta non si limiti a una mera proclamazione, bensì riconosca esplicitamente agli interessati il diritto all'accesso e alla rettifica, subordinando il rispetto del quadro delineato al controllo di un'autorità indipendente.

Se la Corte di Giustizia non ha avuto modo di pronunciare decisioni di particolare rilevanza relative alla segretezza della corrispondenza, essa è stata tuttavia protagonista di una pronuncia senz'altro dirompente allorquando ha sanzionato la violazione degli artt. 7 e 8 della Carta da parte degli obblighi contenuti nella cd. Direttiva sulla *Data retention*[301]. In questo caso, infatti, la causa verteva sulle

---

[298] 7 dicembre 2000.

[299] Con l'entrata in vigore – nel 2009 – del Trattato di Lisbona siglato nel 2007.

[300] G.F. Ferrari, *Le libertà. Profili comparatistici*, *op. cit.*, 295 ss.

[301] Cause riunite C-293/12 e C-594/12, Corte di Giustizia dell'Unione Europea (Grande Camera), 8 aprile 2014, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources, Minister*

disposizioni dell'atto di diritto derivato UE che vincolavano gli Stati membri a predisporre misure legislative affinché i cd. metadati delle comunicazioni telefoniche e digitali (vale a dire quei dati che, pur senza dar conto del contenuto, identificano univocamente le parti del rapporto comunicativo e le circostanze di tempo della comunicazione) fossero conservati dai fornitori del servizio per un periodo di tempo fra sei mesi e due anni, così da poter essere trasmessi alle autorità statali su richiesta delle stesse laddove insorgesse la necessità di prenderne cognizione a fini di indagine penale per la persecuzione o prevenzione dei reati[302].

La Corte, interpellata tramite rinvio pregiudiziale di interpretazione, ha sancito che tali disposizioni violavano i principi di cui agli artt. 7 e 8 della Carta, poiché i dati la cui conservazione veniva imposti ricadevano nell'alveo dei dati personali di cui all'art. 8. Inoltre, il sistematico monitoraggio delle comunicazioni e la raccolta di tali dati poteva consentire di ricostruire in dettaglio la frequenza dei rapporti comunicativi di un individuo con determinati soggetti, con rilevante lesione della sfera di riservatezza della vita privata e familiare tutelata all'art. 7. Assunto il dato dell'interferenza delle misure in oggetto con i diritti fondamentali in questione, la Corte di Lussemburgo ha verificato la rispondenza delle suddette con il canone di proporzionalità che la stessa Carta impone per verificare la legittimità delle limitazioni ai diritti da essa proclamati (art. 52).

Pur riconoscendo che una tale ingerenza non arrecava un pregiudizio irrimediabile ai diritti in parola, che i fini perseguiti dal legislatore europeo erano legittimi e che le modalità attuative adottate erano idonee a conseguire lo scopo perseguito, il giudice ha sanzionato il difetto del requisito della stretta necessità della misura. Essa si risolveva in buona sostanza di una 'pesca a strascico', che raccoglieva i dati comunicativi di praticamente tutti i cittadini europei senza che vi fosse una previa distinzione fra quelli rilevanti ai fini di eventuali futuri accertamenti o indagini penali e quelli invece privi di alcuna utilità prospettica. L'assoluta generalità e la mancanza di qualsivoglia criterio di dettaglio sui dati da conservare e sui soggetti titolati all'accesso a quanto archiviato, nonché l'assenza della previsione di un controllo

for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlanda, The Attorney General e *Kärntner Landesregierung, M.S., C.T. e a.*, §§ 45 ss.

[302] V. anche M. Griffo, *op. cit.*, 299-300.

giurisdizionale su tali attività sono altri aspetti sulla base dei quali la Corte di Giustizia ha basato il proprio giudizio di illegittimità delle disposizioni della Direttiva.

La decisione della Corte di Giustizia sulla Direttiva *Data Retention*, coniugata con la constatazione della divergenza negli esiti concreti dell'attuazione dei contenuti della cd. Direttiva Privacy approvata a metà anni '90[303], hanno condotto negli anni più recenti le istituzioni europee a intervenire tramite la fonte più incisiva a propria disposizione, vale a dire un regolamento. Il Regolamento generale sulla protezione dei dati personali[304] qualifica infatti come fondamentale la protezione delle persone fisiche con riferimento al trattamento dei propri dati personali e ne riconduce la tutela agli artt. 8, §1 della Carta dei diritti fondamentali e all'art. 16, §1 del Trattato sul Funzionamento dell'Unione Europea. Peraltro, in sinergia con l'atto di cui sopra il legislatore europeo ha altresì adottato una direttiva coordinata che riguarda il trattamento dei dati da parte delle pubbliche autorità a fini di indagine penale[305].

Il quadro sinteticamente delineato mostra una decisa aspirazione alla convergenza delle discipline degli Stati membri dell'UE in materia di protezione dei dati personali, testimoniata dal recente ricorso allo strumento del regolamento, pur coadiuvata da direttive che riservano ai singoli ordinamenti una sfera di discrezionalità nella garanzia di quelle forme di tutela prescritte a livello comunitario. Tuttavia, non si può non sottolineare come l'attenzione sia in larga parte rivolta ai dati personali a livello generale, trascurando dunque il profilo delle comunicazioni, sia dal punto di vista dei dati esteriori delle stesse sia, ciò che più rileva ai fini della trattazione in oggetto, del contenuto delle medesime, che rimane perlopiù ignorato dal legislatore europeo e dunque rimane maggiormente influenzato dalla giurisprudenza della Corte EDU che non dal quadro giuridico dell'Unione Europea, pur avendo presente la

[303] 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.
[304] 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, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.
[305] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

compenetrazione che la prima ha nel secondo, specie a partire dal 2009 con l'entrata in vigore del Trattato di Lisbona.

2. *La disciplina nell'ordinamento tedesco*

2.1. La tutela costituzionale nelle Carte di epoca liberale

Analogamente a quanto fatto nel Cap. I con riferimento all'ordinamento italiano, si ritiene di dare conto, succintamente, dell'evoluzione diacronica della tutela costituzionale della libertà e segretezza della corrispondenza nel contesto tedesco, così da poter comprendere il quadro costituzionale andato delineandosi con la Legge fondamentale del 1949, sul quale sono intervenute le due pronunce del *BundesVerfassungsGericht* in tema di sorveglianza occulta delle comunicazioni telematiche, delle quali si dirà in dettaglio nel Cap. IV.

Il primo documento rilevante in questo senso risale all'età liberale: si tratta, infatti, della cd. Costituzione di Francoforte o Costituzione della *Paulskirche*[306]. Questo documento, seppur mai concretamente operativo poiché l'entrata in vigore fu paralizzata dal rifiuto del soggetto designato – il re di Prussia Federico Guglielmo IV – ad assumere la carica di Imperatore dei tedeschi, contiene un catalogo di diritti, approvato dall'Assemblea nazionale il 27 dicembre 1848, molto moderno per l'epoca e la cui eco si sente persino nelle Carte del II dopoguerra[307].

Con specifico riferimento alla prerogativa oggetto del presente studio, è interessante notare come nella Carta di Francoforte faccia la propria comparsa la categoria dell'inviolabilità, che viene tuttavia riservata alla libertà personale, al domicilio e alla proprietà (nonché, al di fuori del catalogo dei diritti, alla persona dell'Imperatore). La libertà e la segretezza della corrispondenza sono quindi 'escluse' dal novero, invero assai circoscritto, dei diritti formalmente inviolabili. Ciononostante, la tutela predisposta nei loro confronti è in ogni caso avanzata per il tempo, specie se

[306] Costituzione dell'Impero Tedesco, 28 marzo 1849 (RGBl, 1849, s. 101). Sull'origine della Carta di Francoforte v. F. Lanchester, *Le costituzioni tedesche da Francoforte a Bonn. Introduzione e testi*, Milano, Giuffrè, 2002, 26-32. La traduzione in italiano delle disposizioni offerta di seguito è tratta dall'appendice all'opera.
[307] G.F. Ferrari, *Le libertà. Profili comparatistici*, *op. cit.*, 123-125.

confrontata con le altre costituzioni coeve di cui si è detto nel Cap. I. Basti pensare che tanto lo Statuto Albertino quanto la Costituzione francese nata dopo i cd. moti di Parigi nemmeno menzionano la libertà di comunicazione e corrispondenza, limitandosi, nell'ambito delle libertà della sfera privata, a riconoscere l'*habeas corpus* e la tutela domiciliare.

In ogni caso, è di rilievo il fatto che la Costituzione della *Paulskirche* distingua i due profili della libertà e della segretezza delle comunicazioni, dedicando una distinta disposizione a ciascuna di esse. Con riferimento al primo profilo, la formulazione non identifica la libertà in sé e per sé, ma si preoccupa piuttosto di delineare quali siano i requisiti per poter disporre il sequestro di corrispondenza epistolare o di altri documenti[308]. Manca, in questo caso, un'esplicita menzione della riserva di legge, per cui se ne potrebbe apparentemente desumere che l'intervento della pubblica autorità che arresti il corso di una comunicazione non sia vincolato al ricorrere di alcuna fattispecie prevista dalla legge. Tuttavia, la disposizione presidia tale prerogativa con una riserva di giurisdizione, alla quale non pare potersi immaginare ipotesi di deroga, anche temporanea. Di rilievo è altresì l'obbligo di notificare tempestivamente, o comunque entro le successive ventiquattro ore, l'avvenuto sequestro della corrispondenza o del documento.

Il secondo profilo presenta una disciplina in parte differente, in primo luogo sotto l'aspetto della formulazione della disposizione. Infatti, in questo caso vi è un esplicito riferimento all'oggetto della tutela, vale a dire il segreto delle comunicazioni per corrispondenza[309]. Questo generico presidio è affiancato da una riserva di legge, che peraltro appare qualificabile come rinforzata per contenuto, poiché vi è un'esplicita menzione delle circostanze in relazione alle quali la legge possa disporre limitazioni del diritto costituzionalmente sancito. Peraltro, non è secondario che si specifichi che le restrizioni previste siano quelle necessarie in tali circostanze, valendo

[308] Titolo VI, Art. III, § 141 "Il sequestro di lettere e carte – salvo in caso di arresto o perquisizione domiciliare – può essere effettuato solo in forza di un ordine motivato dal giudice, che deve essere notificato all'interessato immediatamente, oppure entro le ventiquattr'ore successive".
[309] Titolo VI, Art. III, § 142 "È garantito il segreto epistolare. Le restrizioni necessarie in caso di guerra e di inchieste penali verranno stabilite dalla legge".

in apparenza questa precisazione a escludere una discrezionalità generalizzata del legislatore nella predisposizione di eccezioni al principio costituzionale generale.

L'assenza di una menzione esplicita della riserva di giurisdizione con riferimento alla limitazione del segreto della corrispondenza potrebbe far pensare che i redattori della Carta di Francoforte ritennero di limitare la portata di tale garanzia alla sola libertà di corrispondenza. Tuttavia, a uno sguardo più accorto si potrebbe ragionevolmente inferire che non vi potrebbe essere una violazione della segretezza del contenuto della comunicazione senza un previo arresto del corso della medesima, che è però vincolato a un provvedimento giurisdizionale. Pertanto, risultando l'intervento del giudice un antecedente logico – in quanto presupposto dell'intercettazione della comunicazione – nella catena degli eventi che consentirebbero di prendere cognizione del contenuto della corrispondenza epistolare, si ritiene di poter concludere che la riserva di giurisdizione si applichi *a fortiori* al profilo della segretezza della corrispondenza.

È opportuno tenere a mente che si tratta in ogni caso di una costituzione che, per le ragioni brevemente descritte sopra, rimase allo stadio di tentativo, per quanto di pregevole fattura, soltanto sulla carta e dunque le ipotesi interpretative tratte dal suo testo non possono essere suffragate (o contestate) da alcuna prassi applicativa concreta. Peraltro, a differenza delle altre esperienze europee di costituzionalismo liberale di cui si è dato conto in chiave storica (Francia e Italia, v. *supra* Cap. I), l'ordinamento tedesco si caratterizza per un marcato grado di decentramento della tutela dei diritti in epoca liberale. Infatti, dopo l'unificazione raggiunta al termine della guerra franco-prussiana, tale compito fu affidato dalla Costituzione dell'Impero tedesco del 1871[310] alle carte costituzionali dei singoli *Länder*[311].

Paradossalmente, la scelta di riservare agli Stati federati la disciplina dei diritti dei cittadini (*rectius*, dei sudditi) si rivelò in alcuni casi più favorevole nei loro confronti rispetto alle previsioni dello Statuto Albertino e delle Carte francesi dell'Ottocento, che – come è stato ricordato – non contemplavano una proclamazione della libertà di corrispondenza o dell'inviolabilità della sua segretezza. Basti in questo caso l'esempio

[310] Costituzione imperiale del 16 aprile 1871 (BGBl. 1871, n. 16, S. 63 ss.).
[311] G.F. Ferrari, *Le libertà. Profili comparatistici*, *op. cit.*, 159.

tratto dal *Land* più noto e importante, vale a dire la Prussia, la cui Costituzione – concessa dal Re Federico Guglielmo nel 1850 – qualificava il segreto epistolare come inviolabile, subordinando le limitazioni (necessarie) nei casi di perquisizioni a fini di indagine e in tempo di guerra al rispetto della riserva di legge[312].

È interessante notare come, in questo testo costituzionale, vi sia esplicito riferimento solo al profilo della segretezza del contenuto delle comunicazioni, mentre il tema della libertà di comunicazione fra privati rimane sullo sfondo, appena accennato nella disposizione che presidia il domicilio, ove si dispone che il sequestro di lettere e documenti reperiti presso un'abitazione sono ammessi solo nei casi e con i modi stabiliti dalla legge[313]. Si introduce cioè, apparentemente, una riserva di legge assoluta a presidio della libertà di corrispondenza che, tuttavia, non sia ancora stata inviata oppure che sia già pervenuta a destinazione (cioè quella che si trovi – già o ancora - in ambiente domiciliare). Avverso il sequestro della corrispondenza in via di trasmissione, che si presuppone sia quella soggetta ai rischi di interferenza più significativi, invece nulla si dice. Peraltro, il mancato riferimento ai limiti del potere di sequestro della corrispondenza distanzia non poco questo testo dalla Costituzione della *Paulskirche*, che subordinava tali atti al rispetto della riserva di giurisdizione. L'assenza di quest'ultima con riguardo alla limitazione della libertà della corrispondenza incide direttamente anche sulla tutela della segretezza del contenuto delle stesse, dato che non vi è menzione alcuna dell'obbligo di intervento del giudice nell'unica disposizione in materia della Costituzione prussiana.

[312] Costituzione di Prussia, sancita dal Re il 31 gennaio e giurata il 6 febbraio 1850, Art. 33 "Il segreto delle lettere è inviolabile. Le restrizioni occorrenti nelle perquisizioni giudiziarie e nei casi di guerra saranno indicate e decretate per legge".
[313] Costituzione di Prussia, Art. 6 "Il domicilio è inviolabile. Le infrazioni di esso e le perquisizioni, come pure il sequestro di lettere e carte domestiche, non sono permessi che nei casi e secondo le forme dalla legge stabilite".

2.2. Il laboratorio di Weimar

L'epoca liberale si chiude in Germania con la fine della prima guerra mondiale e la transizione dall'Impero alla forma di Stato repubblicana: si tratta di un'esperienza breve ma significativa sotto il profilo costituzionale, in particolare per quanto riguarda la tutela dei diritti. Infatti, la Costituzione di Weimar (1919), che dopo meno di quindici anni lascerà il campo al lungo decennio nazionalsocialista e alla distruzione causata dagli eventi bellici del secondo conflitto mondiale, marca una netta distinzione con il costituzionalismo liberale ottocentesco, in particolar modo quello di matrice conservatrice che aveva dominato la scena in Germania[314].

La Carta di Weimar risente dell'evoluzione della società e del passaggio dallo Stato monoclasse (borghese) a uno Stato pluriclasse nel quale si affermano partiti di massa. Non è un caso che l'impostazione originaria predisposta sotto la direzione di Hugo Preuss, caratterizzata da un'ottica per così dire minimalista e rivolta in via esclusiva alla disciplina dei rapporti fra organi dello Stato e fra i diversi enti della Repubblica (in guisa della Costituzione guglielmina imperiale del 1871), fu poi soppiantata in favore dell'adozione di un testo ben più articolato e contenente, nella seconda parte, un catalogo dei diritti fino a quel momento ineguagliato per ampiezza e natura[315].

La novità più dirompente del testo weimariano consiste infatti nell'espansione della sfera dei diritti dell'individuo tramite il riconoscimento di prerogative diverse dalle tradizionali libertà negative del costituzionalismo borghese, coincidenti in larga parte con le libertà civili. Con la Carta del 1919 appaiono dunque, per la prima volta nelle vicende del costituzionalismo europeo, i cd. diritti sociali, tanto che tradizionalmente è proprio alla Germania di Weimar che viene ricondotta la prima manifestazione di quella particolare forma di Stato di democrazia pluralista che è lo Stato sociale (*Welfare State*), che si diffonderà nel resto d'Europa solo nel secondo

[314] G.F. Ferrari, *Le libertà. Profili comparatistici*, *op. cit.*, 153-163.
[315] C. Mortati, *La Costituzione di Weimar*, Milano, Giuffrè, 2019 (ed. orig. C. Mortati, *Introduzione a La Costituzione di Weimar*, Firenze, Sansoni, 1946), 31-33.

dopoguerra, a partire dall'influenza del Rapporto Beveridge sul Gabinetto Attlee nel Regno Unito[316].

Per quanto concerne il profilo della libertà e segretezza delle comunicazioni, va senz'altro sottolineato come l'impostazione della Costituzione di Weimar non tragga ispirazione, come forse ci si attenderebbe sulla base dell'assenza di disciplina dei diritti nella Costituzione del II Reich, dal suo più illustre antecedente storico del 1848. Infatti, è del tutto assente nella disposizione che tutela il segreto della corrispondenza epistolare[317] qualsiasi riferimento all'intervento dell'autorità giurisdizionale, che rappresentava la garanzia cardine dinanzi alla limitazione di questo diritto nella Costituzione di Francoforte.

L'assenza di riserva di giurisdizione, l'attenzione al solo profilo della segretezza delle comunicazioni per corrispondenza (senza riguardo alcuno alla proclamazione della loro libertà) e la previsione di possibilità di limitazione della prerogativa in questione per legge mettono in luce le affinità della tutela weimariana con quella della Costituzione prussiana del 1850, seppur senza che la prima vincoli ad alcuna ragione specifica tale compressione del diritto, così 'slegando' le mani al legislatore dal contenuto rinforzato che invece vincolava il decisore politico prussiano. Un'altra differenza che pare d'uopo sottolineare è l'estensione della qualifica di inviolabilità anche al segreto delle comunicazioni, mentre la Costituzione della *Paulskirche* riconosceva come tali soltanto la libertà personale e il domicilio.

Non si può in ogni caso sovrastimare l'effetto pratico di tali garanzie procedurali e formali, non fosse altro che, per quanto moderna, la Costituzione di Weimar non si può ritenere appartenente a pieno titolo alle Costituzioni moderne post-belliche, pur potendosi già qualificare la Germania di Weimar come una forma di Stato costituzionale di diritto. Infatti, la Carta di Weimar è sì un testo costituzionale formalmente rigido, nel senso che non può essere modificato per via legislativa ordinaria: in deroga alla regola della decisione a maggioranza semplice dettata per le

[316] G. Cerrina Feroni, *Forme di Stato*, in P. Carrozza-A. Di Giovine-G.F. Ferrari (a cura di), *Diritto costituzionale comparato*, Roma-Bari, Laterza, 2009, 688 ss.
[317] Costituzione di Weimar dell'11 agosto 1919 (RGBl. n. 152, S. 1383), Art. 117 "Il segreto epistolare e quello telegrafico e telefonico è inviolabile, salvo le limitazioni da stabilire con legge del Reich".

deliberazioni su tutte le altre materie[318], la revisione costituzionale richiedeva un quorum deliberativo di 2/3 dei presenti alla sessione del *Reichstag*, a patto che fosse integrato il quorum costitutivo dei 2/3 dei membri dell'assemblea[319]. Tuttavia, ciò che nella Costituzione del 1919 manca è una qualsivoglia indicazione di limiti (espliciti) alla revisione costituzionale, sì da circoscrivere, ad esempio, il potere di modificare il catalogo dei diritti fondamentali degli individui o l'architettura di base della forma dello Stato, cosa che invece caratterizza la cd. Costituzione di Bonn, che a questo proposito contempla le cd. 'clausole di eternità'[320].

Come è evidente, non si tratta di uno scrupolo irrilevante, poiché fu proprio tale margine indefinito affidato al legislatore a consentire il progressivo ma rapido smantellamento del sistema costituzionale di Weimar e la transizione allo Stato totalitario[321]. Infatti, l'irreversibile crisi nella quale si era avvitata l'esperienza weimariana precipitò già poche settimane dopo la nomina di Hitler a Cancelliere da parte del Presidente del Reich Hindenburg nel gennaio 1933. Quando – a seguito dell'incendio del Reichstag – si fece ricorso ai poteri presidenziali emergenziali ex-art. 48 della Costituzione del 1919, in forza del *Decreto per la difesa del popolo e dello Stato*[322] furono sospesi i diritti civili della sfera privata e pubblica, nonché il diritto di proprietà e di tutela avverso l'espropriazione[323].

Tale eccezionale limitazione in concreto delle prerogative individuali riconosciute dalla Costituzione dimostra altresì come nell'architettura costituzionale di Weimar l'attributo della fondamentalità e dell'inviolabilità non implicasse una generale incomprimibilità dei diritti individuali, che potevano infatti essere (temporaneamente) sospesi al ricorrere di determinate circostanze. Come noto, il provvedimento di cui sopra non fu che l'inizio della fine dell'esperienza di Weimar e dunque, pur nella continuità formale dello Stato, la transizione a un ordinamento totalitario ebbe profili affini a quelli di cui si è detto con riferimento allo Stato fascista

---

[318] Art. 32 Cost. Weimar.
[319] Art. 76 Cost. Weimar
[320] Art. 79, §3 GG.
[321] D. Grimm, *La Costituzione di Weimar vista nella prospettiva del Grundgesetz*, in *Nomos. Le attualità nel diritto*, 2/2012, 3.
[322] *Vorordnung des Reichspräsidenten zum Schutz von Volk und Staaat* [RGBl 1933 I, S.83].
[323] F. Lanchester, *op. cit.*, 71-72.

in Italia con riferimento ai limiti al godimento e alla garanzia dei diritti e delle libertà civili.

2.3. Aspettando la Costituzione federale …

La Legge Fondamentale tedesca, che costituisce il parametro di giudizio del Tribunale costituzionale federale di stanza a Karlsruhe, appartiene allo stesso ciclo costituzionale delle Carte della IV Repubblica Francese (1947) e della Repubblica Italiana (1948). Tuttavia, essa viene redatta in un contesto senz'altro diverso dalle due coeve, non fosse altro perché il territorio del Paese è occupato e sarà ben presto spartito nelle due sfere di influenza atlantica e sovietica.

Peraltro, la struttura federale dell'ordinamento tedesco supplisce in qualche modo al 'ritardo' nella redazione della carta, che verrà a esistenza solo nel 1949. Le prime garanzie dei diritti individuali si possono dunque rintracciare nelle Costituzioni di alcuni dei *Länder*, le quali perlopiù sancivano una generica garanzia[324] o l'inviolabilità[325] del segreto epistolare, talvolta introducendo una riserva di legge per la disciplina delle eccezioni al principio generale[326], che poteva spingersi fino a vietare le limitazioni dovute a ragioni politiche[327]. Vi erano altresì esempi meno inquadrabili nelle categorie generali, quali quello della dettagliata disposizione in materia della Costituzione della Libera Città di Brema, che alla riserva di legge sommava la riserva di giurisdizione ed era rinforzata per contenuto, menzionando esplicitamente i fini di

---

[324] Costituzione della Renania-Palatinato 1947, Art. 14 "*Il segreto postale e delle telecomunicazioni è garantito. Le eccezioni saranno determinate dalla legge*"; Costituzione della Saarland 1947, Art. 17 "*Il segreto delle comunicazioni per lettera o per posta o per telefono è garantito. La legge dispone le eccezioni*"; Costituzione della Sassonia-Anhalt 1947, Art. 15 "*Il segreto delle comunicazioni per lettera, per posta, per telegrafo e per telefono è consentito se non per motivi di legge*".

[325] Costituzione della Baviera 1946, Art. 112–1 "*Il segreto epistolare, quello postale, telegrafico e telefonico sono inviolabili*"; Costituzione della Sassonia 1947, Art. 14 "*Il segreto epistolare, delle comunicazioni postali e delle telecomunicazioni è inviolabile*"; Costituzione di Berlino 1950, Art. 10 "*Il segreto delle comunicazioni per lettera o per posta o per telefono è inviolabile*"; Costituzione dell'Assia 1946, Art. 12 "*Il segreto delle comunicazioni postali è inviolabile*".

[326] Costituzione del Württemberg-Hohenzollern 1947, Art. 19 "*Il segreto delle comunicazioni per lettera o per posta o per telefono è inviolabile. Un'eccezione, che non vada contro lo spirito della Costituzione, si trova nei motivi di legge*"; Costituzione del Meclemburgo 1947, Art. 13 "*Il segreto delle comunicazioni per lettera, per posta, per telegrafo e per telefono è inviolabile. Eccezioni sono consentite solo per motivi di legge*".

[327] Costituzione del Baden-Württemberg 1946, Art. 11 "*Il segreto delle comunicazioni per lettera, posta, telegrafo e telefono è inviolabile. Eccezioni possono essere disposte per legge. Le eccezioni disposte per ragioni politiche sono inammissibili*".

persecuzione penale. Inoltre, essa sanciva il possibile intervento del Pubblico Ministero in deroga alla riserva di giurisdizione in caso di pericoli imminenti[328]. Altro esempio che si differenzia dalle forme più diffuse di tutela del diritto nelle costituzioni statali era quella del Brandeburgo, che sanciva genericamente dei limiti all'azione legislativa dello Stato, identificandoli in una serie di diritti fondamentali fra i quali era ricompresa la tutela del segreto epistolare[329]. Diversamente, vi erano altre carte che a tale prerogativa non facevano alcun riferimento, difettando del tutto di un catalogo di diritti dei propri cittadini[330].

Va senz'altro precisato che queste carte furono perlopiù approvate prima che entrasse in vigore la Legge Fondamentale del 1949, perciò ben si comprende un'esigenza di proclamare questo diritto (insieme ad altri), che altrimenti sarebbe rimasto, seppur momentaneamente, privo di copertura costituzionale. A suffragio di tale lettura, si ponga mente al *Land* Renania Settentrionale-Vestfalia, la cui Costituzione, approvata nel 1950, pur non menzionando questa prerogativa rinviava esplicitamente ai diritti contenuti nel catalogo della *Grundgesetz*, prescrivendone il rispetto[331].

Altro riferimento che è opportuno tenere a mente, prima di passare alla Costituzione della Germania Federale, che sarà il costante riferimento di qui a seguire, salvi riferimenti espliciti ad altra fonte, è che pochi mesi prima entrò in vigore anche la Costituzione della Repubblica Democratica Tedesca, che in una sola disposizione dedicata anche alla libertà personale e al domicilio qualificava il segreto postale come garantito, pur potendo il suo godimento essere limitato o soppresso per effetto di leggi generali[332].

Pur non potendo in questa sede diffondersi sulla sorveglianza occulta che caratterizzava la vita nella porzione di Germania che aderiva al Patto di Varsavia, non si può omettere un assai sintetico riferimento al sacrificio pressoché costante del diritto

---

[328] Costituzione di Brema 1947.

[329] Costituzione del Brandeburgo 1947.

[330] Costituzione della Grande Berlino 1946; Costituzione della Città Anseatica di Amburgo 1946; Costituzione della Turingia 1946; Costituzione dello Schleswig-Holstein 1949.

[331] Costituzione della Renania Settentrionale-Vestfalia 1950.

[332] Legge Fondamentale della Repubblica Democratica Tedesca del 7 ottobre 1949, Art. 8 "*La libertà personale, l'inviolabilità del domicilio, il segreto postale nonché il diritto di scegliere liberamente la propria residenza sono garantiti. I poteri pubblici possono limitare o togliere queste libertà soltanto sulla base di leggi valevoli per tutti i cittadini*".

sancito alla disposizione di cui sopra. Infatti, il famigerato Ministero per la sicurezza dello Stato (*Ministerium für Staatssicherheit*), passato alla storia come *Stasi*, in forza della crasi fra le due parole tedesche che stanno per Stato (*Staat*) e sicurezza (*sicherheit*), ha operato per decenni una capillare sorveglianza dei cittadini della Repubblica Democratica Tedesca per conto del Partito di unità socialista tedesco, nell'ambito di un ordinamento a carattere socialista.

D'altronde, tale funzionalizzazione di tutti i diritti individuali alla realizzazione di una forma di Stato socialista si evince anche dalle enfatiche disposizioni della seconda carta costituzionale della Germania orientale[333], che dedicava sì una disposizione specifica alla proclamazione dell'inviolabilità del segreto di tutte le comunicazioni, ma prevedeva deroghe vincolate alla riserva di legge, rinforzando tale garanzia per contenuto mediante l'indicazione dei fini della sicurezza dello Stato socialista o della persecuzione di un reato in sede penale[334]. Si potrebbe obiettare che si tratta in ogni caso di ipotesi più circoscritte di quelle contemplate dall'art. 10 GG dopo la revisione costituzionale del 1968 (v. *infra*, §2.6), ma in realtà quelle previste dalla Costituzione della Repubblica Democratica Tedesca prevedono deroghe senza specificarne l'estensione, mentre quelle disciplinate dal GG dispensano soltanto dall'obbligo di notifica e consentono di sottoporre a un controllo diverso da quello giurisdizionale la legittimità della misura. Peraltro, è cosa nota che la tutela costituzionale 'sulla carta' può ben divergere dalla garanzia in concreto di un interesse, specie in ordinamenti le cui decisioni politiche e legislative erano almeno parzialmente eterodirette, laddove la Germania occidentale aveva riacquisito, seppure nel corso del tempo, una vera e propria sovranità di diritto ma anche di fatto sul proprio territorio.

[333] Costituzione della Repubblica democratica tedesca del 27 settembre 1974 (GBl. I, nr. 47 - 1974).
[334] Art. 31 "Il segreto epistolare ed il segreto delle telecomunicazioni sono inviolabili. Limitazioni in tal senso sono possibili soltanto in base a leggi se lo richiedono la sicurezza dello Stato socialista o un procedimento penale".

2.4. *La disciplina costituzionale nella* Grundgesetz

La Legge Fondamentale della Repubblica Federale Tedesca si distingue rispetto alla Costituzione di Weimar per la previsione di meccanismi più strutturati a presidio dei diritti fondamentali, che giovano in primo luogo di una tutela esplicita sotto il profilo dei limiti alla revisione costituzionale[335]. Infatti, a differenza del mero requisito dell'aggravio procedurale contemplato nella Carta del 1919, la Costituzione di Bonn, che pure conserva l'obbligo di un voto a maggioranza qualificata delle due Camere del Parlamento federale, erge una barriera formidabile a tutela dei diritti fondamentali sanciti nella prima parte della Costituzione.

In primo luogo, la cd. clausola di eternità (lett. *Ewigkeitklausel*), sottrae alla revisione costituzionale il principio federalista, la partecipazione degli Stati federati all'attività legislativa, ma anche i principi di cui ai primi venti articoli della Carta (dedicati, per l'appunto, ai diritti fondamentali)[336]. Il presidio di tali diritti si sostanzia altresì del principio generale che chiude il catalogo delle libertà, a norma del quale qualsiasi limitazione ai diritti fondamentali consentita dalla Legge Fondamentale, contenuta in una legge o disciplinata in base a una fonte legislativa, deve avere carattere generale e non individuale (vale a dire non si possono approvare cd. leggi-provvedimento che limitino i diritti fondamentali). A ciò, si aggiunge inoltre l'obbligo di menzionare la disposizione della Carta che riconosce il diritto che viene compresso, dovendo curarsi di non lederne il nucleo essenziale (cd. *wesensgehalt*). Peraltro, non secondario è il fatto che la stessa disposizione riconosca in capo a tutti i cittadini l'accesso alla tutela giurisdizionale per la lesione dei propri diritti.

È evidente come le garanzie presenti nel testo del 1949 siano di gran lunga più rigorose di quelle della Carta risalente a trent'anni prima, soprattutto se si considera l'operare di un Tribunale costituzionale federale investito di rilevanti poteri di *judicial review*, che poco o nulla ha da spartire con il timido *Staatsgerichtshof* dell'esperienza di Weimar[337]. Ciò vale a maggior ragione se si tiene conto dello straordinario allargamento della platea dei soggetti titolati ad adire il *BundesVerfassungsGericht*, che

[335] F. Lanchester, *op. cit.*, 87.
[336] Art. 79, §3 GG.
[337] Art. 108 Cost. Weimar, istituito con l. 9 luglio 1921 (RGBl, 1921, I, S. 905)

in Germania è stato a lungo in buona sostanza illimitata in ragione della generosa e ampia formulazione della disposizione sul *Verfassungsbeschwerde*[338].

Assunti tali dati preliminari di contesto, si può dunque procedere a considerare quale tutela sia stata prevista dalla Legge Fondamentale alla libertà di comunicazione e alla segretezza del suo contenuto. L'art. 10 affermava in origine che "[i]l segreto epistolare, come il segreto delle comunicazioni postali telegrafiche e telefoniche, è inviolabile". Si tratta, in tutta evidenza, di una disposizione sintetica e solenne, priva di qualsivoglia riferimento a possibili limitazioni della prerogativa in questione. Peraltro, si noti che anche in questo caso, come nella Carta di Weimar, il costituente si preoccupa di tutelare il profilo della segretezza, senza porre mente, almeno esplicitamente, al tema della libertà di comunicazione privata, che pure si può forse ritenere implicitamente assorbito nella segretezza, del quale è senz'altro prerequisito. Una proclamazione tanto granitica del diritto in questione sembra non avere bisogno né di riserva di legge né di riserva di giurisdizione, che infatti non figurano in questa prima fase, anche forse in ragione del fatto che le attività di sorveglianza occulta erano esercitate in territorio tedesco dalle potenze occupanti e non tanto dalle istituzioni della neonata Repubblica Federale Tedesca[339].

È d'uopo segnalare come la segretezza del contenuto delle comunicazioni rientri fra i diritti dai quali si può decadere a norma dell'art. 18 GG, che ricollega tale conseguenza alle condotte poste in essere al fine di combattere l'ordinamento fondato sui principi di libertà e democrazia abusando di alcuni diritti fondamentali sanciti dalla Legge Fondamentale. Si tratta, in ogni caso, di effetti meramente individuali e non a portata collettiva, disciplinati dalla legge sul Tribunale Costituzionale Federale[340].

L'aspetto originario della *Grundgesetz* è mutato sotto diversi profili nel corso dei decenni, in particolare a partire da quando la Germania occidentale ha recuperato una

---

[338] G. Parodi, *La Germania e l'Austria*, in P. Carrozza-A. Di Giovine-G.F. Ferrari (a cura di), *Diritto costituzionale comparato*, Roma-Bari, Laterza, 2009, 221.

[339] C.D. Classen-A. Gaillet, *Allemagne : la lutte antiterroriste sans régime d'exception*, in *Annuaire international de justice constitutionnelle*, 32-2016, 2017, *Migrations internationales et justice constitutionnelle - Référendums et justice constitutionnelle*, 15-27. V. anche B. R. Ruiz, *Privacy in telecommunications. A European and an American approach*, L'Aja, Kluwer Law International, 1997, 267-268.

[340] *Gesetz über das Bundesverfassungsgericht* del 12 marzo 1951 (BGBl. I S. 243).

propria sovranità piena in forza della Convenzione di Bonn del 1952[341], come poi modificata dagli Accordi di Parigi del 1954[342]. In particolare, a questo nuovo ingresso nel consesso internazionale degli Stati è seguita una prima fase di revisione del testo adottato a Bonn nel 1949, anche se il blocco di modifiche alla Carta più controverso è probabilmente quello del decennio successivo[343]. Infatti, la diffusione di un clima di alta tensione interna e internazionale e il desiderio di evitare un ripetersi degli eventi che avevano portato alla fine dell'esperienza di Weimar portarono alla diciassettesima legge per l'integrazione del testo[344], che introduceva la cd. *Notstandverfassung* (Costituzione d'emergenza)[345].

Questo riferimento è particolarmente rilevante per la presente trattazione, poiché l'intervento di revisione del legislatore introdusse un secondo, significativo comma all'art. 10 GG. Il testo emendato recita dunque "[i]l segreto epistolare, come il segreto delle comunicazioni postali telegrafiche e telefoniche, è inviolabile. Limitazioni possono essere disposte solo in base ad una legge. Se la limitazione è finalizzata a salvaguardare l'ordinamento fondato sui principi di libertà e di democrazia o la stabilità o la sicurezza dello Stato federale o di un Land, la legge può disporre che essa non sia resa nota all'interessato e che al rimedio giurisdizionale subentri un controllo di organi, e di ausiliari di questi ultimi, designati dal parlamento"[346].

Le novità introdotte consistono, in primo luogo, nella menzione esplicita della possibilità di derogare al principio generale dell'inviolabilità del segreto delle comunicazioni, vincolando l'introduzione di tali restrizioni alla riserva di legge. La disposizione prosegue identificando dei fini specifici (ma non tassativi) il cui perseguimento giustifica l'omissione della notifica al destinatario delle misure di interferenza con il diritto in oggetto e ammette l'affidamento del controllo sulla

---

[341] *Convenzione sulle relazioni fra le Tre Potenze e la Repubblica Federale Tedesca*, firmata a Bonn il 26 maggio 1952, da Stati Uniti d'America, Francia, Regno Unito e Repubblica Federale Tedesca.
[342] *Protocollo sulla cessazione del regime d'occupazione nella Repubblica Federale Tedesca*, firmato a Parigi il 23 ottobre 1954 da Stati Uniti d'America, Francia, Regno Unito e Repubblica Federale Tedesca.
[343] D.P. Kommers, *The Basic Law: A Fifty Year Assessment*, in *German Law Journal*, 20, 2019, 571–582.
[344] 17esima l. rev. Cost. 26 giugno 1968 (BGBL. I, S. 709).
[345] F. Lanchester, *op. cit.*, 97-98.
[346] Comma aggiunto in sede di revisione cost.le dalla 17esima l. rev. Cost. 26 giugno 1968 (BGBL. I, S. 709)

legittimità delle stesse a organi diversi dall'autorità giudiziaria, purché chiaramente identificati dal potere legislativo.

I fini specifici menzionati nella disposizione sono spia del desiderio dell'ordinamento tedesco di proteggersi dalle spinte, siano esse endogene o esogene, atte a sovvertire l'ordinamento costituzionale e a mettere in pericolo la sicurezza dei propri cittadini. La tutela avverso tali minacce si coniuga, tuttavia, con un sacrificio non indifferente alla conoscenza della limitazione da parte del destinatario e al diritto alla tutela giurisdizionale ex-art. 19, §4 GG, che pure viene modificato con la legge di revisione costituzionale menzionata facendo esplicitamente salva l'eccezione di cui al nuovo testo dell'art. 10, §2 GG.

Sulla scia di tali modifiche al testo della Legge fondamentale, il legislatore tedesco approvò una legge ordinaria di attuazione del secondo paragrafo dell'art. 10 GG appena introdotto, nota come *Legge sulla restrizione del segreto di lettere, posta e telecomunicazioni* o *legge sull'articolo 10 Legge fondamentale* (G 10)[347] (v. *infra*, § 2.6).
Quanto contenuto nel testo legislativo di cui sopra non esaurisce, come si può ben immaginare, il novero delle fattispecie nelle quali i pubblici poteri sono autorizzati a interferire con la prerogativa individuale in parola. Come avviene d'altronde anche nell'ordinamento italiano, vi è una sezione specifica del codice di procedura penale tedesco (§§99-101b *Strafprozessordnung*, d'ora innanzi StPO) che disciplina i poteri di investigazione in questo senso dell'autorità inquirente nell'ambito di un procedimento in sede penale (v. *infra*, §2.5).

2.5. Le limitazioni ordinarie contenute nel codice di procedura penale

A norma del §99 StPO qualsiasi comunicazione che avvenga per iscritto o altra forma di invio per corrispondenza può essere intercettata dalla pubblica autorità se inviata da o indirizzata a un soggetto accusato della commissione di un fatto di reato e sottoposto a misure cautelari personali nell'ambito di un'indagine penale. Diversamente, per le altre modalità di telecomunicazione, solo nei casi di sussistenza

[347] *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses* (*Gesetz zu Artikel 10 Grundgesetz*) (G 10).

di seri indizi di reato si ritiene di autorizzare l'operazione di intercettazione occulta, a patto che la condotta perseguita sia particolarmente grave e il mancato ricorso a tale strumento sia passibile di vanificare lo sforzo investigativo o frustrare la possibilità di rintracciare la persona sospettata di aver commesso il fatto (§100a StPO). Peraltro, quest'ultima disposizione è stata modificata alla fine degli anni '80 per potersi applicare a tutte le telecomunicazioni e non, come era originariamente, solo a quelle orali.

La disposizione in questione soffriva, già all'origine, di alcuni rilevanti limiti applicativi, quali ad esempio il riferirsi solo a flussi comunicativi e non ai dati elaborati senza che fossero trasmessi (che, peraltro, più che dall'art. 10 GG sarebbero coperti dall'art. 2.1 GG) o il requisito non particolarmente stringente del sospetto che debba gravare sul soggetto destinatario delle misure di intercettazione, anche se esse possono altresì essere disposte nei confronti di una terza persona con la quale è ragionevole pensare il sospettato intrattenga comunicazioni (§100a.3)[348].

Come nel caso italiano, anche in quello tedesco il codice di rito prevede una molto nutrita serie di fattispecie di reato in relazione alle quali sia legittima la ricerca di mezzi di prova tramite operazioni di intercettazione delle comunicazioni (§100a.2). Lo stesso testo legislativo prevede il requisito dell'autorizzazione di un giudice, che può essere legittimamente derogato in casi eccezionali per mezzo dell'atto del pubblico ministero, ma le operazioni devono essere convalidate ex-post da un giudice entro il termine di tre giorni, a pena di decadenza (§§100.1-2). Peraltro, il plico postale il cui corso sia stato interrotto per ordine dell'autorità giudiziaria può essere aperto per prendere cognizione del contenuto solo previa autorizzazione dello stesso giudice (§ 100.4.2), che è il soggetto generalmente titolato a conoscere il contenuto della comunicazione intercettata.

Il codice di rito prevede una disciplina specifica per le perquisizioni di sistemi informatici, pur applicabile in presenza degli stessi presupposti prescritti per le operazioni di intercettazione delle telecomunicazioni (§100b.1). Una delle differenze risiede nella possibilità di porre in essere tale atto investigativo solo nei confronti del soggetto accusato e, pertanto, perquisire digitalmente solo quei sistemi informatici dei

[348] B.R. Ruiz, *op. cit.*, 216 ss.

quali l'indagato abbia la titolarità, a meno che vi siano chiari indizi che esso utilizzi sistemi informatici altrui o che la ricerca sul dispositivo del solo accusato sarebbe insufficiente a stabilire i fatti oggetto d'indagine o il luogo ove si trovi un co-accusato (§100b.3). Analoghi limiti e requisiti sono dettati con riferimento all'intercettazione di conversazioni che avvengano in luoghi di privata dimora, assimilabili a intercettazioni cd. ambientali (§100c). Peraltro, anche l'ordinamento tedesco conosce altre forme di intercettazione tra presenti fuori dai luoghi di privata dimora (§100f) e raccolta di mezzi di prova audiovisivi sempre in aree non private (§100h).

Prima di delineare i contenuti obbligatori dei provvedimenti di autorizzazione a esperire operazioni di intercettazioni o sorveglianza occulta, è opportuno dare conto della disposizione del codice di rito che dispone l'inammissibilità delle operazioni suddette laddove le circostanze di fatto facciano presumere una probabile interferenza nel nucleo più profondo della sfera riservata dell'individuo (§100d). Se, ciononostante, dati relativi a tale ambito vengono registrati, non possono essere utilizzati e devono essere tempestivamente distrutti, dandone conto in apposito verbale. Peraltro, le adeguate accortezze tecniche devono essere adottate affinché, per quanto possibile, tali circostanze non si verifichino.

L'ordinanza che autorizzi l'operazione di intercettazione deve indicare chiaramente l'identità del soggetto destinatario della misura e il suo indirizzo, il capo d'imputazione, nonché contenere specifica descrizione del tipo di misura, dell'ambito di applicazione della stessa e della sua durata, la natura delle informazioni che si intendono ricercare e indicazioni di dettaglio che consentano una precisa identificazione dell'utenza telefonica, sistema informatico o luogo di privata dimora che sia sottoposto alla misura (§100e.3). Le operazioni non possono eccedere i tre mesi e l'autorizzazione non può essere rinnovata che per una volta per quanto riguarda la sorveglianza generica delle telecomunicazioni (§100e.1), mentre nel caso delle perquisizioni digitali occulte e dell'ascolto di conversazioni che avvengano in luogo privato il termine è di un mese, rinnovabile di volta in volta anche se allo scoccare del sesto mese la competenza sul rinnovo spetta alla corte regionale di più alto grado per ogni ulteriore rinnovo (§100e.2).

Condizione necessaria in entrambi i casi è la permanenza delle ragioni che giustificano il ricorso a tale misura, la cui assenza obbliga a interrompere le operazioni (§100e.5). Tanto la domanda di autorizzazione originaria quanto la richiesta di proroga devono contemplare l'indicazione dei fatti che fondano la richiesta e offrire sufficienti giustificazioni sulla necessità e proporzionalità della misura (§100e.4). L'utilizzo dei dati ottenuti in procedimenti connessi o collegati è ammesso solo se si perseguano reati per i quali si possono disporre tali operazioni di ricerca della prova, oppure al fine di prevenire il concretizzarsi di un pericolo imminente di morte o di minaccia alla vita o all'integrità fisica di una persona o alla sicurezza o esistenza dello Stato (§100e.6).

Vige, infine, un obbligo di procedere a distruzione delle informazioni così raccolte non appena ne sia determinata l'irrilevanza a fini processuali (§101.8) e il destinatario delle misure deve essere necessariamente avvisato di tali interferenze nella propria sfera di comunicazione riservata nel momento in cui tale cognizione non metta a repentaglio l'esito delle indagini, la sicurezza pubblica, la vita o l'integrità fisica di una persona o la possibilità di un agente sotto copertura di proseguire a operare in modo efficace (§101.4-5).

2.6. La disciplina della G 10

La *Legge sulla restrizione del segreto di lettere, posta e telecomunicazioni*, nota altresì come *legge sull'articolo 10 Legge fondamentale* (G 10), fu adottata dal legislatore tedesco dopo la revisione costituzionale che aveva aggiunto un secondo comma all'art. 10 GG, così consentendo limitazioni previste dalla legge al segreto delle comunicazioni, ammettendo deroghe all'obbligo di notificazione della restrizione al destinatario e alla devoluzione a un organo giurisdizionale dello scrutinio sulla legittimità del caso. La legislazione in commento si applica a tutti i tipi di comunicazione a patto che il soggetto sul quale grava la limitazione sia sospettato di pianificare, di aver intenzione di commettere o di aver commesso uno dei reati contro la sicurezza dello Stato o l'ordinamento democratico elencati dettagliatamente dall'art. 1, §2 della legge.

Sotto il profilo della sfera di applicazione soggettiva della disciplina, le operazioni di sorveglianza occulta possono essere dirette nei confronti del solo

soggetto gravato dal sospetto delle condotte di cui sopra o di terzi con i quali vi è ragionevole aspettativa che lo stesso intrattenga comunicazioni significative. Inoltre, anche il ricorso a queste modalità di ricerca della prova assume un ruolo residuale, che viene considerato legittimo soltanto laddove l'utilizzo di altre modalità sia impossibile o significativamente più difficile.

L'esperimento di attività di sorveglianza occulta necessita di un impulso specifico che deve obbligatoriamente provenire dall'Ufficio federale per la protezione della Costituzione, dalle analoghe autorità di ciascun *Land*, dal servizio di controspionaggio federale (se relativo alle forze armate) o dai servizi di informazione federali (se a essi pertinente). La richiesta di autorizzazione deve essere presentata per iscritto e deve contemplare l'indicazione del tipo di misura, dell'ambito di applicazione della stessa e della durata, suffragando il tutto con elementi di fatto che giustifichino il ricorso a tali strumenti di indagine[349].

L'ordine di procedere all'attività di sorveglianza deve provenire da un ministro preposto a questo compito dal Primo ministro oppure dalla più alta autorità competente per il *Land* laddove la richiesta provenga dall'ufficio territoriale per la protezione della Costituzione[350]. Sull'autorità procedente grava un immediato obbligo di notifica al destinatario, che viene meno se tale comunicazione sia suscettibile di mettere a repentaglio la riuscita delle indagini. Tuttavia, quando tale pericolo viene meno l'obbligo torna a gravare sull'autorità che ha disposto l'attività di sorveglianza[351]. Il ricorso a una commissione istituita *ad hoc* è l'unico rimedio a disposizione del singolo fino al momento in cui non sia data notificazione, a partire dalla quale è possibile promuovere un'azione per la tutela delle proprie prerogative dinanzi a un giudice.

Altro aspetto che è opportuno menzionare è che la legislazione in commento autorizza l'attività cd. di 'sorveglianza strategica', che non è diretta ad alcun destinatario specifico e, in quanto casuale, non è gravata da obbligo di notificazione[352]. Le attività di sorveglianza strategica condotte da agenzie di *intelligence*, per quanto

[349] Art. 1, §4; §2.2.1.
[350] Art. 1, §5(1).
[351] Art. 1, §5(5).
[352] Art. 1, §3.1.

senz'altro incidano sul godimento del diritto costituzionale al segreto delle comunicazioni, non sono oggetto specifico di questa trattazione, che si concentra sulle interferenze legate alla persecuzione (o alla prevenzione) di determinati reati e, pertanto, indirizzate nei confronti di soggetti ben determinati[353].

La controversa legge G 10, insieme alla legge di revisione costituzionale che aveva introdotto il nuovo comma dell'art. 10 GG, furono presto contestati e il Tribunale Costituzionale Federale, in una decisione assai controversa, si pronunciò per la legittimità costituzionale di entrambi su tutti i motivi di censura salvo quello relativo alla decadenza dall'obbligo di notifica al destinatario[354]. L'imposizione categorica contenuta nella disposizione fu ritenuta in violazione del principio di ragionevolezza, poiché privava il giudice della discrezionalità che esso poteva esercitare nel valutare se la notifica potesse pregiudicare il corso delle indagini o meno. Se infatti tale necessità non si configurasse, sarebbe costituzionalmente illegittimo continuare a celare al destinatario della restrizione che essa sia stata posta in essere.

Se la decisione sul punto di cui sopra è stata generalmente accolta con soddisfazione e ritenuta un'equilibrata applicazione del principio di ragionevolezza, il riconoscimento della legittimità costituzionale della parte della disposizione che sottrae ai singoli l'accesso alla tutela giurisdizionale, invece, è stato criticato aspramente per più ragioni. In primo luogo, è stato affermato che il sacrificio imposto ai diritti fondamentali dei cittadini è esso stesso un *vulnus* all'ordinamento democratico, che sul riconoscimento e l'effettivo godimento di tali diritti fonda la propria architettura. Pertanto, proteggere la Costituzione tramite la soppressione di alcuni suoi principi inalienabili sarebbe un controsenso e non potrebbe reggere alla prova della ragionevolezza del bilanciamento posto in essere, che, anzi, forse nel caso di specie non è stato proprio effettuato.

Altra ragione che deporrebbe a favore di una diversa decisione è che vi sarebbe stata un'alternativa meno gravosa ma che garantisse egualmente la segretezza dell'attività d'indagine in corso. Si tratterebbe, cioè, di mantenere la segretezza sul procedimento ma di consentire l'azione in giudizio, a patto che il ricorrente venga

---

[353] Alcune considerazioni sulla sorveglianza strategica ex. Legge G 10 si trovano in B.R. Ruiz, *op. cit.*, 220.

[354] BVerfG, Secondo Senato, 15 dicembre 1970, 2 BvF 1/69, 2 BvR 629/68 e 308/69.

informato della messa in atto di misure del tipo in parola solo laddove esse siano ritenute illegittime, restandone invece all'oscuro in tutti gli altri casi.

Inoltre, un'ulteriore ragione che ha fondato le critiche alla decisione in questione è stata che la Corte non abbia esercitato uno scrutinio sufficientemente penetrante sulla legge di revisione dell'art. 10 GG, considerandola in parte alla stregua di una porzione del testo già approvata e facente parte integrante della Legge Fondamentale, laddove invece era oggetto del suo scrutinio nel caso di specie[355].

3. *L'esperienza statunitense*

3.1. La tutela delle comunicazioni private prima del bill of rights

Come è noto, il costituzionalismo statunitense è caratterizzato da una traiettoria diversa da quella europea continentale e le sue vicende cominciano prima nel tempo, anche se la Rivoluzione americana (1776) e quella francese (1789) sono di fatto coeve. Inoltre, la cultura giuridica nordamericana deve molto al patrimonio giuridico di *common law* britannico, che influenza grandemente il sistema statunitense e il cui rapporto con i diritti riconosciuti dalla Costituzione federale non è ancora del tutto chiaro sotto tutti i profili. Questa breve premessa serve a spiegare come, pur partendo dal dato costituzionale, l'indagine sulla tutela accordata al segreto delle comunicazioni nel contesto nordamericano non si può arrestare a quel solo livello, ma deve comprendere altresì la logica della protezione degli interessi sottostanti come emersa nella stratificazione nel corso dei secoli partendo dal diritto comune inglese fino alla progressiva acquisizione di un indirizzo interpretativo autonomo nel contesto degli Stati Uniti d'America.

Il primo riferimento è dunque il testo della Costituzione federale del 1787, il quale notoriamente è breve se confrontato con le Costituzioni novecentesche europee e si limita a tracciare il profilo della *frame of government*, vale a dire a distribuire le competenze fra i vari organi della costituenda federazione, avendo cura di garantire quel principio cardine del costituzionalismo liberale che è la separazione dei poteri.

[355] Queste e altre considerazioni si trovano in B.R. Ruiz, *op. cit.*, 269 ss.

Tale criterio è portato a quella che è forse la sua espressione massima proprio dalla Costituzione degli Stati Uniti che, prevedendo quei 'pesi e contrappesi' (*checks and balances*) che consentono alle istituzioni, pur ciascuna titolare di poteri propri, di influenzare l'esercizio delle attribuzioni degli altri organi, serve a evitare il rischio di un'eccessiva concentrazione di tali poteri in capo a uno solo di questi soggetti[356].

Fu solo quattro anni dopo, nel 1791, che fu approvato ed entrò in vigore un catalogo di diritti, il cd. *bill of rights*, che era tuttavia percepito dagli Stati federati come una tutela avverso i penetranti poteri del nuovo governo centrale, tanto che per oltre un secolo l'interpretazione assolutamente prevalente, anche da parte della giurisprudenza, è stata nel senso di escludere l'opponibilità delle prerogative in esso sancite agli Stati della Federazione, limitandone dunque l'efficacia (e la tutela) ai soli casi di interferenza con uno di questi diritti da parte del governo federale[357].

In questo catalogo figura altresì il IV Emendamento alla Costituzione, una disposizione più articolata di molte altre fra le prime dieci, che recita "[i]l diritto dei cittadini ad essere assicurati nelle loro persone, case, carte ed effetti contro perquisizioni e sequestri non ragionevoli, non potrà essere violato, e non potranno essere emessi mandati se non su motivi probabili, sostenuti da giuramenti o solenni affermazioni e con una dettagliata descrizione del luogo da perquisire e delle persone o cose da prendere in custodia"[358].

La prima questione da prendere in considerazione riguarda le ragioni che spinsero i *Founding Fathers* a prevedere una disposizione che tutelasse avverso le perquisizioni personali, domiciliari e di propri oggetti personali da parte delle autorità pubbliche[359]. L'istituto che agitava le menti dei Padri Fondatori era uno strumento

---

[356] M. Comba, *Gli Stati Uniti d'America*, in P. Carrozza-A. Di Giovine-G.F. Ferrari (a cura di), *Diritto costituzionale comparato*, Roma-Bari, Laterza, 2009, 138.

[357] *Barron v. Baltimore*, 32 U.S. (7 Pet.) 243 (1833); *Slaughterhouse cases*, 83 U.S. (16 Wall.) 36 (1873).

[358] Trad. it. tratta da G. Cerrina Feroni- T.E. Frosini-A. Torre (a cura di), *Codice delle Costituzioni*, Torino, Giappichelli, 2009. Il testo originale della disposizione recita "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized".

[359] Tutto quanto si dirà con riferimento all'ordinamento statunitense sarà esclusivamente riferito ai rapporti sul piano verticale fra autorità pubbliche e cittadini, poiché, a differenza del costituzionalismo europeo del II dopoguerra, quello americano non ha accolto allo stato attuale la teoria della cd. *Drittwirkung*. I diritti sanciti a livello costituzionale, cioè, valgono negli Stati Uniti d'America solo per tutelarsi avverso l'interferenza o la violazione di essi da parte degli organi del potere pubblico, ma non

apparso nel corso del XVII secolo nella madrepatria inglese e che, da lì, era stato poi 'esportato' nelle colonie d'oltreoceano. Si trattava dei cd. *general warrants*, vale a dire mandati che autorizzano la perquisizione o il sequestro di beni finalizzati alla ricerca di refurtiva, ma che per la loro ampiezza si prestavano naturalmente agli abusi delle autorità che li ponessero in essere. In realtà, questi strumenti venivano usati per perquisire documenti, fra i quali la corrispondenza, nella disponibilità di oppositori o agitatori politici, sì da poterne monitorare eventuali progetti o trame eversive.

La percezione di questi strumenti come abusi intollerabili del potere pubblico aveva, a dire il vero, portato ben presto anche la tradizione di *common law* a distanziarsene, sancendo in più occasioni come i *general warrants* fossero da considerarsi non validi e che fosse lecito resistere alla loro esecuzione, fino a poter citare in giudizio chi li eseguisse per *trespass* alla propria persona o proprietà privata[360]. Le corti di *common law* inglesi, dunque, già nella seconda metà del 1600 reagirono a questi abusi del potere regio restaurato, tutelando le prerogative tradizionali di integrità fisica e proprietà privata del patrimonio giuridico inglese[361].

Diversamente, nelle colonie della costa atlantica ancora un secolo dopo la questione non si poteva dire risolta: anzi, in realtà cominciavano proprio in quel momento i contrasti più accesi con la madrepatria. In particolare, all'imposizione di severi dazi all'importazione di beni e di limitazioni al commercio con i possedimenti francesi nei Caraibi, la legislazione affiancò uno strumento che fu chiave nel convincere i futuri redattori del *bill of rights* della necessità di una disposizione del tipo del IV Emendamento. La misura in questione era il cd. *writ of assistance*, che altro non era che un potere in capo agli agenti di riscossione di tali dazi che essi potevano esercitare laddove il soggetto obbligato a versare il tributo non cooperasse e rifiutasse di pagare. Questo strumento consentiva di emanare un ordine nei confronti di tutti coloro che si trovassero nelle vicinanze affinché prestassero aiuto al funzionario a

---

sono direttamente opponibili ad altri privati, come invece è il caso per esempio in Germania e in Italia dopo le Costituzioni post-belliche.

[360] S.J. Schulhofer, *More essential than Ever: The Fourth Amendment in the Twenty First Century*, Oxford, Oxford University Press, 2012, in particolare il capitolo *Our Fourth Amendment Tradition*, 23.

[361] *Huckle v. Money*, 95 Eng. Rep. 768 (Common Pleas 1763), *Money v. Leack*, 3 Burr 1742, 97 ER. 1075 (1765) e *Entick v. Carrington and Three Other King's Messengers*, 95 Eng. Rep. 807 (Common Pleas 1765).

riscuotere la somma dovuta tramite la perquisizione della persona o del suo domicilio o dei suoi averi[362].

Si trattava quindi di uno strumento ancora più penetrante di quei *general warrants* menzionati in precedenza, non fosse altro perché quelli erano associati alla persecuzione di una condotta di reato, mentre questo dipendeva dal semplice rifiuto di pagare un tributo. La lotta contro l'applicazione dei *writs of assistance* fu una delle forze che animarono la ribellione dei coloni americani e la sua eco si riconosce senz'altro nel testo della disposizione del IV Emendamento. Nelle intenzioni dei *Framers*, infatti, un mandato che autorizzasse una perquisizione o un sequestro poteva essere emesso soltanto da un giudice sulla base di indizi specifici relativi alla commissione di un reato, inoltre avrebbe dovuto essere indirizzato a un soggetto ben individuato o a un luogo fisico chiaramente identificabile[363].

Se questa era l'intenzione che animava i Padri Fondatori, l'esito del lavoro di *drafting* potrebbe apparire non del tutto rispondente alle aspettative. Infatti, ciò che sembra potersi desumere *prima facie* dalla lettura del testo è che siano state previsti dei requisiti particolarmente stringenti per la concessione di mandati ai fini di condurre perquisizioni e sequestri. Ciò assicura che solo in presenza delle condizioni che i redattori del *bill of rights* ritennero opportune potesse essere autorizzata questa incisiva forma di interferenza nei diritti dei cittadini.

Tuttavia, la prima parte della disposizione non sancisce esplicitamente il divieto di procedere a perquisizioni e sequestri in assenza di mandati, limitandosi a vietare quelli che siano non ragionevoli, che si capisce essere una categoria che si presta a un grado di discrezionalità pericolosamente ampio in fase di interpretazione. Interpretare la disposizione rigorosamente in questi termini renderebbe senz'altro vana l'aspirazione alla liberazione dai *general warrants*. Per tale ragione, la lettura prevalente che è stata fatta della disposizione è quella secondo la quale il mandato, redatto nei termini stringenti indicati nella seconda parte della disposizione, è sempre richiesto,

---

[362] S.J. Schulhofer, *op. cit.*, 28.

[363] Sulle discussioni in sede di Convenzione costituzionale in merito alla formulazione del IV Emendamento si rinvia a W.J. Cuddihy, *The Fourth Amendment. Origins and Original Meaning 602-1791*, Oxford, Oxford University Press, 2009, in particolare il Capitolo 24 (*The Formation and Original Meaning of the Fourth Amendment, 1787-1791*), 669 ss.

salvo nei casi in cui le circostanze di fatto rendano particolarmente complicato o difficile ottenerlo[364]. Peraltro, una lettura di questo tipo non elimina quella 'zona grigia' dove è più probabile che si localizzi la gran parte del contenzioso, anche se fornisce una guida generale all'applicazione della regola ai giudici e alle autorità di pubblica sicurezza.

3.2. L'interpretazione originaria del IV Emendamento

Sebbene fosse contemplata nei primi dieci emendamenti alla Costituzione, la disposizione di cui al IV Emendamento rimase a lungo sullo sfondo del contenzioso federale, tanto che fu solo nell'ultimo quarto del diciannovesimo secolo che la Corte Suprema federale cominciò a decidere casi nei quali era richiesta un'interpretazione un poco approfondita dei contenuti del testo[365]. Il primo punto di svolta della giurisprudenza sul tema del IV Emendamento si può ricondurre alla sentenza nel caso *Boyd v. United States*[366], nel quale i *Justices* inaugurarono quella lettura della disposizione in chiave 'proprietaria' che ha orientato gli indirizzi interpretativi per quasi un secolo, fino a quando questa visione reificata della prerogativa in oggetto è divenuta recessiva (v. *infra*, §3.4).

Il caso riguardava una legislazione che era stata introdotta per prevenire i tentativi di importazione di merci in violazione delle leggi doganali, entro la quale vi era una disposizione che conferiva al legale che agiva nell'interesse dello Stato la facoltà di chiedere al giudice di emettere un ordine di esibizione di libri contabili, fatture e altri documenti commerciali nei confronti dell'altra parte. La Corte Suprema adottò nel caso in questione un approccio particolarmente favorevole al diritto di proprietà, sancendone la prevalenza sempre e comunque contro le pretese dei pubblici poteri; pertanto, una perquisizione o un sequestro che insistesse su un bene su cui il soggetto potesse vantare diritti proprietari sarebbe sempre stato non ragionevole e, di conseguenza, costituzionalmente illegittimo. Diversamente, tutto ciò che non

[364] S.J. Schulhofer, *op. cit.*, 31-32.
[365] Il primo caso di una certa consistenza fu *Ex parte Jackson*, 96 U.S. 727 (1878).
[366] 116 U.S. 616, 625-630 (1886).

rientrasse in senso stretto entro la sfera proprietaria di un soggetto potrebbe ragionevolmente essere soggetto a misure del tipo di cui sopra.

Il secondo argomento su cui i *Justices* basarono la propria decisione fu che obbligare un privato cittadino a produrre in giudizio documenti a sé appartenenti equivalesse ad acquisirli in giudizio per effetto di una perquisizione e un sequestro operati da un pubblico ufficiale entro il proprio domicilio. La ragione per cui la Corte si spinse a fare questa equivalenza, per certi versi ardita, è stata rintracciata nel desiderio della stessa di preservare lo spirito della Costituzione avverso un tentativo di eluderlo tramite un espediente legislativo. Infatti, la legislazione impugnata aveva sostituito dei testi finalizzati ai medesimi scopi ma che prevedevano la possibilità di ottenere quei documenti tramite intervento della forza pubblica. Introducendo un obbligo di esibizione del documento, il legislatore federale aveva creduto di potersi sottrarre alle garanzie di cui al IV Emendamento, ma la decisione della Corte Suprema ricondusse la disciplina nell'alveo della Costituzione[367].

Una prima conseguenza di questa impostazione interpretativa fu che la ragionevolezza citata dalla disposizione veniva declinata in due sensi. Il primo era quello stabilito dalla Corte Suprema stessa nella decisione *Boyd*, vale a dire che erano da considerarsi ragionevoli soltanto quelle perquisizioni o quei sequestri posti in essere nei confronti di beni sui quali i singoli non potessero accampare legittime pretese proprietarie. Tuttavia, in forza della lettera della disposizione, non si poteva non considerare irragionevoli anche quelle interferenze con il diritto che derivassero da mandati di perquisizione o di sequestro che difettassero di alcuni dei requisiti prescritti dalla disposizione[368].

Altri due profili che emergono da questa prima pronuncia sono una spiccata prevalenza dell'attenzione nei confronti dei sequestri, rispetto alle perquisizioni, e la combinazione del rimedio per tali condotte con quello previsto per la violazione del divieto di autoincriminazione di cui al V Emendamento, vale a dire la cd. *exclusionary rule*, cioè l'inutilizzabilità in giudizio degli elementi di prova acquisiti in violazione del IV Emendamento.

---

[367] A questo proposito, più diffusamente, v. B.R. Ruiz, *op. cit.*, 80.
[368] *Ibid.*, 82.

3.3. Le prime avvisaglie di un'evoluzione dell'interpretazione del IV Emendamento

Se con *Boyd* viene inaugurato il filone giurisprudenziale che legge il IV Emendamento come una tutela rigorosa avverso le perquisizioni e i sequestri che riguardano beni di proprietà dei singoli cittadini, nella stessa pronuncia la *concurring opinion* di *Justice* Miller, al quale si unì il *Chief Justice* Waite, contestò le conclusioni della maggioranza. Infatti, pur riconoscendo che la disposizione era stata redatta avendo in mente gli abusi dei funzionari britannici, l'intenzione non poteva essere quella di vietare il ricorso a tali mezzi di ricerca della prova *tout court*. Ciò infatti, avrebbe reso assai difficile la persecuzione dei fatti di reato sottraendo alla disponibilità delle autorità procedenti materiale probatorio altrimenti assai rilevante. Non si trattava, cioè, di un'abolizione di tali misure, bensì di una restrizione finalizzata a prevenirne gli abusi, vietando quelle *searches* e *seizures* (quindi non solo queste seconde) che fossero irragionevoli[369].

Non è un caso che pochi anni dopo apparve un testo, pubblicato su una rivista giuridica, che risponde indirettamente all'argomentazione di *Boyd* ed è universalmente considerato il punto di partenza della moderna concezione della *privacy*, vale a dire del diritto alla riservatezza della vita privata. In "*The Right to Privacy*", Samuel Warren e il futuro giudice della Corte Suprema federale Louis Brandeis sottolinearono la progressiva evoluzione della tutela di *common law*, la quale nel corso del tempo si era espansa oltre il proprio perimetro originario. Infatti, da una concezione della tutela personale limitata alla sfera dell'integrità fisica e della protezione dei beni su cui si vantavano diritti reali, si era progressivamente transitati a una lettura più estesa della sfera di protezione dell'individuo, che andava a coprire anche profili immateriali[370].

In particolare, la prima diffusione dei rotocalchi e la comparsa di immagini che avevano ritratto la buona società borghese del *New England* nel corso di feste e ricevimenti ispira il ragionamento di Warren e Brandeis. Costoro, sul presupposto dell'evoluzione della tutela di *common law* a partire dai nuclei fondamentali della

[369] 116 U.S. 616, 640-641 (1886).
[370] S.D. Warren-L.D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, Vol. 4, No. 5. (Dec. 15, 1890), 193-220.

protezione della vita, dell'esercizio delle libertà civili e della proprietà privata, costruiscono una teoria che rintraccia nel tessuto normativo esistente un "diritto a essere lasciati in pace", che è cosa diversa dal mero obbligo di astensione delle autorità pubbliche dalla sfera privata tipica delle libertà in senso liberale e già evocata qualche anno prima dal giudice Cooley[371]. Più specificamente, con un ragionamento induttivo essi pervengono all'affermazione dell'esistenza di un generale diritto di *privacy* del quale il diritto a tenere le proprie opinioni e convinzioni personali celate alla pubblica opinione, già riconosciuto dal *common law* americano in precedenza, altro non sarebbe che una *species*.

Nel riconoscere che la fattispecie in commento non si poteva correttamente sussumere sotto le figure tipiche del *breach of contract* o della violazione del *trust*, Warren e Brandeis si impegnarono altresì a delineare il campo di applicazione di questa prerogativa. Il primo limite era quello della possibilità di pubblicare tutto ciò che rientrasse nell'interesse generale e pubblico, così facendo un parallelismo con il diritto alla critica esistente nel campo delle norme sulla diffamazione e la calunnia. Inoltre, non si darebbe violazione di tale diritto nel caso di pubblicazione delle informazioni private se avvenuta nell'ambito di un procedimento giudiziario, in un'assemblea elettiva o in qualsiasi altro ente pubblico o associativo. La violazione del diritto alla *privacy* non si configurerebbe poi in caso di comunicazione per via orale, ma solo per iscritto. Inoltre, la pubblicazione delle informazioni da parte dell'interessato lo farebbe decadere dal godimento del diritto. Infine, la veridicità dei fatti pubblicati e l'assenza dell'elemento della *malice*, cioè dell'intento di ledere il soggetto, non sono considerati rilevanti ai fini della configurazione della violazione del diritto.

Se la risonanza del contributo dei due giuristi di Boston fu senz'altro significativa, non altrettanto si può dire dell'accoglimento della loro impostazione teorica da parte della giurisprudenza dei decenni successivi. Infatti, una delle critiche emerse negli anni successivi fu che il diritto a essere lasciati in pace come teorizzato da Warren e Brandeis peccava di incertezza con riferimento alla distinzione tra la sfera pubblica e quella privata. Ciò aveva dunque portato alcuni giudici a rigettare, pur se

[371] T.M. Cooley, *The Elements of Torts*, Chicago, Callahan, 1878.

di misura, azioni promosse per la tutela della propria vita privata avverso la lesione cagionata dall'utilizzo della propria immagine a propria insaputa a fini pubblicitari[372]. Tuttavia, un tale rigetto fu la miccia che portò all'approvazione della prima legge statale sulla *privacy*[373], approvata dallo Stato di New York l'anno successivo, e alla decisione della Corte Suprema della Georgia che soli tre anni dopo il caso *Robinson* sancì l'esistenza di un *common law right to privacy*[374].

Tale apparente riconoscimento del diritto propugnato da Warren e Brandeis, tuttavia, deve essere circoscritto, in quanto il profilo della *privacy* che emerge nella giurisprudenza del primo Novecento è essenzialmente riconducibile a posizioni giuridiche già tutelate dalla tradizione di *common law* precedente, vale a dire il diritto alla tutela del nome e dell'immagine o, ancora, lo sfruttamento non autorizzato a fini commerciali di quest'ultima[375]. Si tratta, cioè, di un coacervo di prerogative riconducibili generalmente al fascio dei diritti della personalità, che già palesavano alcune manifestazioni nel contesto europeo. Ciò che importa, ai fini della trattazione in oggetto, è che questa pretesa rimane confinata all'ambito dei rapporti fra privati e in caso di violazione configura, per dirlo con le categorie del diritto privato europeo continentale, una responsabilità per danno da fatto illecito.

Quanto detto sopra non è secondario, perché la tutela della sfera di riservatezza del singolo si afferma dunque, in questa fase intermedia, al di fuori della sfera costituzionale, in ciò distinguendosi dall'impostazione che progressivamente questa prerogativa va assumendo sulla sponda orientale dell'Atlantico. D'altronde, se quanto illustrato finora sembra in parte alieno a una trattazione dedicata alla tutela del segreto delle comunicazioni, così è solo in apparenza. Infatti, è attraverso la costruzione teorica della *privacy* che il IV Emendamento può essere letto altresì in termini di protezione della riservatezza del contenuto delle comunicazioni fra privati, così superando, come si vedrà di seguito, quell'impostazione originaria secondo la quale la violazione della disposizione del *bill of rights* poteva conseguire soltanto al *trespass* di un bene oggetto della proprietà della persona.

---

[372] *Roberson v. Rochester Folding Box Co.*, 171 U. Y. 538, 64 N.E. 442 (1902).
[373] *N.Y. Civ. Rights Law* §§ 50–51.
[374] *Pavesich v. New England Life Insurance Co.*, 122 Ga. 190, 50 S.E. 68 (1905).
[375] A. Baldassarre, *Privacy e costituzione. L'esperienza statunitense*, Roma, Bulzoni, 1974, 32 ss.

3.4. La tutela del segreto delle comunicazioni telefoniche come paradigma del conflitto fra le diverse concezioni di privacy

Il tema della tutela delle comunicazioni, in specie telefoniche, si afferma nella successiva epoca del proibizionismo, anche in forza della crescente attività in sede penale delle autorità federali, che per l'appunto prevedono reati federali per il contrabbando di liquori o altre bevande alcoliche commesso in frode al divieto stabilito per legge[376]. Se la policy delle autorità di *law enforcement* era quella di astenersi dal ricorso alle intercettazioni (*wiretapping*) come mezzo di ricerca della prova in indagini penali, le prove raccolte a carico del trafficante di alcolici Roy Olmstead erano state ottenute in spregio a tali direttive, intercettando le conversazioni telefoniche in entrata e in uscita dall'ufficio dal quale costui gestiva i propri affari.

La Corte Suprema, dopo aver concesso il *certiorari*, con una decisione di misura si era espressa in favore della legittimità delle prove raccolte con la modalità di cui sopra, basando la propria decisione sul fatto che i dispositivi che trasmettevano il contenuto della chiamata alle autorità investigative erano stati attentamente collocati all'interno dei fili pubblici del telefono che connettevano l'utenza di Olmstead alla rete telefonica. Poiché non vi era stato un *trespass*, cioè l'attività degli agenti di pubblica sicurezza non aveva violato beni di proprietà del destinatario dell'intercettazione, ne discendeva che la fattispecie non era sussumibile sotto il dettato del IV Emendamento[377].

Infatti, secondo la maggioranza, il testo della disposizione, che fa esplicito riferimento alle persone, alle abitazioni e a documenti e carte può ben ritenersi comprendente le lettere e le altre forme di corrispondenza fisica, come peraltro già la stessa Corte Suprema aveva riconosciuto[378], ma non poteva essere interpretato così da includere altresì le comunicazioni telefoniche, che apparvero soltanto decenni dopo l'entrata in vigore del *bill of rights*. Applicando dunque la concezione proprietaria di

[376] *National Prohibition Act 1919*, Pub. L. 66–66, 41 Stat. 305–323.
[377] Le linee principali dell'argomentazione di maggioranza e minoranza sono ricostruite in dettaglio in A. Baldassarre, *op. cit.*, 96-105.
[378] *Ex parte Jackson*, 96 U.S. 727 (1878).

Boyle, l'unico approdo legittimo della decisione della Corte non sarebbe potuto essere che nel senso dell'insussumibilità di un'intercettazione telefonica del tipo in parola sotto la protezione garantita dal IV Emendamento. Una tale protezione avrebbe potuto essere disposta dal Congresso per legge, per esempio rendendo inammissibili nei procedimenti penali le prove così ottenute. Ma una tale estensione non spetterebbe al giudiziario, che si deve attenere all'interpretazione del testo costituzionale così come scritto e interpretato in precedenza[379].

La decisione fu aspramente contestata dalla minoranza, in particolare da quello stesso *Justice* Brandeis che quasi quaranta anni prima aveva avviato il dibattito sull'esistenza di un generale diritto alla *privacy* nel patrimonio giuridico di *common law*. Prima di dare conto di tale opinione, è opportuno altresì segnalare la concisa ma puntuta dichiarazione di *Justice* O.W. Holmes, il quale ritenne che la Corte si trovasse nel caso di specie a dover effettuare una scelta fra due diverse *policies*, essendo così 'slegata' dall'obbligo di attenersi a qualsiasi precedente in materia. Al fine della efficace persecuzione e della cattura di chi commetta condotte di reato, si contrappone il comportamento degli agenti di pubblica sicurezza che ottengono le informazioni rilevanti tramite condotte parimenti vietate dalla legge (quale l'intercettazione telefonica). La scelta del male minore, prosegue Holmes, impone di preferire che alcuni colpevoli riescano a sfuggire alla giustizia rispetto a far compiere alle autorità di governo delle condotte illegittime[380].

L'opinione dissenziente di *Justice* Brandeis, invece, focalizza la propria attenzione sulla peculiarità dell'esercizio interpretativo della Costituzione, sottolineando come sarebbe miope limitare la portata delle disposizioni della stessa al significato che esse potevano assumere al momento della loro approvazione. Infatti, quelle che erano protezioni e garanzie pensate per prevenire gli abusi dei *general warrants* alla fine del diciottesimo secolo impallidiscono dinanzi alla capacità intrusiva che si manifesta per mezzo delle intercettazioni delle conversazioni telefoniche. Se già l'applicabilità del IV Emendamento era stata sancita dalla stessa Corte Suprema federale con riferimento alla corrispondenza epistolare e ai plichi postali, il cui

[379] *Olmstead v. United States*, 277 U.S. 438, 464-466 (1928).
[380] 277 U.S. 470 (1928).

contenuto riservato poteva essere conosciuto solo per effetto della concessione di un mandato specifico a norma della disposizione costituzionale[381], non si vede perché non debba valere lo stesso per la comunicazione telefonica, che è parimenti un servizio pubblico fornito dal governo[382].

D'altronde, prosegue Brandeis, l'esperienza dei Padri Fondatori mostra come la ricerca della felicità menzionata nella Dichiarazione d'Indipendenza non sia necessariamente legata al godimento dei soli beni materiali, poiché il benessere dei cittadini si nutre altresì delle soddisfazioni sotto il profilo morale ed emotivo, che sono per loro natura evidentemente immateriali, ma non per questo non meritevoli di adeguata tutela. Per garantire tale sfera personale, ribadisce Brandeis, i *Founding Fathers* hanno reso opponibile all'autorità di governo il diritto a essere lasciati in pace, che è il diritto insieme più ampio e considerato più di valore dagli uomini civilizzati[383].

3.5. La prima regolazione del wiretapping *negli USA: il* Federal Communications Act *(1934)*

Se la posizione della minoranza esce sconfitta nel caso *Olmsteadt*, la suggestione dell'opinione di maggioranza a che sia il Congresso a regolare la materia si concretizza dopo l'ascesa alla Presidenza da parte di Franklin Delano Roosvelt. Infatti, di lì a poco il legislatore federale introdusse un ampio testo in materia di comunicazioni che, fra gli altri aspetti, vieta indiscriminatamente l'intercettazione di comunicazioni e la divulgazione del contenuto delle stesse da parte di qualunque soggetto[384]. Quale che fosse l'intenzione dei redattori della disposizione, la Corte Suprema federale interpretò fin da subito la disposizione in senso assai rigoroso, ricomprendendo entro i destinatari del divieto altresì i funzionari federali di forze di pubblica sicurezza[385], arrivando fino a dichiarare non ammissibile l'informazione ottenuta tramite l'intercettazione illegale (cd. "frutto dell'albero velenoso")[386].

---

[381] *Ex parte Jackson*, 96 U.S. 727, 733 (1878).
[382] 277 U.S. 438, 472-477 (1928).
[383] *Olmstead v. United States*, 277 U.S. 438, 478 (1928).
[384] §605, Federal Communications Act of 1934.
[385] *Nardone v. United States*, 302 U.S. 379 (1937).
[386] *Nardone v. United States*, 308 U.S. 338 (1939).

È interessante notare come in questi casi, seppur per certi versi involontariamente, la Corte Suprema ottenga in pratica quegli effetti che sarebbero discesi da un'interpretazione del IV Emendamento non più legata al concetto del *trespass* della proprietà, bensì al diritto a essere lasciati in pace invocato da Brandeis. Invero, ciò discende dalla interpretazione rigorosa del testo legislativo, non da un mutamento di atteggiamento mentale dei membri del collegio, tanto che in casi successivi il diritto a contestare il ricorso a forme di intercettazione in violazione della legge federale fu limitato soltanto a coloro che potessero mostrare una lesione di un interesse proprietario da parte dell'autorità che procedeva all'operazione di interferenza[387]. Peraltro, la Corte mutò avviso sull'ammissibilità nei processi dinanzi alle corti statali delle prove raccolte in violazione del *Federal Communication Act* in due pronunce a distanza di soli cinque anni, motivando il mutamento di indirizzo interpretativo con la funzione di conformazione del diritto statale assunto dalla disposizione federale[388].

L'approccio in termini di concezione proprietaria del contenuto del IV Emendamento fu altresì esteso al caso delle microspie installate per l'intercettazione di conversazioni fra presenti, poiché le stesse erano state collocate all'interno di un telefono spia installato sul muro adiacente alla stanza dove si teneva la conversazione oggetto di intercettazione[389]. Anche in questa circostanza non vennero ravvisati gli estremi del *trespass*, scartando altresì la qualificazione dell'attività in termini di intercettazione ai sensi della legislazione federale. Sotto questo secondo profilo, la ragione addotta è quella che la protezione garantita dalla legislazione non si spiega nei confronti del segreto della conversazione, bensì a favore del mezzo di comunicazione. La situazione fu paragonata dalla Corte all'ascolto delle parole pronunciate da un soggetto che si trovi nella stessa stanza di chi stia parlando, non invece l'ascolto occulto di una comunicazione fra soggetti diversi[390].

L'ultimo caso della lunga serie di pronunce che adottano una lettura del IV Emendamento in termini proprietari è di poco precedente alla svolta che si descriverà

[387] *Goldstein v. United States*, 316 U.S. 114 (1942).
[388] *Schwartz v. Texas*, 344 U.S. 199 (1952); *Benanti v. United States*, 355 U.S. 96 (1957).
[389] *Goldman v. United States*, 316 U.S. 129, 134 (1942).
[390] A. Baldassarre, *op. cit.*, 128 ss.

infra e riguardava l'ascolto occulto di conversazioni che si tenevano entro una casa per mezzo di un microfono molto sensibile che, tuttavia, fu appoggiato alle tubature dell'abitazione e, per questa ragione, rese inammissibili tutte le informazioni raccolte in quanto sussumibile in una fattispecie di *trespass* di proprietà privata[391].

3.6. Il dado è tratto: l'avvento della reasonable expectation of privacy *e i suoi limiti*

Dopo che diversi Stati nel corso dei decenni si erano dotati di discipline legislative che autorizzassero operazioni di intercettazione telefonica ai fini di indagine penale, la Corte Suprema si pronunciò sulla legislazione dello Stato di New York, censurando la formulazione della disposizione[392]. Essa mise in luce come una legge che prevedesse la possibilità di fare ricorso a forme di intercettazione delle comunicazioni telefoniche, per poter essere considerata legittima ai sensi del IV Emendamento, dovesse contemplare una verifica dell'esistenza di una *probable cause* da parte di un'autorità indipendente, che la richiesta rivolta al giudice indicasse la fattispecie di reato commessa, il luogo in cui cercare e le persone da arrestare o i beni da porre sotto sequestro, che prevedesse una data per il termine delle operazioni e che venisse notificata (o vi fossero ragioni per non procedere a tale notifica), nonché che fosse redatto un verbale delle operazioni.

A questa rassegna dettagliata degli elementi necessari affinché un'operazione di intercettazione fosse costituzionalmente legittima, seguì la vera rivoluzione nel campo dell'interpretazione del IV Emendamento. Il caso non riguardava, stavolta, l'intercettazione effettuata tramite inserzione di cavi sulle linee telefoniche pubbliche, come avvenuto in passato, bensì riguardava l'apposizione sull'esterno di una cabina telefonica di strumenti che captassero una conversazione[393]. Nonostante le parti in causa avessero focalizzato le proprie prospettazioni della causa sulla qualificazione del luogo in questione come spazio costituzionalmente protetto o meno, l'opinione di maggioranza chiarisce fin da subito che l'impostazione da adottare è differente.

---

[391] *Silverman v. United States*, 365 U.S. 505 (1961).
[392] *Berger v. New York*, 388 U.S. 41 (1967).
[393] *Katz v. United States*, 389 U.S. 347 (1967).

Infatti, sancisce solennemente la Corte, "il IV Emendamento protegge le persone, non i luoghi", tanto che ciò che una persona esponga alla pubblica conoscenza, anche se si trovi in casa propria, decade dalla tutela della disposizione. Diversamente, ciò che ritenga mantenere riservato, anche se si trovi in un'area accessibile al pubblico, può essere costituzionalmente protetto[394]. La Corte afferma poi che una lettura del IV Emendamento che non consideri che chi entri in una cabina telefonica si aspetti che ciò che pronuncia alla cornetta rimanga riservato ignorerebbe il ruolo vitale che il telefono pubblico aveva assunto nelle comunicazioni fra privati.

Ciò che è senz'altro interessante, tuttavia, è che il più famoso lascito del caso *Katz* è contenuto nella breve *concurring opinion* di Justice Harlan, che offre un'interpretazione dell'opinione di maggioranza che associa all'utilizzo della cabina del telefono pubblico una ragionevole aspettativa di riservatezza (*reasonable expectation of privacy*). Tale formula viene spiegata nel senso che le persone giovano della protezione del IV Emendamento laddove abbiano dimostrato di avere una reale aspettativa soggettiva di riservatezza e quando tale aspettativa possa legittimamente essere considerata lecita a livello sociale[395]. L'elemento discriminante, dunque, non sarebbe la natura del luogo (la cabina del telefono è di proprietà pubblica), bensì la presenza di accortezze e l'adeguatezza a garantire la riservatezza della comunicazione che in quella sede abbia luogo. Tale conclusione implicherebbe l'obbligo di ottenere un mandato per procedere a intercettazioni del tipo in questione, a pena di illegittimità dell'attività e quindi di inutilizzabilità degli elementi raccolti.

Il problema principale che emerge a prima vista dall'osservazione del criterio della *reasonable expectation of privacy* risiede nell'incertezza connaturata ad esso. La Corte Suprema si è prodigata nel cercare di attribuire un perimetro più circoscritto a tale aspettativa, talvolta richiedendo che fosse giustificabile[396], altre volte legittima[397] o semplicemente, per l'appunto, ragionevole[398]. Tralasciando in questa sede quanto concerne le perquisizioni e i sequestri in generale ai sensi del IV Emendamento, è

---

[394] 389 U.S. 351.
[395] 389 U.S. 361.
[396] *U.S. v. White*, 401 U.S. 745 (1971).
[397] *U.S. v. Chadwick*, 433 U.S. 1 (1976); *Rakas v. Illinois*, 439 U.S. 128 (1978).
[398] *Terry v. Ohio*, 392 U.S. 1 (1968).

apprezzabile notare che con specifico riferimento alle telecomunicazioni la Corte Suprema abbia sviluppato alcuni criteri che rendono meno nebulosa la determinazione dell'esistenza (o meno) di una ragionevole aspettativa di riservatezza. In particolare, si tratta della cd. *third party exception*, secondo la quale non si può nutrire tale aspettativa protetta dal IV Emendamento quando si svelino determinate informazioni a un soggetto terzo, anche fosse soltanto in forza di disposizioni contrattuali[399].

3.7. Il quadro normativo dopo Katz

È d'uopo dare conto, per quanto sinteticamente, dell'evoluzione del quadro normativo che ha seguito il fondamentale cambio di rotta in *Katz*, non fosse altro perché il terreno sul quale la maggioranza delle controversie in tema di intercettazione di telecomunicazioni vengono risolte è proprio quello dell'interpretazione sul piano legislativo, senza necessità di evocare le tutele di cui al IV Emendamento[400]. In particolare, la disciplina è contenuta nel *Federal Wiretap Act*, altresì noto come *Title III*, in quanto collocato nella terza sezione del cd. *Omnibus Crime Control Act*[401].

Le garanzie in ordine alla riservatezza tradotte in passaggi procedurali da completare prima di poter procedere all'esperimento dell'operazione di intercettazione hanno consentito al testo di resistere a numerose contestazioni dinanzi alle corti federali già nei primi anni dopo la sua entrata in vigore[402]. D'altronde, il processo di autorizzazione prevede: l'ottenimento di apposita autorizzazione da parte del Dipartimento di Giustizia; l'obbligo di dimostrazione che l'intercettazione verrà utilizzata per scoprire elementi di prova di uno dei reati indicati dettagliatamente nel testo; la presentazione di una richiesta che sia corredata da una completa ed esauriente ricostruzione fattuale e una precisa indicazione della natura e della posizione del luogo ove si voglia esperire l'operazione, nonché l'indicazione dell'identità delle persone sottoposte a intercettazione; l'obbligo di dimostrare le ragioni per le quali altri mezzi

---

[399] *United States v. Miller*, 425 U.S. 435 (1976); *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979).
[400] O.S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, in 102 *Mich. L. Rev.*, 2004, 801-888, 851.
[401] Pub. L. 90-351, 82 Stat. 197 (1968).
[402] *United States v. Sklaroff*, 506 F.2d 837, U.S. Court of Appeals for the Fifth Circuit, 4 marzo 1975; *United States v. Ramsey,* 503 F.2d 524, U.S. Court of Appeals for the Seventh Circuit, 6 agosto 1974; *United States v. Martinez*, 498 F.2d 464, U.S. Court of Appeals for the Sixth Circuit, 18 giugno 1974.

di ricerca della prova sarebbero inefficaci; la fornitura al giudice di tutte le richieste di intercettazione presentate in precedenza; l'obbligo di dimostrare la probabilità che l'intercettazione svelerà conversazioni associate a uno dei reati per i quali è possibile procedere a intercettazione; l'obbligo di illustrare il meccanismo attraverso il quale l'autorità procedente minimizzerà l'intrusione nelle conversazioni non attinenti alla condotta di reato. Sussistono inoltre obblighi periodici di documentazione dell'attività e la durata massima non può eccedere i trenta giorni. Entro novanta giorni dal termine delle attività di intercettazione, si deve inoltre procedere alla notifica alle parti interessate.

Si tratta, in tutta evidenza, di disposizioni particolarmente rigorose e che in larga parte 'risparmiano' alle corti il confronto con il testo ben più conciso del IV Emendamento. D'altronde, le corti federali sembrano aver accettato che i mandati ottenuti in forza di autorizzazioni a norma del *Title III* presidino in modo sufficiente la sfera di riservatezza dei singoli individui bersaglio delle operazioni di intercettazione.

Un ulteriore, limitato riferimento è opportuno per quanto riguarda alcune eccezioni alle regole generali in materia di intercettazioni, che sono contenute nel *Foreign Intelligence Surveillance Act* (FISA)[403], che fu approvato per disporre in merito alla sorveglianza di telecomunicazioni per ragioni di sicurezza nazionale, 'liberando' le autorità che perseguano indagini in questo ambito dall'obbligo di presentare elementi che facciano sospettare la commissione di una condotta di reato per poter ottenere l'autorizzazione a predisporre un'intercettazione. Tralasciando in questa sede una trattazione dettagliata dei meccanismi di funzionamento di tale sistema[404], è d'uopo sottolineare come le eccezioni in esso contenute si sono rivelate un pericoloso precedente in quanto poi sfruttate nel primo decennio degli anni 2000 per la lotta al terrorismo, espandendone il perimetro tramite le eccezioni di cui al cd. *Patriot Act*[405].

[403] Pub.L. 95-511, 92 Stat. 1783.
[404] Si rinvia a B.R. Ruiz, *op. cit.*, 242 ss.
[405] Pub.L. 107-56, 115 Stat. 272.

IV. L'avvento delle nuove tecnologie e la crisi del paradigma tradizionale

Sommario: 1. Indagini informatiche e tecnologie digitali. – 1.1. Gli strumenti di controllo a distanza: trojans *e* remote forensic softwares. *– 1.2. La qualificazione giuridica fra sussunzione e categoria* ex novo. *– 1.3. La protezione degli interessi individuali alla riservatezza. – 1.4. L'utilizzabilità delle prove in giudizio. – 1.5. Natura transfrontaliera ed esigenze di coordinamento. – 2. La Germania come precorritrice in campo europeo. – 2.1. I primi tentativi di disciplina della materia a livello statale. – 2.2. La giurisprudenza costituzionale e l'inquadramento del* BVG. *Una prima fase. – 2.2.1 Le disposizioni impugnate e le censure di illegittimità costituzionale. - 2.2.2. Il riconoscimento di un nuovo diritto costituzionale della persona - 2.2.3. L'insufficienza delle garanzie costituzionali preesistenti. - 2.2.4. I limiti all'applicabilità del nuovo diritto della personalità. - 2.2.5. I vizi d'incostituzionalità: il principio di precisione e determinatezza. - 2.2.6. I vizi d'incostituzionalità: lo scrutinio sulla proporzionalità. - 2.2.7. Le deficienze della tutela sotto il profilo procedurale. - 2.2.8. La protezione del nucleo fondamentale della vita privata. – 2.3. Gli sviluppi più recenti della giurisprudenza costituzionale. - 2.3.1. La riproposizione delle disposizioni nella legge antiterrorismo federale. - 2.3.2. Un nuovo giudizio sulla proporzionalità delle misure. - 2.3.3. La necessità delle opportune tutele procedurali e della protezione del nucleo duro del diritto. - 2.3.4. Lo scrutinio concreto sulle disposizioni impugnate. - 2.3.5. I nuovi rilievi sull'intangibile sfera di riservatezza della vita privata. - 2.3.6. Il giudizio sui mezzi di ricerca della prova "insidiosi". - 2.3.7. La modulazione temporale degli effetti e il presidio degli interessi costituzionali individuali. – 3. La tutela dello spazio privato digitale nella giurisprudenza statunitense. – 3.1. L'origine della sorveglianza da remoto: strumenti e strategie delle agenzie di* law enforcement. *- 3.2. La rilettura della* reasonable expectation of privacy *nella recente giurisprudenza federale. - 3.3. La giurisprudenza delle corti inferiori. - 3.4. La giurisprudenza della Corte Suprema. - 3.4.1. La ritrosia nel fronteggiare l'uso della tecnologia nel processo penale. - 3.4.2. Il ritorno a una lettura 'reificata' del IV Emendamento. - 3.4.3. L'ora è giunta: il riconoscimento dell'alterità degli smartphone rispetto agli elementi di prova tradizionali. - 3.4.4. Quali limiti alla* third party exception *nell'era digitale? - 4. La giurisprudenza italiana sull'utilizzo del captatore informatico. - 4.1. Il ruolo di supplenza del giudice di legittimità. - 4.2. Non così in fretta: i distinguo della sentenza Musumeci e le minacce ai diritti costituzionali dei singoli. - 4.3. Un momentaneo punto fermo: il* laissez faire *della sentenza Scurato. - 4.4. Il doppio binario processuale: la perimetrazione degli effetti della pronuncia. - 4.5. La delega parlamentare e la riforma promessa (ma sospesa).*

1. Indagini informatiche e tecnologie digitali.

1.1. Gli strumenti di controllo a distanza: trojans *e* remote forensic softwares

L'esponenziale avanzamento tecnologico degli ultimi decenni ha generato una progressiva transizione dalle forme di comunicazione tradizionali tramite scrittura su supporti fisici (*i.e.*, lettere inviate tramite il sistema postale) a una smaterializzazione del contenuto comunicativo delle conversazioni. Questo passaggio è avvenuto anche a scapito dell'utilizzo della voce come mezzo comunicativo, se si esclude il caso dei cd. messaggi audio registrati, che tuttavia pure non costituiscono una forma di comunicazione del tutto immediata, essendo riprodotti dal destinatario dopo che la registrazione del mittente sia terminata.

Se è indubbio il valore di tali nuovi strumenti a disposizione dei singoli individui, i quali possono raggiungere con maggiore rapidità e agio gli uni gli altri azzerando la distanza fisica mediante l'utilizzo della rete di telefonia mobile e, soprattutto, della rete Internet, non bisogna dimenticare che lo sviluppo di tecnologie innovative si presta altresì all'utilizzo in ambito di indagine penale, finalizzato alla prevenzione e alla repressione delle condotte di reato. Tale ultima considerazione vale *a fortiori* in un contesto storico in cui la spinta al sacrificio delle prerogative individuali a favore della tutela della sicurezza collettiva è vista con un favore crescente dalla pubblica opinione, nonostante il (fondato) scetticismo della comunità giuridica[406].

La riflessione sull'adeguatezza delle soluzioni giuridiche tradizionali nell'ambito del processo penale e sull'opportunità e il grado di limitazione dei diritti in gioco (con risposte eterogenee negli ordinamenti *infra* considerati) non può in ogni caso prescindere dalla preliminare e necessaria identificazione della natura e del funzionamento (o, almeno, delle modalità di impiego astrattamente disponibili) degli strumenti di cui sopra.

L'analisi condotta in questa sede prende in considerazione esclusivamente le investigazioni occulte e non anche quelle palesi (ispezioni, perquisizioni e sequestri informatici), poiché è ben evidente la maggior potenzialità lesiva della segretezza di un contenuto comunicativo che possa derivare dalle prime. Questa categoria generale è omnicomprensiva e necessita di una ulteriore classificazione, a norma della quale è opportuno distinguere le intercettazioni telematiche, l'utilizzo di cd. *malware* o strumenti invasivi analoghi per funzionamento e ogni tipo di attività che implichi un

[406] G. Giostra, *Prima lezione sulla giustizia penale*, Bari-Roma, Laterza, 2020, 19 ss.

accesso a un sistema o dispositivo informatico all'insaputa del proprietario oppure sistemi *hardware* e *software* diffusi da remoto a fini di raccolta ed elaborazione di dati digitali (per i quali è stata proposta la qualificazione generale di *remote forensic softwares*[407]).

Parimenti, se non addirittura più rilevante è la differenza fra le attività di captazione occulta che si limitano a prendere cognizione del contenuto delle comunicazioni (le intercettazioni telematiche) e quelle che invece hanno natura attiva, ben potendo, una volta penetrato il sistema *target*, assumerne il controllo e attivarne funzionalità autonomamente, senza il concorso dell'utilizzatore del dispositivo (i captatori informatici o *malware*)[408].

La prima categoria è dunque costituita dagli strumenti di *online search*, che si limitano cioè a raccogliere i dati senza alterare in alcun modo il sistema *target*. Oltre alle intercettazioni telematiche (su cui v. supra, Cap. II, §4) esistono anche *malware* di questa natura, ossia programmi spia che permettono di estrarre una copia integrale (o, eventualmente, anche solo parziale) dei dati memorizzati dal sistema che si penetra; cioè consente la trasmissione agli inquirenti all'insaputa dell'utilizzatore del dispositivo. Il ricorso a questi strumenti, tuttavia, non altera in modo significativo il paradigma tradizionale dell'intrusione dello Stato nell'ambito della sfera di segretezza delle comunicazioni del singolo.

Diversamente, la seconda categoria include tutte le modalità cd. di *online surveillance*, tramite le quali chi inocula il virus informatico nel dispositivo è in grado di prendere conoscenza in tempo reale di tutti i dati che vengono trasmessi in ogni momento dalle periferiche (tastiera, fotocamera, microfono, ma anche ciò che viene visualizzato sul *display*) al processore (e, quindi, alla memoria) del dispositivo *target*. Il *software* spia può essere installato con due diverse modalità: se si riesce ad accedere al dispositivo oggetto dell'attività di monitoraggio, l'installazione avviene intervenendo direttamente sull'*hardware*; diversamente, se non vi è modo di disporre

---

[407] A. Wiebke, *Agents, Trojans and tags: The next generation of investigators*, in 23 *International Review of Law, Computers & Technology*, 1-2, 2009, 99-108, 100.

[408] La classificazione è tratta da F. Palmiotto, *Le indagini informatiche e la tutela della riservatezza informatica*, in *La legislazione penale*, 1 luglio 2019, 3, disponibile all'url: http://www.lalegislazionepenale.eu/wp-content/uploads/2019/06/Palmiotto-rubrica-speciale-Finale.pdf (ultimo accesso: 22 gennaio 2020).

del sistema *target*, l'inoculazione del malware richiede necessariamente la collaborazione (involontaria) dell'utilizzatore, il quale scarica il programma spia aprendo un collegamento ipertestuale, un messaggio di testo o un *file* di aggiornamento mascherato[409].

L'insidiosità di questo strumenti d'indagine, tale da far loro meritare comunemente l'appellativo di *trojans* o *trojan horses*[410], consente di prendere cognizione anche delle comunicazioni che avvengono tramite canali che si avvalgono della tecnologia *VoIP* (*Voice-over-Internet-Protocol*), che permette di crittografare il contenuto, rendendolo così in buona sostanza inaccessibile ai terzi che non abbiano accesso diretto al dispositivo[411].

La straordinaria gamma di potenzialità di questi strumenti impone di verificare se i sistemi processuali esistenti siano in grado di assorbire tali novità entro il tessuto normativo vigente.

1.2. La qualificazione giuridica fra sussunzione e categoria ex novo.

Una volta tracciato il perimetro dei mezzi di ricerca della prova rilevanti, è d'uopo interrogarsi sull'opportunità di ricondurre i summenzionati strumenti, tramite una tradizionale operazione sussuntiva, sotto le fattispecie astratte previste dalla disciplina processual-penalistica nel nostro e in altri ordinamenti.

Adottando l'ottica di diritto italiano, il primo mezzo di ricerca della prova a cui pare si possano accostare per analogia le operazioni in commento è la perquisizione (in Italia disciplinata dagli artt. 247 ss. del codice di rito). Tuttavia, questa ultima categoria di attività insiste sulla persona o su un luogo fisico, mentre quelle di cui sopra

---

[409] Su natura e funzionamento dei *malware* sopra descritti, v. M. Torre, *Il* virus *di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali*, in *Diritto penale e processo*, 9, 2015, 1163-1172, 1164.
[410] Tale appellativo deriva, come evidente, dal notissimo espediente del cavallo di legno utilizzato dai Greci su suggerimento di Ulisse per espugnare la città di Troia assediata infruttuosamente per dieci anni. Dell'episodio dà conto l'esule troiano Enea nel libro II dell'Eneide di Virgilio, in occasione della narrazione che lo stesso fa della caduta della città alla regina cartaginese Didone.
[411] B. Cupa, *Trojan horse resurrected - On the legality of the use of government spyware*, in C. Webster-R. William, *Living in surveillance societies: The state of surveillance,* Proceedings of LiSS conference 3. 978-1484049082: CreateSpace Independent Publishing Platform, 2013, 419-428, 420, disponibile all'url: https://www.zora.uzh.ch/id/eprint/81157/1/Cupa_Living_in_Surveillance_Societies_2012.pdf (ultimo accesso: 22 gennaio 2020).

riguardano un luogo digitale, *i.e.* i dati memorizzati dal dispositivo, che, siano essi localizzati su una scheda interna o su un server esterno (come nel caso del *cloud*), sono cosa ben diversa dal corpo delle persone fisiche o dagli ambienti e dai luoghi. Inoltre, mentre queste sono preordinate alla ricerca del corpo del reato o di cose pertinenti al reato stesso (sottoposte a sequestro in caso di ritrovamento), non altrettanto si può dire per le attività di sorveglianza occulta *online*, le quali, peraltro, non sono note alla persona interessata, che invece se ne avvede nel momento in cui vengono eseguite le perquisizioni tradizionali (godendo quindi di una serie di garanzie procedimentali, fra le quali l'assistenza di un legale rappresentante)[412].

Se quanto premesso rende poco convincente la sussunzione della sorveglianza occulta tramite programmi spia sotto l'istituto processuale della perquisizione (anche qualora la stessa sia riferita a sistemi informatici o telematici), pare naturale volgere lo sguardo alla fattispecie delle intercettazioni (su cui v. *supra*, Cap. II, §§ 2-4). Entrambe le categorie di attività, infatti, condividono la necessità di mantenere il soggetto destinatario dell'attività d'indagine ignaro dello svolgimento della stessa, a pena della frustrazione della riuscita della stessa. Vale la pena sottolineare come la difficoltà di sussumere sotto una fattispecie già disciplinata dal legislatore le attività d'indagine svolte tramite *software* spia riguarda esclusivamente quelle operazioni che esorbitano dalla mera captazione di conversazione fra utenti che si avvalgano dell'infrastruttura offerta dalla rete Internet. Se questo fosse il caso, d'altronde, di altro non si tratterebbe che di intercettazioni informatiche o telematiche (v. *supra*, Cap. II, §4), in ordine alle quali il legislatore ha già disposto, prevedendo requisiti e sanzionandone il mancato rispetto con l'inutilizzabilità in sede processuale (cfr. artt. 266-*bis* e 271, c.1. c.p.p.)[413].

Come si vedrà in seguito, la giurisprudenza di legittimità italiana ha ritenuto di sussumere la sorveglianza tramite *software* spia del tipo captatore informatico sotto la figura tipica dell'intercettazione tra presenti (SS.UU. Scurato, v. *infra*, §4.3).

Non soccorre a fini classificatori neppure il mezzo di ricerca della prova dell'ispezione: a esso si ricorre infatti allorquando si ritenga necessario cristallizzare, tramite la ricerca di oggetti analoghi a quelli per i quali si autorizza la perquisizione,

---

[412] S. Marcolini, *Le cosiddette perquisizioni on line (o perquisizioni elettroniche)*, in *Cass. Pen.*, 7-8, 2010, 2855-2868, 2858 ss.
[413] *Ibid.*, 2859.

una situazione di fatto suscettibile di alterazione nel corso del tempo; diversamente, l'utilizzo di un programma spia agisce tipicamente su un arco di tempo prolungato e non può essere conciliato con gli obblighi di informazione e le garanzie di assistenza legale da cui è presidiata l'attività di ispezione[414].

Se la sintetica trattazione di cui sopra esclude di poter ricondurre a uno dei mezzi di ricerca della prova tipizzati dal codice di procedura penale italiano (oltre che dalla Costituzione) le attività di indagine svolte tramite programmi spia, non ne segue necessariamente la conseguenza dell'inammissibilità delle stesse nell'ordinamento processuale italiano. Infatti, tanto la dottrina quanto la giurisprudenza processual-penalistica hanno ritenuto esistere un principio di aticipità nell'ambito delle indagini preliminari, a norma del quale il novero di attività a disposizione dell'autorità inquirente in tale fase del procedimento penale non è esaurita dagli atti tipici descritti in precedenza[415].

Vi è stato però chi ha addirittura avanzato dei dubbi sulla legittimità costituzionale della prova ottenuta tramite captatore informatico, poiché anche la prova atipica deve essere costituzionalmente legittima e, quindi, rispettare anche i requisiti previsti dalla giurisprudenza CEDU[416]. Peraltro, questa ricostruzione viene meno nel momento in cui, come è avvenuto con il cd. decreto Orlando, si mette mano al tessuto normativo introducendo una fattispecie *ad hoc* per legge.

Ciò apre la strada al ricorso a un ampio armamentario tecnologico, del quale le autorità investigative potrebbero fare uso nell'attività di prevenzione e repressione dei reati. Per tale ragione è opportuno che l'analisi sull'ammissibilità di un'attività particolarmente intrusiva nei confronti delle prerogative individuali non rimanga feudo esclusivamente della riflessione processual-penalistica, ma sia altresì presidiata

---

[414] *Ibid.*, 2860.

[415] *Ex multis*, Cass. pen., sez. II, 27 marzo 2008, n. 16818, che ricomprende il riconoscimento fotografico fra quegli atti di indagine che la polizia giudiziaria ritiene necessario svolgere per individuare l'autore del reato o l'individuazione del colpevole, i quali rispondono generalmente al canone dell'atipicità, desunto dal combinato disposto degli artt. 55 e 348 c.p.p.; v. anche S. Signorato, *La localizzazione satellitare nel sistema degli atti investigativi*, in *Rivista italiana di diritto e procedura penale*, 2, 2012, 580-607, in particolare 587-589, con riferimento alla localizzazione tramite tecnologia GPS.

[416] F. Iovene, *Le c.d. perquisizioni online tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *DPC*, 3-4/2014, 341.

e approfondita sotto il profilo della compatibilità della stessa con le posizioni giuridiche soggettive riconosciute a norma del dettato costituzionale.

1.3. La protezione degli interessi individuali alla riservatezza.

La rilevanza concreta del ricorso a mezzi di ricerca della prova che richiedono il monitoraggio di sistemi e reti informatiche, così mettendo a rischio la segretezza delle comunicazioni che su tali canali transitano e la riservatezza dei dati degli utenti che adottano tali modalità di comunicazione, è testimoniata dagli impegni assunti dagli Stati membri del sistema del Consiglio d'Europa con la firma e l'entrata in vigore della *Convenzione sul crimine informatico* (su cui v. anche *supra*, Cap. III, §1.1)[417].

Le disposizioni di cui si è dato conto in precedenza specificano che i poteri di intrusione nella sfera di riservatezza personale e di segretezza delle comunicazioni degli utenti sono in ogni caso soggette alle previsioni di cui agli artt. 14 e 15 della Convenzione. Particolare interesse ai fini della trattazione in oggetto riveste la seconda disposizione, a norma della quale ciascuna parte contraente deve assicurare che l'introduzione, l'attuazione e l'applicazione di tali poteri pubblici siano conformi alle garanzie previste dal diritto domestico dello Stato. Esso, afferma l'articolo in questione, dovrebbe prevedere un adeguato grado di protezione dei diritti e delle libertà dell'uomo, ivi inclusi quelli derivanti dall'adesione alla Convenzione EDU, al Patto internazionale sui diritti civili e politici o a ogni altra fonte di diritto internazionale sui diritti umani, oltre a contemplare il principio di proporzionalità[418]. Il testo aggiunge altresì che tali garanzie dovrebbero includere una supervisione da parte di un organo giurisdizionale o comunque indipendente, un obbligo di illustrazione delle ragioni che giustifichino il ricorso a tali poteri e una limitazione dell'ambito di applicazione e della durata degli stessi[419].

Stante la compresenza di due categorie valoriali che, almeno in questo ambito, sono in reciproca concorrenza e, pertanto, richiedono un adeguato bilanciamento per

[417] Il trattato è altresì detto Convenzione di Budapest, dal nome della capitale magiara dove il testo è stato firmato il 23 novembre 2001.
[418] Art. 15, §1 *Convenzione sul crimine informatico* di Budapest.
[419] Art. 15, §2 *Convenzione sul crimine informatico* di Budapest.

limitare i sacrifici dell'una e dell'altra, il suddetto principio di proporzionalità assume un ruolo centrale, tanto da essere l'unico criterio esplicitamente menzionato nel testo della Convenzione. Il rapporto esplicativo del contenuto del trattato precisa come esso vada attuato in conformità alle regole generali in materia del diritto interno di ciascuno Stato. Tuttavia, per gli Stati membri del Consiglio d'Europa, si prescrive che il contenuto dello stesso debba derivare dalle disposizioni della Convenzione EDU come interpretate dalla Corte di Strasburgo. Inoltre, il medesimo principio andrebbe applicato conformemente alla legislazione e alla giurisprudenza nazionale. Diversamente, per gli altri Stati firmatari della Convenzione di Budapest, si dispone che siano soltanto i principi di diritto interno a valere quali limitazioni all'eccessiva intrusività delle ordinanze di produzione in giudizio di elementi di prova, affiancati da requisiti di ragionevolezza per perquisizioni e sequestri[420].

Quanto previsto dall'art. 15 della Convenzione di Budapest si salda idealmente con la previsione dell'art. 52, c.1 della Carta dei diritti fondamentali dell'Unione Europea, a norma del quale le limitazioni ai diritti sanciti dalla Carta stessa (su cui v. *supra*, Cap. III, §1.3), in ossequio al principio di proporzionalità, possono essere disposte soltanto ove necessarie ed effettivamente rispondenti a finalità di interesse generale riconosciute dall'UE o in quanto volte alla tutela di diritti o libertà di terzi. Peraltro, anche la recente direttiva 680/2016 sul trattamento dei dati personali a fini investigativi, pur sottolineando la necessità che il trattamento dei dati a tali scopi debba essere lecito, corretto e trasparente e perseguire fini specificamente previsti dalla legge, precisa che tali obblighi non pregiudicano lo svolgimento di attività d'indagine per la prevenzione e il perseguimento dei reati, a patto che si tratti di misure necessarie e proporzionate in una società democratica[421].

Il riferimento al principio di proporzionalità come chiave di volta per realizzare un equo bilanciamento fra i diversi valori in gioco si riscontra tanto nella

---

[420] § 146, *Explanatory Report to the Convention on Cybercrime*, CETS 185, disponibile all'url: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b (ultimo accesso: 6 febbraio 2020).

[421] Cons. 26, Direttiva (Ue) 2016/680 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

giurisprudenza europea[422] quanto in quella convenzionale[423] in materia di trattamento dei dati personali, anche qualora raccolti a fini di indagine penale, così proponendosi come criterio al quale ispirarsi anche relativamente agli sviluppi più recenti in tema di sorveglianza e monitoraggio occulto del contenuto delle comunicazioni in ambito investigativo[424].

1.4. L'utilizzabilità delle prove in giudizio.

Un aspetto meritevole di considerazione, seppur tendenzialmente pertinente all'ambito processual-penalistico, è quello della legittimità delle operazioni di raccolta degli elementi di prova tramite sorveglianza occulta mediante strumenti digitali e, di conseguenza, della determinazione dei casi di (in)utilizzabilità degli stessi. In particolare, le indagini condotte tramite programmi spia del tipo di cui si è detto in precedenza complicano il quadro rispetto alle indagini tradizionali svolte su sistemi informatici.

Infatti, nel caso di queste ultime le autorità inquirenti procedono usualmente a porre sotto sequestro il dispositivo fisico su cui si presume siano localizzati i dati utili alla persecuzione in sede penale di una condotta di reato, così potendo estrarne copia, evitando di alterare l'esemplare originale e potendo sempre procedere a una comparazione in un momento posteriore. Diversamente, il *software* spia agisce da remoto e, per quanto possa trasmettere dati a chi lo controlla, interagisce con il dispositivo causando una irrimediabile (per quanto consapevole e, anzi, voluta) alterazione del sistema informatico in questione. Quanto premesso pone una non trascurabile questione di preservazione dell'autenticità degli elementi di prova

---

[422] Cause riunite C-293/12 e C-594/12, Corte di Giustizia dell'Unione Europea (Grande Camera), 8 aprile 2014, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlanda, The Attorney General* e *Kärntner Landesregierung, M.S., C.T. e a.*, §§ 45 ss; Cause riunite C-203/15 e C-698/15, Corte di Giustizia dell'Unione Europea (Grande Camera), 21 dicembre 2016, *Tele2 Sverige AB c. Post- och telestyrelsen* e *Secretary of State for the Home Department c. T.W., P.B., G.L.*, §§ 94-96, 116 ss.

[423] *Trabajo Rueda c. Spagna*, no. 32600/12, Corte EDU, III Sez., 30 maggio 2017, §§ 42-48.

[424] Per una riflessione sul tema, con richiami all'esperienza comparata e una particolare attenzione alla giurisprudenza, v. F. Nicolicchia, *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, in *Diritto Penale Contemporaneo*, 2, 2018, 177-189.

raccolti, che può revocare in dubbio l'ammissibilità di tali prove nel processo (così di fatto vanificando l'attività precedente e il sacrificio dei diritti individuali già avvenuto)[425].

La prima giurisprudenza sul piano comparato in tema di *software* spia ha effettivamente mostrato un certo scetticismo sull'affidabilità delle prove raccolte tramite questi strumenti, in particolare nei processi con giuria in sistemi di *common law*[426]. Diversamente, vi è chi ha sostenuto che la discrezionalità del giudice (togato) sull'ammissibilità degli elementi di prova comune alla generalità dei sistemi di *civil law* possa prevenire il rigetto di quanto ottenuto tramite captazione informatica occulta[427].

Se il tema dell'ammissibilità delle prove in giudizio e della loro utilizzabilità rimane senz'altro 'provincia' del diritto processuale penale, non è questione del tutto indifferente alla riflessione in chiave costituzionale sui limiti da imporre a tali strumenti per la tutela delle prerogative individuali.

1.5. Natura transfrontaliera ed esigenze di coordinamento.

Quanto premesso è necessariamente una semplificazione che non tiene conto di un elemento potenzialmente in grado di alterare lo scenario precedentemente illustrato: i dispositivi sui quali i programmi spia possono essere inoculati sono infatti nella maggioranza dei casi mobili, perciò suscettibili di viaggiare insieme ai loro utilizzatori e superare i confini di Stato. Ciò impone di considerare la legittimità di attività invasive del tipo in parola quando controllate dall'autorità pubblica di un Paese su un dispositivo fisicamente localizzato in un Paese terzo.

Per disinnescare tale cortocircuito giuridico, sarebbe necessario ottenere il consenso dello Stato in cui tale attività di sorveglianza occulta ha luogo; ciò può avvenire in due forme: o con un'autorizzazione generale contenuta in un accordo (trattato) internazionale bi- o plurilaterale, oppure tramite un provvedimento *ad hoc*

---

[425] W. Abel, *op. cit.*, 105-106.
[426] È il caso di quanto avvenuto nel Regno Unito nella controversia *Regina v. Aaron Caffrey*, Southwark Crown Court, 17 Ottobre 2003; v. E. George, *UK Computer Misuse Act – The Trojan Virus Defence. Regina v Aaron Caffrey, Southwark Crown Court, 17 October 2003*, in 1 *Digital Investigation*, 2, 2004, 89.
[427] W. Abel, *op. cit.*, 106.

relativo a un'indagine specifica e ben individuata (con evidenti complicazioni e ritardi rispetto all'ipotesi più sistematica di cui sopra). Peraltro, la situazione può essere complicata dalla previsione di requisiti fra i quali il rispetto dei principi della legislazione in materia dello Stato terzo in cui il dispositivo viene trasportato e dalla necessità di ricorrere a canali diplomatici per ottenere tali autorizzazioni, anziché muoversi su un piano orizzontale tramite un contatto stabilito fra le autorità inquirenti dei Paesi interessati[428].

D'altra parte, forme di cooperazione a livello internazionale fra gli Stati divengono sempre più necessarie in ragione del fatto che lo spazio informatico e digitale appare per sua natura refrattario alle limitazioni territoriali.

2. *La Germania come precorritrice in campo europeo.*

2.1. I primi tentativi di disciplina della materia a livello statale.

Un interessante dibattito sul tema dell'intrusività delle indagini penali digitali si è sviluppato a partire circa dalla metà del primo decennio del XXI secolo in Germania. Tale discussione traeva origine dal rigetto da parte della Corte di Giustizia Federale (*Bundesgerichtshof*, BGH) della richiesta di un procuratore statale che chiedeva la concessione di un mandato per effettuare una ricerca da remoto sul computer di un sospettato in un'indagine di terrorismo internazionale tramite l'installazione all'insaputa del proprietario di un programma spia simile al tipo *trojan*[429]. Il rigetto fu fondato dal disaccordo del BGH con l'argomentazione del procuratore, a parer del quale era possibile fondare un'analogia fra la tradizionale ricerca di elementi di prova in un luogo fisico e una ricerca segreta su un sistema informatico[430]. Tuttavia, l'argomentazione del BGH si basava sull'assenza di un'apposita legislazione, senza la

---

[428] *Ibid.*, 107.

[429] W. Abel-B. Schafer (trad. it. a cura di A. Piccinin), *La decisione della Corte Costituzionale tedesca sul diritto alla riservatezza ed integrità dei sistemi tecnologici d'informazione – un rapporto sul caso BVerfGE, NJW 2008, 822*, in *JEI – Jus e Internet*, 15 novembre 2009, §2, disponibile all'url: https://www.jei.it/approfondimenti-giuridici/23-la-decisione-della-corte-costituzionale-tedesca-sul-diritto-alla-riservatezza-ed-integrita-dei-sistemi-tecnologici-d-informazione-un-rapporto-sul-caso-bverfge-njw-2008-822 (ultimo accesso: 18 aprile 2020).

[430] BGH, 31 gennaio 2007, StB 18/06. Cfr. G. Vaciago, *Remote Forensics and Cloud Computing: An Italian and European Legal Overview*, in 8 *Digital Evidence & Elec. Signature L. Rev.*, 2011, 127.

quale la concessione del mandato avrebbe potuto essere considerata eccessivamente discrezionale; ciò lasciava aperta la porta all'eventuale futura introduzione di nuovi poteri di perquisizione e sequestro non previsti in precedenza[431].

A seguito di questa pronuncia e del dibattito che la stessa aveva innescato, il *Land* della Renania Settentrionale-Vestfalia approvò delle modifiche alla cd. *Legge per la protezione della Costituzione*[432], la quale venne a includere alcune disposizioni rilevanti ai fini della trattazione in oggetto. In particolare, il §5, c.2, n. 11 conferiva a un organismo (*rectius*, un'agenzia) di *intelligence* "a protezione della Costituzione" (*Verfassungsschutzbehörde*) il potere di effettuare indagini tramite monitoraggio e ricognizione segreta di Internet o accesso segreto a sistemi informatici[433]. Si trattava del primo caso di riconoscimento di poteri cd. di *Online Durchsuchung* (lett. "perquisizione in rete") a una pubblica autorità nel Paese, in un momento in cui, peraltro, si era ipotizzato di conferire tali poteri all'Ufficio Federale di Polizia con competenza penale (*Bundeskriminalamt*), in attuazione della competenza da poco attribuita alla Federazione stessa in materia di prevenzione dei pericoli connessi al terrorismo internazionale (Art. 73, n. 9a, *Grundgesetz*).

2.2. La giurisprudenza costituzionale e l'inquadramento del BVG. Una prima fase

2.2.1 Le disposizioni impugnate e le censure di illegittimità costituzionale

La controversa disposizione di cui alla *Legge per la protezione della Costituzione* del *Land* Renania Settentrionale-Vestfalia è stata fin da subito oggetto di critiche da parte di una pluralità di soggetti, che ne hanno contestato la legittimità costituzionale impugnandola dinanzi al Tribunale Costituzionale Federale. I giudici di Karlsruhe hanno deciso il ricorso nel febbraio 2008, con una pronuncia storica che ha riconosciuto la sussistenza di un vizio di illegittimità costituzionale nel testo in questione e,

---

431 W. Abel-B. Schafer, *The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems - A Case Report on BVerfG, NJW 2008, 822*, in 6 *SCRIPTed*, 1, 2009, 106-123, in particolare 107-108.

432 *Gesetz über den Verfassungsschutz in Nordrhein-Westfalen*, come emendata il 20 dicembre 2006 dalla *Gesetz zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen* (Gazzetta delle leggi e ordinanze della Renania Settentrionale-Vestfalia (GVBl NW) 2006, p. 620).

433 R. Flor, *Brevi riflessioni a margine della sentenza del BundesVerfassungsGericht sulla cd. Online Durchsuchung*, in *Riv. Trim. Dir. Pen. Econ.*, 3, 2009, 695-716, in particolare 699.

contestualmente, ha sancito l'esistenza di un nuovo e inedito diritto costituzionalmente garantito[434].

Lo scrutinio di legittimità costituzionale è stato avviato dall'iniziativa di un giornalista, un membro locale del partito di sinistra *Die Linke* e due avvocati soci di uno studio legale che assisteva un richiedente asilo in Germania: tutti costoro condividevano, seppur per ragioni diverse, la soggezione alle attività dell'Ufficio per la protezione della Costituzione del *Land*. La doglianza dei ricorrenti consisteva nell'allegazione secondo la quale la disposizione oggetto del giudizio di legittimità costituzionale, poiché prevedeva un intervento sulle infrastrutture comunicative della rete Internet, regolava una forma di limitazione della segretezza delle telecomunicazioni, protetta dall'art. 10 GG. L'accesso occulto a sistemi informatici sarebbe stato altresì configurabile, a opinione dei ricorrenti, come una limitazione della libertà di domicilio di cui all'art. 13 GG, in specie ove il dispositivo in questione si trovi in un luogo di privata dimora. Ulteriori vizi di illegittimità costituzionale censurati furono l'asserita insussistenza di alcuna delle fattispecie alle quali sono accordate eccezioni a norma dello stesso art. 13 GG, nonché la mancata menzione del diritto il cui contenuto fosse limitato, conformemente a quanto previsto dall'art. 19, c.1 GG.

Il *BVerfG* si cura fin dal principio della pronuncia di distinguere chiaramente le due modalità di misure investigative che la legge impugnata contempla. Da un lato, le autorità del *Land* hanno facoltà di svolgere ricognizioni di varia natura sulla rete Internet, ottenendo informazioni sia da siti liberamente accessibili dagli utenti sia tramite la partecipazione a piattaforme di messaggistica, che promuovano aste o che favoriscano transazioni commerciali, ivi compresi i contenuti rintracciabili soltanto nel cd. *dark web*. Dall'altro lato, le medesime autorità possono accedere in segreto a sistemi informatici mediante specifiche tecniche di infiltrazione, attività che è stata ricompresa nella categoria generale della "*online search/online surveillance*" e che, dà conto la sentenza, è già stata posta in essere in alcuni casi isolati dalle autorità federali, pur in

[434] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, § 8, nella trad. in lingua inglese disponibile all'url: https://www.bundesverfassungsgericht.de/SharedDocs/Downloads/EN/2008/02/rs20080227_1bvr037007en.pdf?__blob=publicationFile&v=5 (ultimo accesso: 7 febbraio 2020). Per una traduzione (parziale) in lingua italiana della pronuncia v. R. Flor, *La sentenza del* BundesVerfassungsGericht *del 27 febbraio 2008 sulla cd.* online durchsuchung, in *Riv. trim. dir. pen. econ.*, 3, 2009, 679-694.

mancanza di un riconoscimento normativo di tale potere. La pronuncia del BGH di cui si è detto *supra* ha dissuaso gli uffici inquirenti dal ricorso a tali strumenti nel periodo intercorso fra le due pronunce, rimettendo di fatto la decisione sulla questione di diritto al solo Tribunale Costituzionale Federale[435].

Le ragioni addotte per giustificare la particolare intrusività delle suddette tecniche di indagine furono le difficoltà associate alla prevenzione delle condotte terroristiche, per la cui organizzazione ed esecuzione il ricorso alle tecnologie informatiche è sempre più frequente. In particolare, la decrittazione delle comunicazioni fra sistemi informatici rende quasi impossibile il monitoraggio delle attività criminose da parte di tali gruppi, motivo per cui l'infiltrazione del sistema *target* tramite un programma spia, sempre ammesso che si riesca a portare a termine in concreto, offre una serie di rilevanti vantaggi rispetto alle forme di investigazione tradizionali. Più nello specifico, a differenza di una perquisizione in un luogo di dimora o abitazione, nel caso dell'infiltrazione del sistema informatico il soggetto bersaglio non ha contezza, per il futuro, della conoscenza da parte della pubblica autorità dei dati che transitano sul proprio dispositivo; inoltre, i dati archiviati in forma crittografata potrebbero essere raccolti in forma de-crittata, così da poterne conoscere il contenuto[436].

2.2.2. Il riconoscimento di un nuovo diritto costituzionale della persona

Il Tribunale di Karlsruhe sanziona entrambe le modalità di indagine previste dalla summenzionata legge della Renania Settentrionale-Vestfalia, con ciò sancendo l'emersione di un nuovo diritto costituzionalmente garantito e afferente alla sfera dei diritti della persona. In particolare, il §5, c.2, n. 11 non è ritenuto conforme ai principi sanciti dalla Legge fondamentale in quanto viola il diritto alla personalità nella sua particolare manifestazione come diritto fondamentale alla garanzia della confidenzialità e dell'integrità dei sistemi informatici. Se il riferimento al diritto alla personalità non è inedito, in quanto si ritiene che esso possa essere derivato dal

[435] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, §§ 3-7.
[436] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, §§ 9-11.

combinato disposto degli artt. 2.1 (diritto al libero sviluppo della personalità di ciascuno) e 1.1 (inviolabilità della dignità umana) GG, si tratta invece della prima circostanza in cui il giudice delle leggi tedesco declina tale prerogativa individuale nell'ambito delle tecnologie informatiche e digitali.

In questa accezione, il diritto alla personalità si aggiunge alle garanzie di cui agli artt. 10 (inviolabilità della segretezza della corrispondenza) e 13 (inviolabilità del domicilio) GG, laddove il contenuto di tali disposizioni non offra sufficienti garanzie alla protezione degli interessi dei singoli. Tale formula ampia tutela quegli elementi della personalità che non sono oggetto di una specifica garanzia costituzionale esplicitata nella Legge fondamentale, senza che ciò valga a sancirne un rango inferiore nella determinazione della personalità dell'individuo. Richiamando la propria giurisprudenza precedente, il *BVerfG* riconosce la natura di clausola di chiusura della disposizione stessa, finalizzata a contrastare le nuove minacce che si possano manifestare con il progresso tecnologico e scientifico[437].

Il Tribunale Costituzionale Federale dedica un certo spazio alla sottolineatura della sempre maggior rilevanza assunta dall'uso delle tecnologie informatiche per l'esplicazione della personalità e lo sviluppo dell'individuo, focalizzando l'attenzione in particolare sulla nascita delle infrastrutture di rete che hanno contribuito a un progressivo spostamento delle comunicazioni dagli strumenti tradizionali alla rete Internet. In un tale contesto, i sistemi informatici in questione creano, gestiscono e immagazzinano una serie di dati, siano essi provenienti direttamente da input degli utenti o creati in automatico dai sistemi stessi sulla base dell'utilizzo del dispositivo in questione da parte dell'utente. La raccolta seriale di questi dati può dunque consentire, anche a terze parti, una forma di "profilazione" della personalità del soggetto, rischio che è acuito dalla sempre maggior connessione reciproca dei sistemi informatici, i quali non sempre è possibile schermare avverso l'accesso non autorizzato a fini di estrazione di dati prodotti o archiviati dal sistema stesso[438].

[437] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, §§ 168-169.
[438] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, §§ 170-180.

2.2.3. L'insufficienza delle garanzie costituzionali preesistenti

Il *BVerfG* illustra in seguito le ragioni che fondano il riconoscimento di un diritto all'integrità e confidenzialità dei sistemi informatici, a partire dall'insufficienza delle garanzie contemplate dalle disposizioni della Legge Fondamentale relative alla tutela del segreto delle comunicazioni e dell'inviolabilità del domicilio e dalle declinazioni del diritto alla personalità a favore delle quali la giurisprudenza degli stessi giudici di Karlsruhe aveva già riconosciuto copertura costituzionale[439].

In particolare, il Tribunale Costituzionale Federale sottolinea come la protezione del segreto delle comunicazioni a norma dell'art. 10 GG si applica in ogni circostanza ove avvenga una telecomunicazione, in qualsiasi forma essa si manifesti e tramite qualunque mezzo. Peraltro, tale garanzia si estende anche ai cd. dati esteriori del flusso comunicativo (vale a dire mittente e destinatario della comunicazione, frequenza dei contatti, etc.). Non si pongono, dunque, questioni nuove quando l'attività svolta dall'autorità pubblica si limiti a un "ascolto" o più generica "intercettazione" di forme di comunicazione che avvengano tramite sistemi informatici[440].

Tuttavia, lo spettro di azioni alle quali la disposizione dedotta in giudizio autorizzava l'autorità investigativa esorbita la suddetta cornice, in quanto consente altresì di entrare all'interno del sistema informatico e da lì avere accesso alle conversazioni che siano avvenute anche in precedenza (escluse, per evidenti ragioni pratiche, quelle a voce) e all'intero archivio del dispositivo *target*. La garanzia dell'art. 10 GG si applica infatti esclusivamente alle comunicazioni nel momento in cui avvengono, senza che disponga con riferimento alla protezione del contento delle stesse una volta che la comunicazione abbia esaurito la sua attualità. È qui che il *BVerfG* identifica una scappatoia dalla tutela costituzionale di cui sopra, alla quale ritiene di poter porre rimedio ricorrendo a quella ricostruzione del generale diritto alla

[439] Per esempio il diritto alla sfera privata, segreta e intima (BVerfGE, 27, 1) o il diritto all'autodeterminazione dei propri dati personali (BVerfGE, 65, 1). Sulla precisazione del diritto generale alla personalità per mezzo di posizioni giuridiche soggettive più concrete come procedimento tipico per la definizione specifica del contenuto di clausole generali, v. R. Alexy, *Teoria dei diritti fondamentali*, Bologna, Il Mulino, 2021, 393-394.

[440] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, §§ 183-184.

personalità dell'individuo come clausola aperta, declinata in questa circostanza nel senso di protezione dell'integrità e della confidenzialità dei sistemi informatici[441].

I giudici di Karlsruhe spostano poi l'attenzione sulla tutela dell'inviolabilità domiciliare di cui all'art. 13 GG, sottolineando come la disposizione si applichi alla sfera spaziale in cui la vita privata ha luogo, ivi compresi i luoghi ove si svolge l'iniziativa economica privata. Ciò che è vietato all'autorità pubblica non è soltanto l'ingresso all'interno di tali luoghi, bensì anche la captazione di elementi di prova audio-visivi che non sarebbero percepibili liberamente tramite osservazione semplice dall'esterno. La disposizione verrebbe in soccorso laddove vi fosse un tentativo di accedere a un luogo di privata dimora per manipolare un sistema informatico o per fare in modo che capti ciò che avviene in tale sede nel futuro prossimo, trasmettendolo a un sistema esterno[442].

Tuttavia, come noto, l'ipotesi più frequente di accesso a dispositivi e monitoraggio degli stessi avviene non tramite installazione diretta avendo a disposizione l'*hardware*, bensì intervenendo da remoto con tecniche insidiose tramite il ricorso a un apposito *software*. In questi casi, la protezione di cui all'art. 13 GG non può essere applicata, anche perché sovente le stesse autorità investigative non riescono a determinare se il sistema informatico penetrato sia localizzato, in un dato momento, in uno dei luoghi di cui sopra[443].

Il *BVerfG* aggiunge che nemmeno le particolari manifestazioni del diritto alla personalità consistenti nella garanzia del diritto alla riservatezza e all'autodeterminazione informativa[444], che la giurisprudenza costituzionale precedente aveva riconosciuto, offrono un presidio sufficiente agli utenti delle tecnologie informatiche. Nell'un caso, infatti, l'accesso al sistema informatico è suscettibile di collegare i dati personali riservati, che di per sé potrebbero non far emergere la rilevanza per il soggetto, con un contesto di riferimento, grazie al quale diviene ben più agevole desumere un quadro preciso della persona dell'utente.

---

[441] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, §§ 185-187.
[442] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, §§ 191-193.
[443] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, §§ 194-195.
[444] BVerfG, Primo Senato, 15 dicembre 1983, 1 BvR 209/83; la traduzione di *Recht auf informationelle Selbstbestimmung* è tratta da R. Flor, *La sentenza del* BundesVerfassungsGericht *del 27 febbraio 2008 sulla cd.* online durchsuchung, *op. cit.*, 682.

Nell'altro, è pur vero che tale prerogativa consente l'esercizio di un controllo dell'individuo sulla rilevazione e l'uso dei propri dati personali, così anticipando la soglia di tutela al momento della messa in pericolo della personalità. Tuttavia, l'affidamento del singolo a determinati sistemi informatici per lo sviluppo della propria personalità, tramite il conferimento di dati all'atto dell'utilizzo del sistema stesso, rende in ipotesi possibile a terzi l'estrazione di una significativa quantità di informazioni senza doversi impegnare in ulteriori attività di raccolta e analisi di dati. Un tale atto lede la personalità dell'individuo in una misura che il diritto all'autodeterminazione informativa non è dunque in grado di limitare in modo efficace[445].

L'assenza di forme di tutela adeguate contro le minacce alla personalità di ciascun individuo quando questi faccia affidamento su un sistema informatico per lo sviluppo della propria personalità, argomenta il *BVerfG*, richiedono l'intervento del più generale diritto alla personalità nella sua funzione di clausola aperta che supplisce alla lacuna dell'ordinamento costituzionale. Il diritto all'integrità e confidenzialità dei sistemi informatici, che condivide con quello all'autodeterminazione informativa la derivazione dal combinato disposto degli artt. 2.1 e 1.1 GG, protegge dunque la vita personale e privata del singolo avverso l'accesso da parte dello Stato nell'area della tecnologia informatica, ivi incluso il mero accesso ai dispositivi e non anche ai dati in essi contenuti[446].

2.2.4. I limiti all'applicabilità del nuovo diritto della personalità

I giudici di Karlsruhe si preoccupano, tuttavia, di limitare il campo di applicazione di questa nuova prerogativa, precisando come non ricada in tale perimetro l'utilizzo di un qualsiasi strumento tecnologico che, per sua natura, contenga dati pertinenti solo a una limitata sfera della personalità del singolo (es. sistemi elettronici a uso domestico privi di accesso a una rete): per tale ipotesi si continuerà ad applicare la disciplina relativa alla raccolta dei dati personali. Diversamente, la nuova posizione giuridica

[445] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, §§ 196-200.
[446] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, § 201.

soggettiva si riferisce solo all'utilizzo di tutti quei dispositivi che contengano dati e informazioni tali da consentire di inferire tratti caratteriali e di personalità significativi di una persona (primi fra tutti i computer, fissi o portatili che siano, o i telefoni cellulari di ultima generazione)[447].

Il collegio aggiunge che, per quanto fondamentale, il diritto in questione non ha natura assoluta, ben potendo essere compresso per ragioni di prevenzione dei reati o persecuzione degli autori degli stessi. Tali limitazioni dovranno però derivare da una disposizione di rango legislativo il cui contenuto sia conforme al dettato costituzionale[448].

2.2.5. I vizi d'incostituzionalità: il principio di precisione e determinatezza

La *Legge per la protezione della Costituzione* adottata dalla Renania Settentrionale-Vestfalia non fu considerata tuttavia costituzionalmente legittima dal giudice delle leggi, che ne censurò il mancato rispetto del principio di chiarezza (*rectius*, di precisione[449]) e di determinatezza delle disposizioni, come anche la violazione del principio di proporzionalità. In particolare, il Tribunale Costituzionale Federale riconnette il principio di determinatezza a quello dello Stato di diritto (artt. 20 e 28, §1 GG), ricordando come il Governo e le amministrazioni pubbliche trovino nella legge indicazioni che restringono la sfera d'azione degli stessi e le corti siano intitolate a svolgere il controllo di legittimità dei provvedimenti dell'amministrazione proprio per assicurare che sia un'assemblea parlamentare a legittimazione democratica a stabilire la natura delle limitazioni ai diritti fondamentali e l'estensione delle stesse.

La determinatezza sta in stretto rapporto con il requisito della chiarezza, in osservanza del quale i destinatari delle disposizioni normative devono essere in grado di comprendere le fattispecie contemplate dalla legge e potersi adattare all'applicazione di misure restrittive della propria sfera di libertà. È compito del Parlamento stabilire in modo chiaro e preciso, identificando l'ambito di applicazione,

---

[447] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, §§ 202-203.
[448] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, § 207.
[449] Favorevole a tale resa in italiano del termine è R. Flor, *La sentenza del* BundesVerfassungsGericht *del 27 febbraio 2008 sulla cd.* online durchsuchung, *op. cit.*, 683, n. 5.

casi, scopi e limitazione di tali prerogative. Il ricorso a concetti giuridici indefiniti non è del tutto escluso, ma non può cagionare l'effetto di minare la prevedibilità e la possibilità di impugnare in giudizio l'attività delle pubbliche autorità che la legge investe di tali poteri[450].

Più nel dettaglio, i vizi censurati dal giudice delle leggi furono relativi alla tecnica utilizzata dal legislatore statale nella fonte in questione: le precondizioni per il ricorso a tali misure si individuano infatti tramite un doppio rinvio legislativo (in entrambi i casi i rinvii sono interni alla medesima legge, ma nel secondo il riferimento è alle condizioni previste per la limitazione del segreto della corrispondenza). Il Tribunale costituzionale federale argomenta infatti che l'identificazione di quali diritti fondamentali siano lesi dalle misure investigative poste in essere dall'autorità amministrativa in questione può richiedere complicate valutazioni che spettano al legislatore. Esso non può esimersi, tramite un mero rinvio a un diritto fondamentale potenzialmente rilevante, dal garantire in concreto quella posizione giuridica delegandone la messa in atto a un'amministrazione. L'adozione di una simile tecnica legislativa, proseguono i giudici di Karlsruhe, viola il principio di determinatezza, laddove impiegata in una disposizione che introduce nuove categorie di misure investigative finalizzate a far fronte a recenti sviluppi in campo tecnologico. Peraltro, la disposizione violerebbe anche il principio di chiarezza (precisione) in quanto non viene specificato quali aspetti della disciplina dettata dalla fonte con riferimento alla tutela del segreto della corrispondenza si applichino anche al caso dei mezzi di ricerca della prova su sistemi informatici[451].

2.2.6. I vizi d'incostituzionalità: lo scrutinio sulla proporzionalità

Per quanto concerne il principio di proporzionalità, il *BVerfG* ricorda come esso imponga che la limitazione di un diritto fondamentale debba servire al perseguimento di un fine legittimo e sia utile, necessaria e appropriata per conseguirlo. Se i giudici di Karlsruhe riconoscono che la raccolta dati è finalizzata alla tutela dell'ordinamento

[450] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, §§ 209-210.
[451] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, §§ 212-213, 216.

democratico dello Stato dinanzi alle minacce di matrice terroristica, essi puntualizzano altresì come né il testo della disposizione né un'interpretazione sistematico-contestuale della stessa autorizzino a ritenere tali poteri confinati al solo dominio dell'attività di prevenzione delle condotte terroristiche. La ragione giustificatrice di tali misure intrusive si rintraccia nell'assolvimento di quel dovere di protezione dei cittadini, gravante sulle istituzioni dello Stato, avverso attività terroristiche o diverse, la cui efficace prevenzione potrebbe difficilmente prescindere dal riconoscimento ad autorità pubbliche di poteri di indagini penetranti sugli strumenti informatici ormai a larga diffusione[452].

Nulla da eccepire ha il Tribunale costituzionale federale sull'utilità o strumentalità delle misure, non rilevando in sede di scrutinio la possibilità (invero astratta e da verificare in concreto) che l'utilizzatore di un sistema informatico possa rendere vani gli sforzi della pubblica autorità adottando efficaci strategie di protezione. Nemmeno rende inutile tali poteri la maggiore o minore rilevanza probatoria degli elementi raccolti, anche in considerazione dell'ampia discrezionalità di cui gode il legislatore nella determinazione dell'utilità di una misura a perseguire un dato fine. Ad analoghe conclusioni giunge il giudice delle leggi con riferimento al requisito della necessità, non riscontrando la disponibilità di altri metodi di raccolta dei medesimi dati a natura meno intrusiva[453].

Più critico è il giudizio sull'adeguatezza dello strumento adottato: tale criterio richiede infatti che, sotto un profilo generale, la gravità della limitazione non possa essere sproporzionata alla serietà delle ragioni che la giustificano. A parere del *BVerfG* le misure previste dalla disposizione in commento non soddisfano tale requisito, poiché implicano limitazioni di diritti fondamentali tanto intense da apparire non proporzionate all'interesso pubblico all'investigazione su tali circostanze di pericolo. Vi è inoltre una carenza di garanzie procedurali che tengano in dovuta considerazione gli interessi dei soggetti coinvolti, protetti da diritti fondamentali a riconoscimento costituzionale[454].

---

[452] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, §§ 218-220.
[453] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, §§ 221-225.
[454] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, §§ 226-228.

A causa della suddetta intensità, la limitazione di diritti fondamentali che consista in un accesso segreto a un sistema informatico nell'esercizio di una funzione preventiva soddisfa il requisito dell'appropriatezza soltanto laddove sussistano fatti che indichino l'esistenza, nel caso specifico, di un pericolo posto nei confronti di un interesse giuridico di importanza soverchiante, anche in assenza della determinazione del probabile verificarsi dello stesso nel futuro prossimo. Inoltre, le disposizioni che riconoscano tali poteri devono assicurare la tutela dei diritti fondamentali della persona che subisce le dette limitazioni anche nella forma di garanzie procedurali[455].

In circostanze in cui si manifesta una tale tensione fra l'obbligo che grava sullo Stato di proteggere interessi a rilevanza collettiva e interessi individuali garantiti dal dettato costituzionale, il compito del legislatore, argomenta il *BVerfG*, consiste nel raggiungere un compromesso in astratto fra interessi divergenti. Ciò implicherebbe dunque che la significativa limitazione di dati diritti fondamentali potrebbe essere attuata soltanto per la protezione di determinati interessi giuridici e solo ove si accertasse il superamento di una soglia di pericolo predefinita. Il divieto di limitazioni dei diritti fondamentali che non siano appropriate richiede inoltre che le soglie di compressione di tali posizioni giuridiche siano contemplate da testi con forza di legge.

Limiti all'esercizio dei diritti costituzionali tanto onerosi sono da considerarsi sproporzionati di per sé laddove le disposizioni che li prevedano difettino di requisiti di sufficiente gravità. Se il testo di riferimento è finalizzato a prevenire determinati rischi, sono rango e natura delle situazioni di pericolo corse dagli interessi protetti che rilevano ai fini della valutazione della incisività di una data limitazione. Laddove gli interessi sottostanti al conferimento di poteri di limitazione dei diritti costituzionalmente sanciti abbiano preponderanza tale da giustificare la compressione delle dette pretese costituzionali, il principio di proporzionalità fa sorgere dei requisiti costituzionali da porre quali condizioni fattuali che ammettano l'adozione di misure restrittive dei diritti riconosciuti dalla Costituzione. Il legislatore deve quindi sforzarsi di mantenere un equilibrio fra la natura e l'intensità di tali limitazioni dei diritti fondamentali e gli elementi di fatto che giustificano l'adozione di queste misure. Tali

[455] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, § 242.

valutazioni devono in ogni caso tenere in considerazione il requisito della sufficiente probabilità di realizzazione di una data ipotesi di pericolo[456].

Più nello specifico, l'adozione di misure che limitino il godimento di diritti costituzionalmente protetti può avvenire soltanto laddove il conferimento di tali poteri sia vincolato alla verifica della sussistenza empirica di elementi di fatto spia di pericolo concreto a un interesse giuridico di fondamentale rilevanza, quali la vita, l'integrità fisica e la libertà personale, ma anche quelli che, laddove venissero a mancare per causa di un attacco esterno, siano suscettibili di minare la sopravvivenza dello Stato o le basi dell'esistenza dell'uomo, quali il corretto funzionamento delle strutture di servizio pubblico che sostentano la vita dei cittadini. Una misura statale che renda conoscibile, per effetto di un monitoraggio particolarmente intrusivo, a un'autorità investigativa i tratti salienti della personalità di un singolo non appare appropriata a proteggere altri interessi giuridici, individuali o collettivi che siano, laddove le circostanze non suggeriscano l'imminenza di una minaccia gravosa agli interessi fondamentali di cui sopra. Le pubbliche autorità dovrebbero, in circostanze simili, fare ricorso agli altri strumenti investigativi a fini preventivi riconosciuti dalla disciplina processual-penalistica.

Le disposizioni che autorizzino l'esercizio di tali poteri dovrebbero quindi richiedere esplicitamente la verifica della sussistenza di elementi di fatto tali da giustificare un giudizio prognostico sull'imminenza di una minaccia a uno dei diritti fondamentali suindicati. Presunzioni e massime d'esperienza non sarebbero quindi sufficienti, essendo necessaria una verifica caso per caso della serietà dei rischi sottostanti. Tali prerequisiti impongono quindi di considerare giustificato il ricorso alle misure di sorveglianza segreta da remoto solo ove sia verificata l'esistenza di una sufficiente probabilità che un danno sia inferto da uno o più soggetti determinati a uno di quegli interessi fondamentali protetti, in un tempo futuro prevedibile, in mancanza di un intervento preventivo dello Stato. Tali considerazioni non possono tuttavia essere traslate anche al periodo che precede il sorgere concreto di tale pericolo, ben

[456] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, §§ 243-245.

potendosi poi la situazione risolvere con esiti privi di lesività per i diritti fondamentali dei cittadini tutti[457].

2.2.7. Le deficienze della tutela sotto il profilo procedurale

Per quanto attiene alle garanzie procedurali opportune, se anche esse non possono ovviare alle mancanze di una disciplina che fissi una soglia per la limitazione dei diritti non sufficientemente determinata, sono comunque passibili di costituire un elemento significativo per un'efficace tutela dei diritti fondamentali. Più nello specifico, i giudici di Karlsruhe affermano che il controllo esercitato da un organo indipendente e neutrale sul ricorso a tali misure da parte delle autorità investigative sia desiderabile. Per quanto una verifica preventiva della legittimità degli strumenti di indagine di cui sopra sia pertanto costituzionalmente richiesta, il legislatore gode di una certa discrezionalità nella determinazione dell'organo di controllo e delle procedure applicabili. Tuttavia, quando la violazione dei diritti fondamentali consista in una condotta tanto invasiva quanto l'accesso a un dispositivo informatico, si presume che la sede privilegiata per il controllo su tale attività sia quella giurisdizionale, in ragione della terzietà dei giudici e della loro soggezione alla sola legge. Ciò vale a patto che essi conducano un esame dettagliato e in profondità della legittimità delle misure prospettate, recando in motivazione il ragionamento giudiziale seguito. L'affidamento di tale funzione di controllo ad altro organo dello Stato è condizionale alla sussistenza di pari requisiti di indipendenza e neutralità e al vincolo di motivazione della legittimità (o meno) del ricorso ai detti strumenti investigativi. Solo dinanzi a casi urgenti di pericolo imminente si potrebbe derogare a tali prescrizioni, a patto che uno scrutinio sulla legittimità dell'adozione delle misure da parte di un organo neutrale sia svolto in seguito[458].

Sulla base della cornice costituzionale delineata, il *BVerfG* procede a ravvisare il mancato rispetto dei requisiti summenzionati da parte delle disposizioni impugnate. In primo luogo, argomenta il collegio, le ragioni che autorizzano il ricorso a strumenti

[457] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, §§ 247-253.
[458] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, §§ 257-261.

di *intelligence* da parte dell'autorità di protezione della Costituzione si fondano soltanto sulla sussistenza di elementi di fatto che facciano presumere (senza certezza) di poter ottenere informazioni riguardanti attività contrarie alla Costituzione attraverso tali tecniche d'indagine. Una tale soglia di limitazione sostanziale di un diritto costituzionalmente protetto non risulta sufficiente a soddisfare i requisiti costituzionali, sia sotto il profilo dei prerequisiti fattuali previsti sia sotto quello del peso degli interessi giuridici perseguiti; peraltro, nemmeno si introduce la garanzia procedurale del controllo da parte di un organo terzo e indipendente. Tali carenze del dettato normativo non possono considerarsi ovviate dal rinvio ai prerequisiti che l'atto indica per la limitazione del diritto al segreto della corrispondenza di cui all'art. 10 GG. Infatti, la disposizione in oggetto non circoscrive l'accesso da remoto a sistemi informatici ai casi e alle modalità con cui la medesima legge disciplina la limitazione del summenzionato diritto costituzionale. Peraltro, aggiunge la Corte, né la soglia di compressione del diritto indicata né le garanzie procedurali previste risultano sufficienti alla luce del dettato costituzionale[459].

La disposizione a cui si rinvia autorizza il dispiegamento di una misura di sorveglianza in presenza di elementi fattuali che fondino un sospetto che un soggetto stia pianificando, stia commettendo o abbia già commesso un reato incluso in un catalogo predeterminato. Tale lista, osservano i giudici di Karlsruhe, difetta di un principio ispiratore comune che giustifichi la possibilità di applicare le invasive misure di sorveglianza informatica da remoto a un tale numero di condotte di reato. Questa osservazione fa sorgere due ordini di problemi. Il primo è che non vi è garanzia che in tutti questi casi l'utilizzo delle misure di monitoraggio occulto serva lo scopo di proteggere uno dei rilevanti interessi giuridici menzionati in precedenza (vita, integrità fisica, libertà personale). Il secondo è che il rinvio alla disposizione relativa alla limitazione del segreto della corrispondenza non assicura che l'accesso occulto a un sistema informatico abbia luogo soltanto ove tali interessi giuridici siano messi in pericolo in un caso concreto con un sufficiente grado di probabilità in un prossimo futuro[460].

---

[459] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, §§ 263-265.
[460] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, §§ 266.

La stessa disposizione che si riferisce all'art. 10 GG consente il ricorso a misure di sorveglianza in presenza di elementi di fatto che facciano sorgere il sospetto che il soggetto in questione sia membro di un'associazione che si prefigga lo scopo di compiere condotte criminali lesive di interessi costituzionalmente protetti. Tuttavia, tali condotte non sono indicate che in termini generali, ben potendo così ingenerare il rischio di un'interpretazione estensiva, la quale potrebbe rendere possibile una limitazione allo scopo di proteggere interessi giuridici non di fondamentale importanza. Inoltre, non si prevede che tali elementi di fatto debbano esistere in ogni singolo caso.

Da un punto di vista procedurale, poi, il *BVerfG* evidenzia come l'obbligo di ottenere un'autorizzazione dall'autorità suprema del *Land* per poter adottare una misura di sorveglianza del tipo in commento, in osservanza della disposizione relativa all'art. 10 GG, non sia sufficiente a soddisfare il requisito del controllo preventivo a norma degli artt. 2.1 e 1.1 GG. L'autorità in questione, infatti, non appartiene all'ordine giudiziario e potrebbe dunque trovarsi in una situazione di parzialità nel prendere la decisione, dettata dalla possibile comunanza di interessi con l'autorità procedente[461].

2.2.8. La protezione del nucleo fondamentale della vita privata

Infine, il giudice delle leggi censura l'inesistenza di adeguate precauzioni di legge volte a evitare limitazioni del nucleo specialmente garantito della vita privata, che lo stesso Tribunale costituzionale federale aveva già sancito essere inviolabile[462]. Nell'ambito di attività di sorveglianza occulta del tipo in parola, infatti, le autorità statali potrebbero raccogliere dati ed elementi attinenti a tale nucleo protetto: note a mo' di diario personale, filmati audiovisivi, tracce audio, i quali godono di protezione assoluta in quanto incarnano esperienze profondamente personali. Inoltre, il rischio si estende anche ai contenuti oggetto di una comunicazione fra l'utilizzatore del dispositivo e terzi, tanto attraverso i canali usuali della telefonia mobile, quanto attraverso le comunicazioni che si servono della rete Internet (es. posta elettronica).

[461] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, §§ 266-269.
[462] BVerfG, Primo Senato, 16 gennaio 1957, 1 BvR 253/56.

Il ricorso a mezzi di ricerca della prova tanto invasivi e suscettibili di raccogliere dati a sensibile valore personale presenta minacce più serie alla sfera della personalità dell'individuo rispetto a quelle relative al monitoraggio degli spostamenti tramite sistemi GPS. La segretezza del monitoraggio rende impossibile a chi utilizza il dispositivo verificare che le autorità pubbliche rispettino tale nucleo essenziale garantito, imponendo così la previsione di specifiche precauzioni procedurali che assicurino i singoli nei confronti di tale rischio[463].

Qualora la raccolta di dati del genere di cui sopra sia inevitabile, prosegue il *BVerfG*, sussiste un obbligo di cancellazione tempestiva degli stessi e un'esclusione della loro utilizzazione a fini d'indagine o probatori. Questa deroga discende dalla natura spesso automatizzata dei sistemi di sorveglianza, che pertanto non dispongono di una sensibilità sufficiente a distinguere in modo efficace tale nucleo protetto da altri dati, ma vale parimenti per il controllo che avvenga a opera di soggetti in carne e ossa, per le difficoltà intrinseche dell'operazione, che può altresì riguardare dati in lingua straniera. In tali circostanze una valutazione ex-ante non è quindi praticabile e la soluzione non può che risiedere in una cancellazione ex-post.

Il collegio suggerisce dunque il ricorso a un meccanismo in due stadi. Le disposizioni dovrebbero prevedere che si eviti, per quanto possibile con la tecnologia a disposizione, la raccolta di dati attinenti a tale nucleo protetto. Elementi di fatto concreti che suggeriscano che in un dato caso il ricorso a tali misure lederebbe tale sfera garantita dovrebbero far rinunciare all'utilizzo di tali strumenti, a meno che il riferimento agli stessi elementi personali sia pretestuoso e privo di collegamento con il resto della comunicazione che intercorre, volto soltanto a impedire che possa essere oggetto di sorveglianza. In ogni caso, dati attinenti a tale sfera dovrebbero essere cancellati senza indugio in seguito, non appena ci si avveda della natura degli stessi. Le disposizioni oggetto dello scrutinio del Tribunale costituzionale federale difettano di tali garanzie procedurali, né si può considerare affine quanto previsto dalla disposizione relativa all'art. 10 GG, in quanto essa fa riferimento soltanto al principio

[463] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, §§ 270-275.

di necessità (cancellazione dei dati non utili o che non rivestano più importanza a fini di indagine)[464].

Con riferimento all'altra ipotesi di monitoraggio e ricognizione da remoto prevista dalla legge in questione, il *BVerfG* ne sancisce la violazione del diritto alla segretezza delle telecomunicazioni di cui all'art. 10.1 GG qualora l'autorità procedente abbia ottenuto l'accesso al contenuto delle comunicazioni (es. posta elettronica o cd. chat room) senza la previa autorizzazione di una delle due parti del rapporto comunicativo. Diversamente, se questa è stata ottenuta, non configura violazione della disposizione costituzionale (che non si estende al rapporto di fiducia nella confidenzialità della comunicazione instaurato fra mittente e destinatario). Inoltre, tali compressioni del diritto costituzionalmente sancito sono, a parere dei giudici di Karlsruhe, prive della necessaria precisione e chiarezza con riferimento ai requisiti necessari.

Le maglie larghe di tali requisiti generali implicano anche la violazione del principio di proporzionalità, poiché alla rilevanza degli interessi ristretti (che comprendono anche la sfera personale di chi comunica con la persona posta sotto sorveglianza) non corrisponde una sufficiente specificazione degli scopi fondamentali perseguiti. Un'ulteriore violazione ravvisata dal giudice costituzionale risiede nel mancato riferimento nella legge al diritto fondamentale limitato, come disposto dall'art. 19.1 GG (il mero rinvio alla disposizione relativa all'art. 10 GG non si qualifica come tale).

Nonostante la declaratoria di nullità della disposizione, misure di monitoraggio via rete Internet non sono precluse *tout court* alle autorità in questione, a patto che le stesse non comprimano alcun diritto fondamentale. In particolare, la sorveglianza *online*, quando non ricada nell'ipotesi di cui al suddetto art. 10 GG, non necessariamente comprime il diritto alla personalità costituzionalmente sancito. È questa l'ipotesi dei dati forniti al *provider* del servizio di rete o dei dati che siano liberamente accessibili al pubblico sulla rete, senza che vi sia violazione del diritto all'autodeterminazione informativa, oppure che siano ottenuti in una comunicazione diretta con un soggetto agendo sotto copertura, sempre che non derivino da una

[464] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, §§ 276-287.

fiducia che la persona sorvegliata pone nell'identità dell'altra persona (così che diversamente non li avrebbe rivelati). Non sorge aspettativa degna di protezione costituzionale, dunque, per il solo fatto di partecipare a forum *online*, ove l'identità degli altri utenti non è nota e quindi ben potrebbe trattarsi di agenti governativi sotto copertura[465].

2.3. Gli sviluppi più recenti della giurisprudenza costituzionale.

2.3.1. La riproposizione delle disposizioni nella legge antiterrorismo federale

Il *BundesVerfassungsGericht* è tornato a occuparsi della vicenda otto anni dopo, questa volta con riferimento alla legislazione federale e non più statale come nella prima pronuncia[466]. L'oggetto del giudizio di legittimità costituzionale era costituito, nel caso di specie, da una serie di disposizioni contenute nel sotto-titolo 3a della *Legge sull'ufficio di polizia criminale federale* (*Bundeskriminalamtgesetz*, per brevità *BKAG*), introdotte dalla *Legge sulla prevenzione da parte dell'ufficio di polizia criminale federale delle minacce legate al terrorismo internazionale* meno di un anno dopo la prima pronuncia del *BVerfG* sul tema[467].

Le disposizioni in questione, analogamente a quelle già impugnate della legge della Renania Settentrionale-Vestfalia, conferiscono alle autorità di polizia del summenzionato ufficio poteri preordinati alla raccolta in segreto di dati personali nel contesto dell'attività volta a contrastare la minaccia e a prevenire la commissione di attività penalmente rilevanti. Tali condotte sono suscettibili di interferire con i diritti fondamentali di inviolabilità del domicilio (art. 13, §1 GG), segretezza della corrispondenza (art. 10, §1 GG) e tutela della personalità (art. 2, §1 GG in combinato disposto con art. 1, §1 GG), intesa nel senso di garanzia sia dell'autodeterminazione informativa che della confidenzialità e integrità dei sistemi informatici.

---

[465] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, §§ 288-311.

[466] Per un breve resoconto immediatamente successivo alla decisione v. A. Venegoni, L. Giordano, *La Corte costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici*, in *Diritto Penale Contemporaneo*, 8 maggio 2016, ora disponibile all'url: https://archiviodpc.dirittopenaleuomo.org/d/4703-la-corte-costituzionale-tedesca-sulle-misure-di-sorveglianza-occulta-e-sulla-captazione-di-conversa (ultimo accesso: 11 maggio 2020).

[467] *Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt*, 25 dicembre 2008, in vigore dal 1 gennaio 2009.

Prima di addentrarsi nell'analisi concreta delle questioni, il collegio ricorda, sulla base di giurisprudenza costituzionale consolidata, come la legittimità costituzionale dei summenzionati poteri dipenda dai limiti derivanti da ciascuno dei diritti fondamentali in gioco e dai requisiti di proporzionalità da determinarsi caso per caso, questi ultimi da intendersi come verifica del perseguimento di fini legittimi e della natura idonea, necessaria e proporzionata delle misure al conseguimento di tali fini. Ulteriori principi prescritti per tali forme di limitazione dei diritti sono la precisione e la determinatezza delle disposizioni, così da incrementare la possibilità di prevedere l'interferenza con il godimento dei diritti da parte dei cittadini, costituire un limite effettivo ai poteri delle amministrazioni e offrire un efficace controllo giurisdizionale[468].

Nulla quaestio, secondo il Tribunale costituzionale federale, vale la pena sollevare con riferimento alla legittimità del fine perseguito e alla idoneità e necessità dei poteri conferiti a tale scopo. In particolare, il collegio sottolinea come i reati alla cui prevenzione tali misure sono preordinate sono di particolare gravità in quanto finalizzati a destabilizzare la società e si servono a fini strumentali di condotte che mettono a repentaglio la vita e l'integrità fisica di terzi. Né la pronuncia si diffonde in dettaglio sull'idoneità e la necessità, argomentando quasi apoditticamente e specificando soltanto come non siano evidenti misure alternative con minore afflittività ma pari efficacia nel perseguimento di tali condotte di matrice terroristica[469].

2.3.2. Un nuovo giudizio sulla proporzionalità delle misure

Con riferimento alla proporzionalità delle limitazioni di diritti fondamentali rispetto ai fini perseguiti, il *BVerfG* riconosce la spettanza al legislatore di tale valutazione discrezionale. Da un lato della bilancia pesa l'interferenza nella sfera privata dei soggetti e, talvolta, persino nei luoghi ove essi dimorano, con inevitabili ed evidenti conseguenze sulla dignità degli stessi[470], oltre ai ben noti rischi di profilazione

[468] BVerfG, Primo Senato, 20 aprile 2016, 1 BvR 966/09, 1 BvR 1140/09, §§ 93-94.
[469] BVerfG, Primo Senato, 20 aprile 2016, 1 BvR 966/09, 1 BvR 1140/09, §§ 95-97.
[470] Che, come noto, è sancita come inviolabile dall'art. 1 *GG* e si ritiene informi di sé tutto il testo costituzionale, v., *ex multis*, E.J. Eberle, *Human Dignity, Privacy, and Personality in German and American Constitutional Law*, in *Utah L. Rev.*, 1997, 969.

derivanti dalle accresciute possibilità di incrociare dati raccolti con strumenti e in circostanze diverse. Dall'altro lato, il legislatore è altresì chiamato a garantire un'effettiva protezione dei diritti fondamentali e degli interessi giuridici dei cittadini, fra i quali rientrano d'altronde, con la massima rilevanza, l'ordine costituzionale, l'esistenza e la sicurezza della Federazione e dei *Länder* e la vita, integrità fisica e libertà delle persone.

Richiamando nuovamente una precedente giurisprudenza dello stesso *BVerfG*, la pronuncia ricorda dunque che la sicurezza dello Stato, intesa come il mantenimento della pace e della sicurezza, e la tutela della popolazione sono fini di egual valore rispetto ad altri principi costituzionali assiologicamente rilevanti. Ciò implica che grava sullo Stato il compito di proteggere le prerogative individuali dei cittadini anche dall'interferenza a opera di terzi[471].

Il cuore della questione, nonché il tema su cui i giudici di Karlsruhe si concentrano maggiormente, è rappresentato dalla verifica e dallo scrutinio sul rispetto del principio di proporzionalità. Secondo tale criterio, il sacrificio dei diritti di un singolo non può essere autorizzato sulla base della mera intuizione o sospetto che da tale monitoraggio possano essere ottenuti elementi utili ulteriori a fini di prevenzione di condotte terroristiche. Al contrario, deve essere possibile inferire ragionevolmente dalle circostanze di fatto il coinvolgimento del soggetto in un'attività che metta in pericolo un bene giuridico. Il collegio sottolinea come ciascuno di tali poteri debba essere cucito su misura al grado di interferenza coi diritti individuali, così che per misure di particolare intrusività quali la sorveglianza di luoghi di privata dimora e l'accesso a sistemi informatici si debbano prevedere requisiti particolarmente stringenti[472].

Il Tribunale Costituzionale Federale precisa che, mentre per gli interventi preordinati all'esecuzione di misure repressive di condotte già poste in essere ciò che rileva è la gravità delle condotte penalmente rilevanti (suddivisa dal legislatore in

---

[471] BVerfG, Primo Senato, 20 aprile 2016, 1 BvR 966/09, 1 BvR 1140/09, §§ 95-97. Peraltro, il riconoscimento di tale obbligo a carico delle autorità pubbliche dimostra come sia riduttivo concepire i diritti civili come mere libertà negative, in quanto sono tali soltanto se immaginate sull'asse verticale del rapporto Stato-cittadinanza; diversamente, se si aderisce all'impostazione ideologica e interpretativa che legge le disposizioni costituzionali come efficaci (e azionabili in giudizio) altresì nei rapporti tra privati (cd. *Drittwirkung* o effetto orizzontale), emerge come la tutela in concreto di tali posizioni giuridiche e pretese non possa prescindere da un *facĕre* dello Stato.

[472] BVerfG, Primo Senato, 20 aprile 2016, 1 BvR 966/09, 1 BvR 1140/09, §§ 103-105.

significativa, grave e particolarmente grave), con riguardo alle misure preventive è il peso degli interessi giuridici che si intende proteggere a essere decisivo. La giurisprudenza dello stesso *BVerfG* ha qualificato come interessi di particolare rilevanza la vita, l'integrità fisica e la libertà degli individui, ma anche l'esistenza e la sicurezza della Federazione e di un *Land*, mentre non ha ritenuto tale la tutela degli interessi proprietari. In ogni caso, prevedere precauzionalmente la possibilità di accedere a dati immagazzinati o di sorvegliare luoghi di privata dimora in caso di pericolo o di effettuare il monitoraggio da remoto di sistemi informatici qualora sussistano rischi per interessi pubblici tali da ledere l'esistenza del popolo è stato considerato generalmente compatibile con il dettato costituzionale. Pertanto, il legislatore non incontra alcun impedimento nello stabilire uniformemente le soglie che tali situazioni di pericolo devono superare per poter fare ricorso alle date misure finalizzate alla tutela dei summenzionati interessi[473].

Con specifico riferimento al requisito della proporzionalità, la pronuncia afferma che esso si considera generalmente integrato, con riferimento a misure ad alto grado di interferenza con il godimento dei diritti individuali come quelle in commento, laddove sussista un rischio prevedibile e sufficientemente specifico a tali interessi protetti in un caso determinato e la persona destinataria di tali misure appaia ragionevolmente (sulla base di una valutazione obiettiva delle circostanze di fatto) coinvolta in tali condotte. La natura di tale minaccia, peraltro, può variare a seconda dell'intrusività di una misura: la sorveglianza di un luogo di privata dimora richiede, ai sensi dell'art. 13, §4 GG un pericolo imminente, qualificandolo cioè anche sotto il profilo della probabilità di realizzazione[474].

I diversi gradi in cui viene classificata la gravità del rischio per un interesse protetto ai fini dell'ordinaria prevenzione dei reati (specifico, direttamente imminente e attuale) non vincolano, tuttavia, il legislatore il quale può spostare a un momento antecedente la soglia al cui superamento si avvia il meccanismo di tutela, anticipando i requisiti di prevedibilità della catena causale. In ogni caso, ricorda il collegio, la base giuridica che giustifica l'interferenza con un dato diritto deve prevedere la verifica

[473] BVerfG, Primo Senato, 20 aprile 2016, 1 BvR 966/09, 1 BvR 1140/09, §§ 107-108.
[474] BVerfG, Primo Senato, 20 aprile 2016, 1 BvR 966/09, 1 BvR 1140/09, §§ 109-111.

della sussistenza di una minaccia sufficientemente specifica, intesa nel senso dell'esistenza almeno di elementi fattuali spia dell'emergere di uno specifico rischio gravante su interessi giuridicamente protetti. Inferenze tratte da massime d'esperienza non possono quindi fondare il ricorso a misure tanto intrusive: solo il riferimento a dati empirici, tratti da circostanze concrete alla base di un giudizio prognostico che determini la probabilità che un tale evento avvenga, viene considerato legittimo.

Il *BVerfG* aggiunge che tale minaccia specifica può essere ritenuta sussistente anche laddove non sia del tutto prevedibile la catena causale che porti all'evento lesivo della posizione giuridica individuale, a patto che vi siano fatti tali da fondare la previsione della possibilità di un danno a interessi giuridici di particolare rilevanza. In questo caso tali circostanze devono consentire l'inferenza di quale tipo di atto verrà perpetrato e della cornice temporale dello stesso e, inoltre, deve essere possibile circoscrivere il perimetro dei soggetti coinvolti, così che la sorveglianza e il monitoraggio possano essere limitati agli stessi e incidere quanto meno possibile sulla sfera giuridica di terzi.

Non trascurabile è il rilievo che, con riferimento alle attività terroristiche, le cui circostanze di tempo e di luogo sono notoriamente difficili da individuare con anticipo, il giudice costituzionale ritiene sufficiente il richiamo a elementi desumibili dal comportamento individuale del soggetto tali da far concludere che esiste una specifica probabilità che lo stesso ponga in essere condotte del genere in un futuro prossimo (es. il rientro in patria a seguito di un periodo trascorso in un centro d'addestramento terroristico in un paese estero). Diversamente, sarebbe tuttavia costituzionalmente inaccettabile, argomenta la pronuncia, dedurre la probabilità di tali condotte da comportamenti meramente preliminari e caratterizzati, per loro natura, da una certa ambivalenza con riferimento ai possibili esiti (es. l'attrazione nei confronti di una lettura fondamentalista di dati testi religiosi)[475].

Qualora si dia il caso di misure di sorveglianza suscettibili di incidere altresì sulla sfera giuridica di soggetti terzi estranei alle condotte in oggetto, è richiesta l'insufficienza di misure di monitoraggio da remoto relative alla sola persona *target*, tale da richiedere ai fini della buona riuscita dell'attività d'indagine altresì la

[475] BVerfG, Primo Senato, 20 aprile 2016, 1 BvR 966/09, 1 BvR 1140/09, §§ 112-113.

sorveglianza su un luogo di privata dimora di terzi (nel momento in cui il soggetto sorvegliato vi si trattenga) e l'accesso ai sistemi informatici di terze parti (ove il sospettato vi abbia salvato dati non altrimenti accessibili). Diversamente, la sorveglianza diretta di terzi è legittima solo ove vi siano ragioni di credere che i contatti che avvengono fra il soggetto principale indiziato e la persona terza siano strumentali a gettare luce su alcuni aspetti dell'attività di indagine, non meramente sul presupposto di andare alla ricerca di eventuali ulteriori elementi in una sorta di "pesca a strascico" fra i contatti della persona sorvegliata. Se però misure investigative meno intrusive delle suddette offrissero ragioni valide per ricorrere a quelle a più grave interferenza di cui sopra, nessuna violazione del dettato costituzionale sarebbe censurabile[476].

2.3.3. La necessità delle opportune tutele procedurali e della protezione del nucleo duro del diritto

Il Tribunale costituzionale federale ricorda, inoltre, come misure tanto invasive da risultare nella raccolta e registrazione di dati particolarmente riservati e senza che gli interessati ne abbiano contezza debbano prevedere opportune garanzie procedurali, vale a dire uno scrutinio preventivo da parte di un'autorità indipendente, ad esempio un'ordinanza di un giudice. Non solo tale passaggio deve essere contemplato, ma deve altresì esserne garantita l'effettività: le richieste per la concessione di tali misure dovranno cioè recare una giustificazione sufficientemente circostanziata e indicare dei limiti di azione, così che l'autorità investita della decisione possa adottare un provvedimento informato e in maniera indipendente[477].

Il giudice costituzionale rammenta l'esistenza di una sfera privata profonda e intangibile che viene sottratta integralmente all'interferenza dei pubblici poteri. L'espressione di pensieri, sensazioni e convinzioni personali rivolta a persone particolarmente fidate quali coniugi, ascendenti e discendenti, in particolare ove conviventi, ma anche legali rappresentanti o specialisti medici, ministri di culto e amici

[476] BVerfG, Primo Senato, 20 aprile 2016, 1 BvR 966/09, 1 BvR 1140/09, §§ 115-116.
[477] BVerfG, Primo Senato, 20 aprile 2016, 1 BvR 966/09, 1 BvR 1140/09, §§ 117-118.

stretti, non perde la propria natura protetta in quanto privata per la sola commistione con conversazioni su argomenti contingenti e non privati. Diversamente, se gli scambi verbali con una o più persone appartenenti alle suddette categorie sono pertinenti alla preparazione e organizzazione di condotte penalmente rilevanti, essi perdono il carattere privato e assumono importanza pubblica, così potendo essere oggetto di attività di monitoraggio e sorveglianza[478].

Peraltro, precisa la pronuncia, la sfera privata protetta alla quale si fa riferimento non è suscettibile di giudizi di bilanciamento con esigenze di sicurezza pubblica che adottino come criterio guida il principio di proporzionalità. Questo non esclude che possano accidentalmente essere poste in essere misure del tipo in questione, dato lo scenario di incertezza sul quale le autorità investigative operano. Ciò che però è necessario è che nella previsione astratta di tali strumenti da parte del legislatore il rispetto di tale nucleo privato sia qualificato come limite, non derogabile sulla base delle circostanze del caso concreto. Quand'anche non sia possibile evitare la raccolta di dati promiscui, fra cui anche alcuni appartenenti a tale area privata protetta, andrebbe previsto uno scrutinio preventivo all'utilizzo dei dati per stralciare quelli non utilizzabili in quanto attinenti a tale sfera riservata. Peraltro, non è necessario che di tale funzione sia investita un'autorità *ad hoc*, ben potendo bastare il controllo della medesima autorità investigativa[479].

Il *BVerfG* sottolinea anche l'esigenza di garantire degli elevati standard di trasparenza della procedura e di controllo sulla correttezza della stessa: poiché la segretezza di tali attività è requisito imprescindibile per il raggiungimento dei fini prefissati, non è ragionevole che vi sia un obbligo di notifica preventivo, ma ben si può richiedere che esso sorga una volta che tali attività si siano concluse e che gli elementi di prova siano stati raccolti (pur potendosi configurare eccezioni che, tuttavia, necessiterebbero di uno scrutinio giudiziale e di una verifica a cadenza regolare). Poiché l'accesso a tali informazioni può dunque essere ristretto per ragioni cogenti, particolarmente importante è l'esistenza di un effettivo organo di controllo della legalità del ricorso a tali misure e, inoltre, sulle competenti autorità gravano obblighi

[478] BVerfG, Primo Senato, 20 aprile 2016, 1 BvR 966/09, 1 BvR 1140/09, §§ 120-122.
[479] BVerfG, Primo Senato, 20 aprile 2016, 1 BvR 966/09, 1 BvR 1140/09, §§ 127-129.

di informazione nei confronti del Parlamento e dell'opinione pubblica, i quali devono essere regolarmente relazionati sul ricorso a tali misure[480].

2.3.4. Lo scrutinio concreto sulle disposizioni impugnate

Una volta inquadrata la questione sotto il profilo dei principi e dei criteri costituzionali di riferimento, il collegio si volge alla verifica concreta della legittimità delle disposizioni impugnate dinanzi a sé. Le prime disposizioni oggetto di scrutinio (art. 20g, §1-3 *BKAG*) riguardano soltanto la sorveglianza nelle vicinanze dell'abitazione o del luogo di dimora di un soggetto, non autorizzando quindi alcuna forma di interferenza con il diritto alla segretezza delle telecomunicazioni (art. 10 GG), né con quello all'inviolabilità del domicilio (art. 13 GG).

Tuttavia, pur nella discrezionalità riconosciuta al legislatore, le disposizioni sono censurate per l'eccessiva ampiezza (*rectius*, l'assenza di sufficiente delimitazione) delle ipotesi in cui si possa fare ricorso a tali tecniche d'indagine, non prevedendo alcun requisito relativo al riscontro di dati empirici che favoriscano una prognosi positiva del giudizio di probabilità di commissione della condotta. Inoltre, se anche si ritiene che l'utilizzo di tali misure per periodi temporali limitati sia ammesso senza necessità di ottenere un favorevole provvedimento giudiziale, esso diviene obbligatorio laddove l'attività di sorveglianza si prolunghi continuativamente per un certo periodo di tempo[481].

Con riferimento alla successiva disposizione impugnata (art. 20h *BKAG*), relativa alla possibilità di effettuare riprese audio-visive all'interno di luoghi di privata dimora, il *BVerfG* argomenta che, pur nel rispetto degli obblighi di perimetrazione dell'ambito di applicazione delle misure ai casi ove si faccia questione di diritti di particolare rilevanza e di previsione del requisito di pericolo imminente, profili di illegittimità costituzionale si ravvisano con riferimento ai soggetti potenziali destinatari di tali misure. In particolare, la disposizione viola il dettato costituzionale, argomenta il collegio, laddove consente il ricorso a tali misure di sorveglianza con

[480] BVerfG, Primo Senato, 20 aprile 2016, 1 BvR 966/09, 1 BvR 1140/09, §§ 134-143.
[481] BVerfG, Primo Senato, 20 aprile 2016, 1 BvR 966/09, 1 BvR 1140/09, §§ 146-177.

riferimento ai luoghi di abitazione di terze parti che con i soggetti sorvegliati intrattengano meri rapporti di conoscenza, in assenza di qualsivoglia coinvolgimento in fasi anche preliminari alla preparazione di condotte penalmente rilevanti.

D'altronde, una tale interferenza è tanto grave da essere paragonabile soltanto a quella che avviene attraverso l'accesso remoto a sistemi informatici. Tale determinazione non esclude comunque che si possa effettuare sorveglianza di tali terze parti all'interno dell'abitazione del soggetto *target*, laddove inevitabile, o ancora che si possano utilizzare tali strumenti per monitorare ciò che avviene all'interno della dimora di una terza parte, con specifico ed esclusivo riferimento alla condotta e all'espressione del pensiero del soggetto sotto sorveglianza[482].

Nulla quaestio, secondo il Tribunale costituzionale federale, sulla misura del monitoraggio audio-video di quanto accade in un luogo di privata dimora fintanto che il ricorso a tale strumento sia autorizzato da un giudice sulla base di circostanze di fatto adeguatamente motivate, né il ripetuto rinnovo di tale autorizzazione è di per sé costituzionalmente illegittimo, potendosi configurare limiti a esso solo per effetto del principio di proporzionalità. Diversamente, il giudice costituzionale ritiene insufficienti i presidi a tutela della area riservata della vita privata. Dato il contesto e i soggetti con i quali solitamente si interagisce al suo interno, deve vigere una presunzione (relativa) di pertinenza delle conversazioni che avvengono all'interno delle mura domestiche a tale area di privatezza, con la conseguenza di doverle interrompere laddove emergano elementi di riservatezza, salvo che siano strumentalmente confusi con comunicazioni relative alla programmazione di condotte di reato.

Inoltre, i dati raccolti andrebbero sottoposti a un'autorità indipendente che ne verifichi la corretta raccolta e la pertinenza all'attività d'indagine, cosa che la legge sotto scrutinio prevede solo con riferimento a quelle registrazioni in automatico su cui siano sorti dei dubbi e non per l'interezza delle stesse, prevedendo inoltre che la cancellazione di quelle non pertinenti possa avvenire soltanto entro un lasso di tempo eccessivamente ristretto[483].

---

[482] BVerfG, Primo Senato, 20 aprile 2016, 1 BvR 966/09, 1 BvR 1140/09, §§ 179-193.
[483] BVerfG, Primo Senato, 20 aprile 2016, 1 BvR 966/09, 1 BvR 1140/09, §§ 194-205.

2.3.5. I nuovi rilievi sull'intangibile sfera di riservatezza della vita privata

Se nulla ha da ridire il *BVerfG* sulle misure di ricerca relative ai profili elettronici di utenti su piattaforme *online*, la previsione del potere di interferenza con il diritto all'integrità e confidenzialità dei sistemi informatici, sancito nella pronuncia del 2008, pur potendo essere conciliata con il dettato costituzionale tramite interpretazione adeguatrice (o costituzionalmente conforme), difetta di adeguata tutela del nucleo intangibile della vita privata. Il *BVerfG* sottolinea l'invasività di tali forme di interferenza ricordando la pressoché totale transizione delle comunicazioni da supporti materiali a vesti elettroniche, sostenendo che il grado di afflittività della ricerca e sorveglianza da remoto su sistemi e dispositivi informatici equivale a quello dell'accesso ai luoghi di privata dimora o domicilio. La disposizione devoluta allo scrutinio del giudice costituzionale dispone che l'adozione delle misure in oggetto sia condizionata alla sussistenza, nel caso concreto, di elementi di fatto spia di un pericolo imminente a un interesse giuridico di straordinaria rilevanza.

Tuttavia, prosegue il collegio, la previsione che autorizza il ricorso alle misure di sorveglianza occulta anticipatamente, sulla base di fatti determinati che testimonino, nel caso concreto, che una minaccia terroristica sia sussistente, deve essere interpretata restrittivamente. In particolare, l'utilizzo degli strumenti in commento sarebbe concesso solo laddove gli elementi raccolti delineino un evento specifico sotto il profilo tipologico e circoscrivibile temporalmente, e quando sia evidente il coinvolgimento di determinati soggetti e la loro identità, così che tali misure possano essere quanto più possibile limitate agli stessi. Alternativamente, anche in assenza di indizi specifici sul genere e il momento in cui la condotta possa avere luogo, può bastare un comportamento individuale tale da fondare una probabilità specifica che il soggetto in questione compia azioni di questo tipo in un futuro prossimo. Poiché tale disposizione riflette la giurisprudenza costituzionale in materia, pur senza richiamo esplicito, essa è da intendersi come parametro interpretativo che consente di armonizzare tale disciplina con il dettato costituzionale[484].

[484] BVerfG, Primo Senato, 20 aprile 2016, 1 BvR 966/09, 1 BvR 1140/09, §§ 206-215.

Se sotto il profilo procedurale il *BVerfG* non avanza rilievi di sorta, sottolineando che tali misure sono concesse da un giudice con provvedimento motivato e con un orizzonte temporale che, per quanto lungo (fino a tre mesi) è comunque determinato e deve essere proporzionato al caso di specie, censure di illegittimità costituzionale vengono ravvisate con riferimento alla tutela della sfera di vita privata specialmente protetta dalla Costituzione. Dato il rischio di raccolta di dati altamente confidenziali associato ai mezzi di ricerca della prova in parola, esplicite forme di tutela e protezione di tale nucleo riservato della vita privata devono essere previste per legge, pur senza dover coincidere con quelle previste per la tutela del domicilio. In questa circostanza è rilevante soprattutto il momento della cognizione dei dati stessi e della lettura combinata che se ne può fare per tracciare un ritratto della personalità di un soggetto.

Idealmente, le tecnologie utilizzate dovrebbero essere in grado di scremare automaticamente i dati pertinenti e accessibili da quelli protetti. Tuttavia, laddove ciò non sia possibile, la raccolta può ugualmente avvenire ma la cognizione e l'utilizzo degli stessi deve essere vagliato da un soggetto indipendente prima che l'Ufficio di Polizia Criminale Federale possa accedervi e utilizzarli. Se la disposizione impugnata può essere interpretata conformemente al dettato costituzionale con riferimento al momento della raccolta dei dati, altrettanto non può dirsi, affermano i giudici di Karlsruhe, relativamente alla fase successiva. Infatti, il controllo affidato a un soggetto indipendente non serve solo lo scopo di verificare la legittimità degli atti d'indagine, ma anche di svolgere funzione di filtro per evitare che le autorità di pubblica sicurezza prendano cognizione di informazioni pertinenti tale sfera privata tutelata. Ciò non significa che il soggetto incaricato non possa essere un dipendente dell'autorità in questione, ma che lo svolgimento in concreto e la decisione in materia devono essere presidiate dalla massima indipendenza[485].

[485] BVerfG, Primo Senato, 20 aprile 2016, 1 BvR 966/09, 1 BvR 1140/09, §§ 216-224.

2.3.6. Il giudizio sui mezzi di ricerca della prova "insidiosi"

Fra le disposizioni impugnate, il *BVerfG* si trova a giudicare altresì del potere di disporre l'intercettazione delle comunicazioni fra soggetti, sia con gli strumenti tradizionali a ciò deputati, sia 'alla fonte', vale a dire accedendo ai sistemi informatici fra i quali le comunicazioni siano scambiate, a patto che la sorveglianza si limiti esclusivamente a esse e non si estenda a contenuti estranei alle stesse. Si tratta cioè di una disposizione che 'protegge' lo strumento investigativo dell'intercettazione, mettendolo al riparo da forme di comunicazione innovative capaci di resistere agli strumenti tradizionali con cui tale misura viene posta in essere. Trattandosi di comunicazioni, in ogni caso, il parametro di riferimento non può che essere quello di cui all'art. 10, 1§ *GG*, che giustifica interferenze senz'altro rilevanti con il godimento del diritto in quanto preordinate alla tutela avverso il rischio di condotte terroristiche, a patto che sia garantita una limitazione proporzionata al caso concreto.

Se non vi sono censure costituzionali relative alla sorveglianza applicata a soggetti ritenuti responsabili nei sensi di cui alle rilevanti leggi di pubblica sicurezza, l'allargamento indiscriminato della sfera di applicazione della misura a soggetti a carico dei quali siano stati raccolti soltanto fatti determinati che giustifichino il sospetto che stiano preparando atti terroristici non è ritenuto compatibile con il dettato costituzionale. L'anticipazione dell'ambito di applicazione a una fase precedente che esorbita da una minaccia specifica, pure a fini di prevenzione, violerebbe il principio di certezza del diritto e sarebbe sproporzionatamente ampia. Diversamente, l'estensione della sorveglianza ai messaggi scambiati con terze parti non violerebbe i principi costituzionali in materia, potendo essere interpretata conformemente a essi, circoscrivendone la sfera di applicazione. Inoltre, se pure la disposizione richiede di ottenere un'autorizzazione alla sorveglianza da parte di un giudice, non specifica la necessità di motivare tale provvedimento indicando gli elementi di fatto su cui esso si basa, così difettando di un requisito costituzionalmente prescritto che non può essere colmato in via di interpretazione.

Sotto il profilo della tutela della sfera personale riservata, il collegio riconosce una certa discrezionalità al legislatore in ragione della diversa natura dell'intrusione in commento rispetto al monitoraggio delle condotte in luoghi di privata dimora,

ritenendo che spetti allo stesso legislatore determinare la necessità o meno di una fase di *screening* da parte di un'autorità indipendente. Con riferimento a tali requisiti, le disposizioni impugnate sono ritenute dal giudice costituzionale legittime, se non per il troppo breve periodo di tempo previsto dai protocolli sulla cancellazione delle conversazioni registrate. Analoghe censure e considerazioni sono inoltre svolte con riferimento ai dati relativi alle comunicazioni telefoniche (contatti, frequenza, orari, etc.)[486].

Parimenti insufficienti vengono qualificate le tutele predisposte per la protezione di gruppi professionali che, in ragione della natura della loro attività, godono di un particolare diritto alla confidenzialità delle proprie comunicazioni (in particolare con riferimento al caso degli avvocati). Ulteriori rilievi sono espressi dal giudice costituzionale con riferimento alla mancata sanzione formale di controlli a intervalli regolari sull'esercizio di tali poteri, così come sull'assenza di obblighi di riferire al legislatore. Vengono invece bocciate su tutta la linea le disposizioni relative alla cancellazione dei dati raccolti e ritenuti non pertinenti[487].

Il *BVerfG* censura inoltre ulteriori disposizioni relative all'uso, alla cancellazione e al trasferimento ad autorità straniere dei dati e degli elementi di prova ottenuti, che per ragioni di sintesi e di omogeneità della trattazione non vengono prese in considerazione in questa sede.

2.3.7. La modulazione temporale degli effetti e il presidio degli interessi costituzionali individuali

Interessante, sotto il profilo delle tecniche decisorie, è l'opzione del Tribunale di Karlsruhe per una declaratoria di illegittimità costituzionale divaricata in quanto alla portata temporale degli effetti. Per l'autorizzazione alla sorveglianza in luoghi di privata dimora e per un'ulteriore disposizione in tema di cancellazione dei dati l'effetto ablativo della sentenza è immediato. Con riferimento alle altre norme dichiarate costituzionalmente illegittime, invece, la pronuncia prevede un'efficacia differita, tale da lasciarle in vigore fino al 30 giugno 2018, poiché l'impianto generale

[486] BVerfG, Primo Senato, 20 aprile 2016, 1 BvR 966/09, 1 BvR 1140/09, §§ 228-252.
[487] BVerfG, Primo Senato, 20 aprile 2016, 1 BvR 966/09, 1 BvR 1140/09, §§ 253-274.

dei poteri conferiti alle autorità non è stato sanzionato, ma vi è il difetto di disposizioni che assicurino il rispetto del principio di proporzionalità, che la sentenza invita il legislatore a inserire. Tale effetto differito, tuttavia, viene affiancato da alcuni requisiti che il giudice costituzionale introduce in ciò che appare un afflato di legislazione positiva, ad esempio l'autorizzazione da parte di un giudice delle misure di sorveglianza su luoghi di privata dimora.

È d'uopo dare conto del fatto che, a seguito delle due pronunce adottate in materia dal Tribunale costituzionale federale, il legislatore tedesco sia intervenuto, nell'ambito di un più generale riassetto delle norme relative al processo penale[488], dettando disposizioni dettagliate sull'utilizzo dei *trojans* tanto a fini preventivi quanto a fini di repressione, distinguendo in concreto fra quelle operazioni di intercettazione vera e propria di telecomunicazioni (*Quellen-TKÜ*), che attraverso una *fictio iuris* vengono ammesse anche "a ritroso" (cioè nei confronti di quelle comunicazioni già avvenute), e le cd. perquisizioni online (*Online Durchsuchung*), con riferimento alle quali sono previste garanzie più rigorose dato la grande intrusività delle stesse. Sul tema non si può escludere un nuovo intervento della giurisprudenza costituzionale, anche in considerazione delle voci critiche che si sono levate nei mesi successivi l'entrata in vigore delle nuove disposizioni[489].

Come si desume dalla diffusa trattazione di cui sopra, il giudice delle leggi tedesco adotta un approccio marcato da una vena di certo garantismo a favore della sfera personale delle prerogative individuali dei cittadini, che si esemplifica in due principali direzioni. Da un lato, il *BVerfG*, pur riconoscendo al legislatore una certa discrezionalità nella determinazione degli strumenti attraverso i quali perseguire fini meritevoli di tutela, sottolinea che il ricorso a misure intrusive che interferiscano pesantemente con il godimento di diritti costituzionalmente protetti deve necessariamente rispondere a criteri di proporzionalità. A questo fine, il bene giuridico che si intenda tutelare deve essere di importanza tale da giustificare la compressione

[488] *Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens*, (BGBl, I. 2017, p. 3202).
[489] L. Parlato, *Il legislatore tedesco approfitta di una più ampia riforma per disciplinare le perquisizioni* online, in *Cass. pen.*, 2, 2019, 854-872; v. *Id.*, *Problemi insoluti: le perquisizioni* on-line, in G. Giostra-R. Orlandi (a cura di), *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, Torino, Giappichelli, 2018, 297 ss.

di un diverso bene giuridico (in ipotesi "più sacrificabile"). Peraltro, tale enfasi sulla necessità dell'intervento ablativo di una prerogativa individuale ai fini del perseguimento di un altro rilevante bene della vita echeggia la rilevante giurisprudenza della Corte europea dei diritti dell'uomo in ambito di tutela della vita privata (cfr. Cap. III, §1.2).

Secondariamente, un certo significato non si può negare alla riaffermazione, da parte del collegio, dell'obbligo di rispettare il nucleo duro (*wesensgehalt*) del diritto sancito dalla *Grundgesetz*, anche se i giudici di Karlsruhe non si spingono fino a proibire, laddove la sorveglianza si estenda in una "zona grigia", il completamento dell'operazione. Essi impongono però che l'attività sia presidiata da un adeguato controllo sulla qualità dei dati raccolti in una fase successiva a quella della raccolta[490].

Il riferimento al principio di proporzionalità non può essere considerato episodico o circoscrivibile alle circostanze del caso di specie, sulla base di un'opzione interpretativa discrezionale, poiché è la stessa giurisprudenza costituzionale federale a sottoporre con costanza l'esercizio dei pubblici poteri a uno scrutinio che si articola su una struttura precisa. Alla base di essa si colloca la verifica della proporzionalità delle misure adottate, intesa quale elemento imprescindibile che si desume dall'impegno della *Grundgesetz* a garantire lo stato di diritto. Tale vaglio giurisdizionale si sviluppa in un percorso trifasico, che contempla una prima identificazione delle prerogative costituzionali oggetto di limitazione da parte delle autorità pubbliche e del grado di afflittività che date misure impongono sul godimento delle medesime. Segue una determinazione degli interessi giuridici che vengono perseguiti tramite l'adozione delle iniziative che sfocino in limitazioni dei diritti, con preferenza per la tutela del diritto alla vita, all'integrità fisica e alla libertà personale. Infine, si paragona la lesione cagionata dalla restrizione di uno o più diritti con gli interessi che attraverso il ricorso a tale misura si possano perseguire o garantire (cd. verifica della proporzionalità in senso stretto).

---

[490] Entrambi i profili sono illustrati da F. Nicolicchia, *I limiti fissati dalla Corte costituzionale tedesca agli strumenti di controllo tecnologico occulto: spunti per una trasposizione nell'ordinamento italiano*, in *Archivio penale*, 2, 2017, disponibile all'url: http://www.archiviopenale.it/File/DownloadArticolo?codice=a6b3ff73-ab8a-40ba-9fb1-422ebfd12304&idarticolo=15150 (ultimo accesso: 11 maggio 2020).

Nel caso in commento lo scrutinio del *BVerfG* si è concentrato sulle modalità con cui si fosse riusciti a minimizzare le conseguenze sul godimento dei diritti derivanti dai poteri riconosciuti dalle disposizioni impugnate, in particolare attraverso la predisposizione di garanzie sotto il profilo procedurale[491]. Si tenga presente che, mentre i primi due livelli di verifica pertengono al riscontro dell'idoneità e della necessità della misura (questa seconda nel senso di minimo grado di interferenza possibile), è il terzo che introduce il vero e proprio bilanciamento fra valori, sulla scorta di una concezione dei diritti fondamentali proprio in termini di valori a formulazione indeterminata e natura non assoluta, passibili di limitazione quando in conflitto con altri diritti del medesimo rango[492] (v. anche *infra*, Cap. V).

3. *La tutela dello spazio privato digitale nella giurisprudenza statunitense.*

3.1. L'origine della sorveglianza da remoto: strumenti e strategie delle agenzie di law enforcement.

Anche nel contesto nordamericano i primi dibattiti sul monitoraggio e la sorveglianza da remoto a fini di prevenzione e perseguimento di condotte di reato risalgono al primo decennio del XXI secolo. Diversamente da quanto accaduto in Germania, tuttavia, il fenomeno sembra essersi guadagnato l'attenzione dei giuristi in conseguenza di un ricorso a tali strumenti da parte delle agenzie di *law enforcement* nella prassi, secondo un approccio che si potrebbe definire dal basso (*bottom-up*), in opposizione alla dinamica tedesca, ove sono state piuttosto iniziative legislative (statali prima e federali poi) a porre sul tavolo il tema (secondo una logica dall'alto, *top-down*).

Come si intende dimostrare nella trattazione che segue, anche nel contesto statunitense il formante giurisprudenziale è stato chiamato a svolgere un ruolo rilevante, pesando e bilanciando le esigenze investigative sottese al ricorso a tali

---

[491] R.A. Miller, *A Pantomime of Privacy: Terrorism and Investigating Powers in German Constitutional Law*, in 58 *B.C. L. Rev.*, 2017, 1545-1628, 1570-1571.

[492] Sull'origine del principio di proporzionalità nell'ordinamento tedesco v. E.A. Imparato, *Diritti fondamentali e principio di proporzionalità: dalla "tirannia dei valori" alla tirannia dei giudici nell'esempio tedesco*, in *Id.* (a cura di), *Diritti o giudizi? Le libertà tra regole e casistica interna ed europea in una riflessione comparata*, Napoli, uniorPress, 2014, 31-51, e i relativi riferimenti bibliografici in nota.

strumenti da un lato con la protezione delle prerogative individuali dei cittadini dall'altro. Ciononostante, l'atteggiamento del vertice del giudiziario federale si è dimostrato tendenzialmente più cauto nel delineare in concreto dei requisiti ai quali sottoporre tale potere pubblico, anche in ragione dell'assenza di una disciplina legislativa di dettaglio come quella tedesca, su cui pure il *BVerfG* non ha lesinato osservazioni e rilievi critici.

L'agenzia investigativa federale (*Federal Bureau of Investigation*, *postea FBI*) fece ricorso per la prima volta a uno strumento informatico del tipo in parola (in particolare un *software* di natura *key-logger*) in un'indagine a carico del presunto organizzatore di scommesse clandestine e usuraio Nicodemo Scarfo[493]. Nel corso di un'ispezione dei luoghi in cui l'attività commerciale del suddetto aveva la propria sede, in esecuzione di un apposito mandato, l'*FBI* era acceduta al computer in dotazione all'azienda, ma senza riuscire a consultare tutti i *file* presenti sullo stesso. Per ovviare a tale inconveniente, la medesima autorità investigativa aveva richiesto e ottenuto un secondo mandato che consentisse l'installazione di un apposito programma su tale computer, affinché fosse possibile accedere a quei dati diversamente protetti da un sistema di decrittazione. Tramite questo stratagemma, gli inquirenti raccolsero elementi di prova che ritenevano potessero far valere in giudizio nei confronti del soggetto in questione.

Le rimostranze della difesa dell'imputato sull'ammissibilità delle prove raccolte con tali modalità costrinsero il Governo federale a invocare le disposizioni rilevanti del *Classified Information Procedures Act*[494], al fine di evitare che la pubblicità del procedimento potesse mettere a repentaglio la sicurezza nazionale tramite il disvelamento della modalità di funzionamento di *software* del tipo *key-logger* in dotazione alle agenzie federali di pubblica sicurezza. L'istanza avverso l'ammissione delle prove così raccolte fu infine rigettata dal giudice competente, che respinse le

[493] Le caratteristiche del *software* utilizzato sono descritte nel cd. *Murch affidavit*, disponibile all'url: https://www.epic.org/crypto/scarfo/murch_aff.pdf (ultimo accesso: 1 giugno 2020).

[494] Usualmente abbreviato in CIPA, Pub.L. 96–456, 94 Stat. 2025. Questo *statute* fu introdotto per prevenire il fenomeno cd. del *graymailing*, cioè la necessità dell'amministrazione di dirimere il dilemma fra il ricorso in giudizio a elementi di prova la cui presentazione possa risultare nel disvelamento di informazioni secretate (in particolare laddove sia l'imputato a minacciare di rivelarle) o la rinuncia alla persecuzione in sede penale dell'imputato. L'atto consente l'utilizzo di tali informazioni senza che esse siano rese note al pubblico, per proteggerne la segretezza.

censure che sostenevano l'illegittimità del mandato perché redatto in termini troppo generali, in presunta violazione del IV Emendamento, e poiché il programma utilizzato sarebbe stato in grado di intercettare comunicazioni che avvenissero tra quel terminale e un altro sistema informatico (il *software* era infatti stato programmato così da registrare i dati battuti sulla tastiera singolarmente, pertanto non violava le disposizioni legislative in materia di intercettazione delle comunicazioni telefoniche o elettroniche).

È interessante notare come il giudice autore dell'ordinanza in questione si premuri di sottolineare il ruolo delle corti come bastioni della libertà nella società odierna, funzionali alla protezione dei diritti individuali contemplati dalla Costituzione. La diffusione di strumenti tecnologici sempre più avanzati, argomenta il magistrato, impone di mantenere alta la guardia per evitare che i diritti costituzionalmente sanciti siano soppressi per mano della moderna tecnologia. D'altro canto, conclude, di questi strumenti si serve chi intende delinquere, rendendo le condotte penalmente rilevanti più ostiche da prevenire e sopprimere. A patto di una scrupolosa osservanza dei requisiti costituzionali in materia, dunque, la capacità delle autorità di perseguire tali malefatte non deve incontrare ostacoli[495].

Di poco successivo al caso Scarfo, il cd. caso Alba-Forrester costituisce un secondo, rilevante esempio di ricorso delle agenzie di *law enforcement* a strumenti di monitoraggio da remoto per la prevenzione e la repressione delle condotte penalmente rilevanti. In particolare, nel caso in questione un agente della *Drug Enforcement Administration* (*DEA*) aveva ottenuto un apposito mandato da un giudice federale per accedere a locali ove si sospettava vi fosse il quartier generale di un'organizzazione dedita alla produzione e al traffico di sostanze stupefacenti (nello specifico, Ecstasy). Lo scopo era quello di installare su un terminale un programma spia in grado sorvegliare l'attività di navigazione in Internet e lo scambio di e-mail da parte dell'utente (il *software* usato ricorreva alla tecnica cd. del *port mirroring*[496]) e,

[495] *Letter opinion and order* nel caso *United States v. Nicodemo S. Scarfo,* 180 F.Supp.2d 572, U.S. District Court for the District of New Jersey, 26 Dicembre 2001, disponibile all'url: https://www.epic.org/crypto/scarfo/opinion.html (ultimo accesso: 1 giugno 2020).

[496] Per un sintetico approfondimento sul funzionamento di questo metodo di raccolta dei pacchetti di dati si rinvia a S. Cooper, *The Ultimate Guide to Port Mirroring*, disponibile all'url:

successivamente, anche di captare e trasmettere gli input da tastiera, secondo il modello del programma *key-logger* già utilizzato nel caso Scarfo.

Lo stesso imputato, impugnando la condanna pronunciata all'esito del processo con giuria dal giudice distrettuale, contestava l'ammissibilità degli elementi di prova raccolti tramite l'attività di monitoraggio occulto in quanto in violazione dei propri diritti sanciti dal IV Emendamento alla Costituzione federale e sosteneva che tale attività non ricadesse entro le fattispecie di cui alla pertinente legislazione federale[497]. La Corte d'appello federale per il Nono circuito respinse entrambe le doglianze, in primo luogo richiamando la giurisprudenza secondo la quale il ricorso a uno strumento del tipo *pen register*, vale a dire un registro in cui viene presa nota dei dati dei mittenti e destinatari delle comunicazioni intrattenute da un utente di una linea telefonica, non è configurabile come una perquisizione ai sensi del IV Emendamento poiché si limita a dati esteriori alla cui segretezza l'utilizzatore rinuncia con il contratto di fornitura del servizio stipulato con la compagnia telefonica[498].

In assenza di qualsivoglia precedente relativo a strumenti informatici, il giudice d'appello ritenne in tale circostanza di poter assimilare il funzionamento del programma spia a quello di un *pen register*, concludendo quindi che l'operazione della *DEA* non ricadesse nell'ambito di applicazione del IV Emendamento. Infatti, la raccolta degli indirizzi e-mail di chi scambia messaggi con un utente e dei siti Internet visitati è una delle condizioni che gli utenti sottoscrivono con gli *Internet Service Provider* per ottenere la fornitura del servizio. Dinanzi all'esistenza di una rinuncia alla riservatezza di tali dati a favore di terzi (l'*ISP*, appunto), qualsiasi tentativo di accampare una *reasonable expectation of privacy* a quel proposito dovrà essere ritenuta infondata[499].

Inoltre, proseguì il collegio giudicante, lo strumento di sorveglianza in questione consentiva di prendere conoscenza soltanto dell'identità di coloro che ricevevano messaggi di posta elettronica dall'utente o a esso li inviavano, senza che ne

---

https://www.comparitech.com/net-admin/ultimate-guide-to-port-mirroring/ (ultimo accesso: 17 giugno 2020).

[497] Cd. *Federal Pen Register Statute*, 18 U.S.C. § 206.

[498] Cd. *third party exception*, v. *Smith v. Maryland*, 442 U.S. 735 (1979).

[499] *United States v. Forrester*, 495 F.3d 1041, U.S. Court of Appeals for the Ninth Circuit, 6-25 luglio 2007.

fosse disvelato il contenuto. La Corte d'appello applicò dunque una analogia a tutto tondo fra l'invio di lettere cartacee tramite i servizi postali e quello di messaggi di posta elettronica per mezzo della tecnologia informatica. In entrambi i casi il contenuto è protetto dall'intrusione della pubblica autorità e del vettore dalle garanzie del IV Emendamento, ma le informazioni esteriori, desumibili dall'esterno della busta o dai campi del mittente e destinatario del messaggio digitale sono esclusi da tale tutela, poiché l'affidamento al servizio di posta o all'*ISP* costituisce già una rinuncia alla segretezza di tale informazione. Sul punto, il giudice precisò altresì che quanto deciso con riferimento ai sistemi di *pen register* non andasse inteso come applicabile in ogni caso ad altre forme di monitoraggio occulto più intrusive.

La Corte respinse anche la seconda doglianza in tema probatorio, sostenendo come, anche se non si ricadesse nell'ipotesi di uno strumento del tipo *pen register*, l'appellante non aveva ragione di chiedere la non ammissione di tali elementi di prova, che, in ogni caso, avevano rivestito un'importanza secondaria e solo corroborante di altri ben più gravi e circostanziati elementi di prova delle condotte di reato.

Sebbene strumenti del genere di quelli impiegati nei due casi di cui sopra fossero già disponibili da anni, alla fine del primo decennio del XXI secolo non erano chiare le dimensioni del fenomeno quando riferito all'uso da parte delle autorità di pubblica sicurezza[500]. Si ritiene che il primo strumento di questo tipo sviluppato direttamente da un'agenzia federale sia stato il *software* soprannominato *Carnivore*, che consentiva di monitorare il contenuto di comunicazioni elettroniche tramite e-mail e *chat rooms* ma la cui operatività poteva altresì essere circoscritta alla raccolta dei dati esteriori delle comunicazioni (mittenti e destinatari delle comunicazioni). Tale versatilità lo rendeva un programma flessibile e modulabile alle esigenze del caso concreto e alle prescrizioni contenute nel mandato ottenuto dall'autorità giudiziaria. La particolarità di *Carnivore*, che lo distingueva dagli *spyware* veri e propri, era che esso non veniva installato sul dispositivo *target* in uso all'utente, bensì funzionava come una scatola nera collocata presso i server dell'*ISP* che fornivano il servizio di linea all'utilizzatore del dispositivo.

---

[500] D. McCullagh, *Feds use keylogger to thwart PGP, Hushmail*, disponibile all'url: https://www.cnet.com/news/feds-use-keylogger-to-thwart-pgp-hushmail/ (ultimo accesso: 17 giugno 2020).

Altro programma spia sviluppato nel medesimo periodo di tempo, ma rientrante nel quadro dei veri e propri *spyware*, in quanto fondato sull'installazione sul dispositivo in uso al soggetto su cui vertano le indagini, è il cd. *Magic Lantern*. Creato anch'esso dall'*FBI*, questo secondo programma, a differenza di *Carnivore* che si basava sullo strumento del *pen register*, applica una tecnologia del tipo *key-logger*, che quindi basa la raccolta di informazioni sulle digitazioni degli utenti sulla tastiera per superare le barriere costituite da sistemi di decrittazione tramite *password*. Il rischio associato, qui, è quello di raccogliere anche informazioni sul contenuto di comunicazioni elettroniche dell'utente. Si tratta della medesima tecnologia utilizzata dalle autorità pubbliche nei casi *Scarfo* e *Alba-Forrester* di cui sopra. Peraltro, *Magic Lantern* è considerato il programma utilizzato nel primo caso noto di sorveglianza tramite inoculazione da remoto da parte dell'*FBI*, nell'ambito dell'indagine cd. *Operation Trail Mix*¸ rivolta nei confronti di attività di sabotaggio di un gruppo animalista a danno di una società di sperimentazione scientifica sulla fauna animale[501].

Successivamente, l'*FBI* ha altresì chiesto e ottenuto il ricorso a un programma spia di creazione federale soprannominato *Computer & Internet Protocol Address Verifier* (*CIPAV*), che consente di individuare l'identificativo IP di un dato computer connesso alla rete Internet e di trasmetterlo alle autorità di pubblica sicurezza, per poi passare in modalità *pen register*. Come per *Magic Lantern*, anche *CIPAV* si installa da remoto 'ingannando' il sistema informatico *target*, che evidentemente non lo riconosce come programma spia e ne consente l'installazione all'insaputa dell'utente. Tale strumento fu usato nel caso delle ripetute minacce di far esplodere una bomba presso la *Timberline High School of Lacey* nel 2007, poi ricondotte a uno studente che fu identificato installando il *software* spia per mezzo di un apposito link di *phishing*[502].

Un ulteriore forma di *government hacking*, seppur differente sotto diversi aspetti dalle precedenti, è quella denominata *watering hole attack*, che si basa sulla strategia cd. dell'avvelenamento dei pozzi. Si tratta cioè di un sistema che infetta tutti coloro che

[501] K.E. Aucoin, *The Spider's Parlor: Government Malware on the Dark Web*, in 69 *Hastings L.J.*, 2018, 1444-1445.

[502] Per una disamina dettagliata sui tre tipi di *fedware* e alcune considerazioni di *policymaking*, per quanto non del tutto recenti, v. B. Lawson, *What Not to Ware: As Congress Struggles against Spyware, the FBI Develops Its Own*, in 35 *Rutgers Computer & Tech. L.J.*, 2008, 77-103.

accedono o visitano una o più determinate pagine o siti web, consentendo di tracciarne l'indirizzo IP e di ottenere i dettagli personali dell'utente tramite un apposito mandato presentato all'*ISP*. Questa tecnica è stata utilizzata in più occasioni dalle agenzie di *law enforcement* per il perseguimento di attività caratterizzate dalla natura di contrabbando o vietate e che avvenivano sul cd. *dark web*, in particolare reati attinenti alla pedopornografia[503].

3.2. La rilettura della reasonable expectation of privacy *nella recente giurisprudenza federale.*

Avendo tracciato un quadro sintetico, ma auspicabilmente a tutto tondo, sulle modalità adottate dalle agenzie federali per infiltrare i dispositivi informatici o rintracciare l'identità dei loro utenti a fini di prevenzione o repressione del crimine, è d'uopo riprendere quanto accennato sopra con riferimento all'inquadramento di tali tecniche d'indagine. Tale analisi non può prescindere dalla sottolineatura di come la transizione da un mondo prevalentemente animato da interazioni personali fisiche e materiali a uno in cui la comunicazione digitale la fa da padrone abbia contribuito a rendere meno evidente la differenza fra i casi in cui sussista una *reasonable expectation of privacy* o meno. A tal fine soccorre, come spesso accade, la giurisprudenza federale (soprattutto, ma non soltanto, da parte della Corte Suprema): il giudiziario ha infatti affrontato il tema in un limitato ma significativo numero di pronunce, attraverso le quali è possibile operare una ricostruzione della concezione presente delle garanzie di cui al IV Emendamento in un contesto digitale.

Come illustrato in precedenza (v. *supra*, Cap. III, §3.6), a partire dal celebre caso *Katz v. United States*[504], la giurisprudenza federale ha superato l'interpretazione consolidata del IV Emendamento secondo la quale la disposizione proteggeva i luoghi e gli spazi fisici (concezione proprietaria della *privacy*). Essa ha sancito come il testo fosse preordinato a proteggere le persone e quindi si basasse su una duplice

[503] I più noti sono la cd. Operazione Torpedo, l'intervento che ha consentito di spegnere i server di *Freedom House* e la cd. *Operation Pacifier*, v. K.E. Aucoin, *op. cit.*, 1446 ss.
[504] 389 U.S. 347 (1967).

sfaccettatura di riservatezza, quella dell'aspettativa soggettiva della persona che compieva l'atto comunicativo e quella dell'oggettiva comprensione degli altri consociati che il soggetto volesse mantenere il contenuto di tale attività privato. Tale rigorosa tutela viene, tuttavia, temperata dalla cd. *third party exception*, a norma della quale non esiste una ragionevole aspettativa di riservatezza laddove determinate informazioni siano trasmesse a una qualsiasi terza parte (anche in forza di disposizioni contrattuali di servizio, come quelle che regolano la fornitura di servizi di telefonia, di rete Internet o di servizi bancari)[505].

La cornice di riferimento sembrava dunque sufficientemente chiara e adeguata a regolare un mondo di comunicazioni analogiche; tuttavia, la sempre maggior diffusione delle forme di comunicazione elettroniche ha costretto i giudici, dinanzi all'incapacità del Congresso di disciplinare organicamente la materia, a riesaminare nell'ultimo decennio la questione dell'interpretazione del IV Emendamento, pervenendo a conclusioni non del tutto coerenti fra loro anche a distanza di pochi anni.

3.3. La giurisprudenza delle corti inferiori

Le corti federali distrettuali e d'appello hanno avuto modo di pronunciarsi con maggiore frequenza sui temi in parola, in particolare occupandosi direttamente tanto dell'estensione dell'ambito di applicazione del IV Emendamento alle comunicazioni in forma digitale, quanto della sussumibilità sotto la cornice della disposizione del tracciamento degli indirizzi IP degli utenti tramite il meccanismo del *watering hole*.

Per quanto concerne il primo tema, si segnala il caso *US v. Warshak*[506], ove il giudice d'appello adito era chiamato a decidere sull'impugnazione di una precedente pronuncia basata, sotto il profilo probatorio, su comunicazioni elettroniche ottenute da un ente federale tramite un'apposita richiesta, priva di mandato, a un *ISP* di conservazione dei contenuti delle e-mail inviate e ricevute da un soggetto. La decisione, il cui principio di diritto non è stato finora contestato o denegato da altri giudici di pari grado, ha stabilito che il sottoscrittore di un servizio di posta elettronica

[505] *United States v. Miller*, 425 U.S. 435 (1976); *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979).
[506] U.S. Court of Appeals for the Sixth Circuit, 631 F.3d 266, 14 dicembre 2010.

detiene una *reasonable expectation of privacy* nei confronti del contenuto delle proprie comunicazioni, per cui serve un mandato per poterle chiedere al fornitore di servizi Internet. Tale pronuncia implicava l'illegittimità costituzionale dello *Stored Communications Act*[507], il quale consentiva appunto di procedere all'esperimento di tali invasivi mezzi di ricerca della prova anche senza aver ottenuto un mandato da un organo giurisdizionale, così violando il IV Emendamento. Ciò, nella controversia concreta, non implicò l'inutilizzabilità degli elementi di prova raccolti per l'applicazione della cd. *good faith exception*[508].

Il principio più significativo sancito dalla pronuncia, tuttavia, è proprio che la *third party exception* si applica soltanto ai cd. metadati delle comunicazioni, cioè quei dati esteriori alla cui riservatezza si rinuncia consentendo alla stipula del contratto di fornitura del servizio[509], non estendendosi altresì al contenuto di tali comunicazioni, che rimane coperto da una *reasonable expectation of privacy* (tanto soggettiva quanto oggettiva). Peraltro, sottolinea il giudice d'appello a supporto della propria argomentazione, l'*ISP* nel caso di specie è mero intermediario del contenuto di tali comunicazioni e non destinatario, come era l'istituto di credito nel caso *Miller*.

Con riferimento al secondo dei temi introdotti sopra, più di recente una corte federale distrettuale ha affermato, nel caso *US v. Lough*[510], che non sussiste alcuna ragionevole aspettativa di *privacy* (né sotto il profilo soggettivo, né sotto quello oggettivo) nel mantenimento della riservatezza dell'indirizzo IP trasmesso a una terza parte, anche laddove si sia fatto ricorsi a strumenti in grado di 'mascherare' tale dato, come l'utilizzo del sistema cd. *TOR* (*The Onion Router*)[511]. Questa decisione ribadisce l'attualità, almeno secondo il giudice che l'ha pronunciata, della *third party exception* con riferimento ai dati esteriori di una eventuale comunicazione o di un'attività che si

---

[507] 18 U.S.C. 121 §§ 2701–2712, Pub.L. 99–508.

[508] A norma di questo istituto processuale gli effetti delle attività poste in essere da un soggetto pubblico in esecuzione di una disposizione di legge dichiarata successivamente incostituzionale non decadono laddove tale incostituzionalità non fosse palese ed evidente e, per ciò stesso, il soggetto incaricato di svolgere tale attività avrebbe dovuto rifiutarsi di porla in essere, v. *United States v. Leon*, 468 U.S. 897 (1984).

[509] In ossequio all'esclusione dei sistemi di tipo *pen register* dall'ambito di applicazione del IV emendamento, come già stabilito dalla Corte Suprema in *Smith v. Maryland* (1979).

[510] 221 F. Supp. 3d 770, U.S. District Court for the Northern District of West Virginia, 18 novembre 2016.

[511] R. Dieter, *You've Got Mail: FBI Hacking in* United States v Lough *and Why It Is a Fourth Amendment Search*, in 63 *Vill. L. Rev. Online*, 2018, 101-125.

svolga in rete (in questo caso la consultazione e l'eventuale *download* di determinate pagine o contenuti *online*).

Il portato della pronuncia consiste nel riconoscimento di una patente di legittimità costituzionale al ricorso alla summenzionata tecnica del *watering hole*, fornendo alle autorità investigative uno strumento formidabile per risalire agli autori di condotte di reato che si consumano integralmente in rete (in particolare lo scambio o la consultazione di materiale pedopornografico). Tale strumento può, infatti, essere dispiegato senza la necessità di dover ottenere uno specifico mandato dall'autorità giudiziaria, come avverrebbe laddove si ritenesse tale attività sussumibile sotto la fattispecie di una *search* ai sensi del IV Emendamento.

3.4. La giurisprudenza della Corte Suprema

3.4.1. La ritrosia nel fronteggiare l'uso della tecnologia nel processo penale

La Corte Suprema non ha ancora avuto occasione di esprimersi direttamente in una controversia riguardante l'utilizzo di strumenti di sorveglianza digitale da remoto installati su dispositivi a uso personale, ma nell'ultimo decennio si è confrontata in più occasioni con l'uso della tecnologia nelle indagini penali. Gli approdi della sua giurisprudenza, come si intende illustrare di seguito, non appaiono sempre del tutto agevoli e sembrano testimoniare un certo 'disagio' nel misurarsi con un ambito della vita di relazione umana che è in mutamento continuo e che mal si presterebbe a una regolazione stringente e poco flessibile[512].

Tale impostazione di fondo emerge da quanto scrisse *Justice* Kennedy nell'opinione di maggioranza nel caso *City of Ontario v. Quon*[513], laddove egli sostenne che la prudenza consiglia di esercitare cautela nel trarre dai fatti di causa una regola generale tale da disciplinare l'esistenza e l'ambito di applicazione delle aspettative di riservatezza dei lavoratori, laddove utilizzino strumentazioni elettroniche date in

[512] V., a questo proposito, G. Romeo, *La Corte Suprema e l'approccio minimalista alle nuove tecnologie*, in *Diritti Comparati*, 8 marzo 2012, disponibile all'url: https://www.diritticomparati.it/la-corte-suprema-e-lapproccio-minimalista-alle-nuove-tecnologie/ (ultimo accesso: 18 giugno 2020), nel quale si dà altresì conto del diverso esito in *Jones v. United States* rispetto a *City of Ontario v. Quon*.
[513] 560 U.S. 746 (2010).

dotazione dal datore di lavoro (nel caso di specie, il dipartimento di polizia di una città della California, per cui un ente pubblico). Infatti, prosegue la decisione, questi rapidi mutamenti implicano anche una correlata evoluzione nella percezione delle condotte che siano ritenute accettabili dalla collettività, come l'uso promiscuo (lavorativo e personale) di strumenti in dotazione per fini lavorativi. Per questa ragione, anche nel caso di specie il vertice del giudiziario federale decise la questione evitando di pronunciarsi sul tema in modo pervasivo e limitandosi a ritenere che la perquisizione digitale del dispositivo fosse in realtà ragionevole e pertanto costituzionalmente legittima. Peraltro, tale approccio particolarmente cauto non convinse tutto il collegio, come testimonia la breve ma puntuta *concurring opinion* vergata da *Justice* Scalia, che non condivideva la ritrosia della maggioranza all'applicazione del IV Emendamento alle nuove tecnologie, laddove le circostanze del caso lo richiedessero.

3.4.2. Il ritorno a una lettura 'reificata' del IV Emendamento

Tuttavia, quando due anni dopo si ripresentò l'occasione di misurarsi con il tema, seppur nell'ambito del tracciamento degli spostamenti di soggetti di interesse investigativo tramite tecnologia GPS (*Global Position Monitoring*), pur avendo lanciato il sasso due anni prima, Scalia ritira la mano e guida una maggioranza trasversale (composta, oltre a lui, dai conservatori Thomas, Roberts e Kennedy e dalla *liberal* Sotomayor, sebbene in una decisione senza formali opinioni dissenzienti) a una conclusione per certi versi inattesa. Infatti, in *United States v. Jones*[514], l'installazione di una microspia sul veicolo di un sospettato per reati di narcotraffico viene considerata una perquisizione ai sensi del IV Emendamento e come tale sottoposta al rispetto delle garanzie previste dalla disposizione[515].

In questa pronuncia, *Justice* Scalia, coerentemente con la propria adesione alla scuola originalista, rievoca come un'intrusione fisica su un bene di proprietà privata (cioè l'installazione del dispositivo che trasmette il segnale GPS sul paraurti del veicolo) fosse da intendersi senz'altro come rientrante nel novero delle perquisizioni

[514] 565 U.S. 400 (2012).
[515] Sull'evoluzione del concetto di privacy nel percorso fra *Katz* e *Jones*, v. R.L. Weaver, *Privacy in an Age of Advancing Technology*, in 82 *Miss. L.J.*, 2013, 975-996.

("*searches*") al tempo in cui il *bill of rights* fu approvato ed entrò in vigore. A supporto di tale affermazione, Scalia cita sinteticamente la lunga e consolidata giurisprudenza che, per oltre un secolo e mezzo, ha legato la prerogativa riconosciuta dalla disposizione al diritto di proprietà, sanzionandone regolarmente la violazione tramite l'applicazione del tradizionale istituto di *common law* noto come *trespass* (v. *supra*, Cap. III, §3.2).

Pur riconoscendo che, con la decisione in *Katz v. US*, la giurisprudenza federale aveva adottato un approccio più ampio, abbracciando la teoria della cd. *reasonable expectation of privacy* di cui alla *concurring opinion* di *Justice* Harlan, Scalia sostiene che questa non ha inteso sostituirsi al tradizionale test sul *trespass*, che costituisce un'alternativa laddove la pubblica autorità violi il diritto di proprietà di un soggetto[516]. È interessante notare come, adottando tale approccio e applicandolo al caso del monitoraggio da remoto, l'installazione di un programma spia fisicamente rientrerebbe nello schema tradizionale del *trespass*, mentre il caso più comune dell'inoculazione da remoto rimarrebbe soggetto al solo test della *reasonable expectation of privacy* risalente al caso *Katz*.

Interessante è notare come *Justice* Sotomayor, che pure si unisce alla maggioranza nel ritenere la protezione avverso l'intrusione fisica sul diritto di proprietà il nucleo essenziale e non derogabile della garanzia di cui al IV Emendamento, metta in guardia da possibili abusi. Ciò che la giudice sottolinea è come un uso distorto da parte delle pubbliche autorità di una tecnologia tutto sommato poco costosa e facilmente reperibile come quella GPS possa prestarsi a comportamenti non adeguati, specialmente con riferimento all'esistenza di una ragionevole aspettativa di riservatezza sugli spostamenti da parte dei cittadini. Peraltro, la stessa Sotomayor critica abbastanza apertamente la *third party exception*, mettendo in luce come sia difficilmente adeguata all'era digitale, in cui la comunicazione di dati ai fini dell'esecuzione di un'amplissima gamma di attività quotidiane porti al disvelamento di molte informazioni personali. La soluzione risiederebbe nell'abbandonare la

[516] A supporto di tale affermazione viene citata la decisione di poco successiva in *Alderman v. United States*, 394 U. S. 165, 176 (1969) e la più recente *Soldal v. Cook County*, 506 U. S. 56, 64 (1992).

concezione della riservatezza come necessariamente implicante il mantenimento della segretezza dell'informazione.

Diversamente, la *concurring opinion* di *Justice* Alito critica l'opinione di maggioranza sul presupposto che la stessa applica a una tecnologia del XXI secolo (il tracciamento tramite segnale GPS) un rimedio giuridico del XIX secolo, senza apprezzare come esso non si possa trasferire automaticamente su una fattispecie tanto differente. Non esisteva la possibilità di svolgere un monitoraggio tanto pervasivo e a lungo termine degli spostamenti di un soggetto al tempo, salvo che uno zelante agente di pubblica sicurezza occultasse la propria presenza tanto a lungo su una carrozza o un mezzo a trazione animale (cosa che, fa intendere Alito, è del tutto implausibile). Citando la giurisprudenza successiva a *Katz*, la *concurring opinion* sottolinea come il *trespass* sia non solo non sufficiente ma nemmeno più necessario per stabilire una *reasonable expectation of privacy* e l'esistenza dello stesso non fondi, di per sé stessa, una perquisizione ai sensi del IV Emendamento. Ciò che non convince la minoranza, in questo caso, è la necessità di contatto perché si possa configurare il *trespass*, cosa che renderebbe l'attività una *search*, soggetta alle garanzie di cui al IV Emendamento, anche qualora si protraesse per un molto limitato lasso di tempo, poiché derivata dalla violazione del diritto di proprietà privata del soggetto. Diversamente, laddove tale monitoraggio avvenisse senza contatto diretto (quindi senza *trespass*, ad esempio tramite inoculazione da remoto o in forma di sorveglianza a distanza) ma pure si prolungasse a lungo, ci si troverebbe in un caso di insussistenza di *search* e, pertanto, di impossibilità di invocare le tutele del IV Emendamento.

Justice Alito ritiene quindi che l'applicazione in tutte le circostanze del test elaborato in *Katz* possa soccorrere a tali mancanze, ma precisa che si tratta in ogni caso di un criterio che presenta alcune problematiche. In particolare, le aspettative di riservatezza dei singoli potrebbero non essere costanti e variare con una certa frequenza, soprattutto a fronte di un ambiente digitale che attraversa mutamenti molto rapidi, così frustrando la concreta applicazione di tale principio. Come contraltare, tuttavia, ciò potrebbe spingere il Congresso a legiferare sulla materia per regolamentare il ricorso a mezzi di ricerca della prova così intrusivi. È proprio questa la soluzione che Alito propone, anche se i legislatori federali e statali sono sembrati

finora restii a dare seguito a tale sollecitazione, non lasciando al giudiziario altra scelta, secondo la minoranza, se non quella di interrogarsi sulla ragionevolezza dell'aspettativa di riservatezza del soggetto *target* (che, applicando il test di *Katz*, essa ritiene sussistente).

3.4.3. L'ora è giunta: il riconoscimento dell'alterità degli smartphone rispetto agli elementi di prova tradizionali

Questa apparente spaccatura nella ricostruzione dell'ambito di applicazione del IV Emendamento in seno alla Corte Suprema, tuttavia, sembra essersi ricomposta con la significativa decisione in *Riley v. California*[517], che il collegio ha pronunciato all'unanimità. La sentenza è particolarmente significativa perché riguarda l'ammissibilità probatoria di informazioni che agenti di pubblica sicurezza hanno raccolto, in assenza di un apposito mandato, accedendo allo *smartphone* di un guidatore fermato per una violazione del codice della strada, e che una volta allegate in giudizio ne hanno causato la condanna[518]. La pronuncia segna uno spartiacque rispetto all'approccio timido che aveva contraddistinto la giurisprudenza federale negli anni precedenti, testimoniando un rinnovato spirito della Corte Roberts nell'affrontare anche le questioni giuridiche spinose derivanti dal progresso tecnologico senza schivarle ricorrendo al canone della *constitutional avoidance*[519].

Chief Justice Roberts prende le mosse ricordando che le perquisizioni personali in assenza di mandato sono ragionevoli (e, pertanto, costituzionalmente legittime) solo ove ricadano in una delle eccezioni che la giurisprudenza della stessa Corte ha formulato nel corso del tempo, come quella che consente il ricorso a tale mezzo di ricerca della prova in occasione di un fermo o arresto, ma limitata alla persona dell'arrestato e all'area immediatamente circostante, in specifiche circostanze con

---

[517] 573 U.S. 373 (2014).

[518] Questa la vicenda del ricorrente Riley, mentre la causa trattata congiuntamente originava dal rinvio a giudizio di un soggetto il cui indirizzo di residenza era stato rintracciato da un elenco telefonico dopo che il numero associato all'utenza di rubrica "casa" era apparso sul *display* in occasione di una chiamata in entrata ricevuta a seguito del fermo.

[519] A questo proposito, si rinvia a G. Romeo, *Time is (finally) ripe: la Corte Suprema degli Stati Uniti ridefinisce il bilanciamento tra il diritto alla privacy e le nuove tecnologie*, 3 luglio 2014, disponibile all'url: https://www.diritticomparati.it/time-is-finally-ripe-la-corte-suprema-degli-stati-uniti-ridefinisce-il-bilanciamento-tra-il-diritto/ (ultimo accesso: 18 giugno 2020).

riferimento ai veicoli, anche se senza bisogno di ulteriori ragioni rispetto all'arresto stesso[520]. Dato tale quadro di riferimento, il compito che spetta alla Corte, prosegue Roberts, è quello di verificare l'applicabilità di tali criteri ai moderni telefoni cellulari connessi alla rete Internet. Il *Chief Justice* ci tiene particolarmente a sottolineare la pervasività dell'uso di tali strumenti nella società contemporanea che ricorre a quella che, almeno a prima vista, appare come un'iperbole relativa al ruolo degli smartphone nella società odierna, scrivendo che "*il proverbiale visitatore da Marte potrebbe desumere che si tratti di una significativa parte dell'anatomia umana*"[521].

Richiamando le decisioni che fondano le diverse eccezioni alla regola generale, alle quali si è fatto riferimento in precedenza, il collegio sottolineò come esse soppesino le esigenze di protezione degli agenti di pubblica sicurezza e di salvaguardia della prova in modo efficace per quanto riguarda gli oggetti materiali, ma altrettanto non facciano con riferimento agli oggetti in grado di immagazzinare o scambiare dati in forma digitale. Infatti, i dati contenuti su uno *smartphone* non possono provocare danni all'agente che proceda all'arresto né possono favorire la fuga dell'arrestato, né infine possono essere occultati dall'arrestato.

Sotto questo ultimo aspetto, tuttavia, i dati digitali possono, in ipotesi, opporre due forme di barriera alla conoscenza da parte delle forze di pubblica sicurezza, vale a dire la cancellazione da remoto e la decrittazione dei contenuti tramite la richiesta di chiavi d'accesso. Pur considerando seriamente tali eventualità, Roberts argomentò che si tratta di circostanze tendenzialmente marginali e che, in ogni caso, esistono dei rimedi a tali inconvenienti, quali lo spegnimento del dispositivo con la rimozione della batteria, per evitare che si connetta alla rete, o l'impiego di cd. "gabbie di Faraday", atte a mantenere un telefono cellulare nella modalità sbloccata isolandolo dalle onde radio circostanti. Tutto ciò senza dimenticare che, in caso di necessità, la dottrina delle *exigent circumstances* può sempre soccorrere le autorità di pubblica sicurezza che stiano procedendo all'arresto.

La Corte respinse l'allegazione del governo federale secondo la quale l'ispezione di un telefono cellulare non differirebbe per natura da quella di altri oggetti

[520] Rispettivamente, *Chimel v. California*, 395 U. S. 752 (1969), 762-763; *United States v. Robinson*, 414 U. S. 218 (1973), 235; *Arizona v. Gant*, 556 U. S. 332, 343 (2009).
[521] Pag. 9 Slip op.

trovati sul corpo dell'arrestato, sottolineando come i moderni telefoni cellulari differiscano invece da qualsiasi altro oggetto che si possa rinvenire addosso a un soggetto. La preoccupazione principale di Roberts era a buon diritto rivolta alla molto consistente memoria di cui tali *smartphone* sono dotati, che consente di immagazzinare quantità di informazioni sulla persona (e sulle sue comunicazioni, quali quelle tramite posta elettronica o applicazioni di messaggistica istantanea) non paragonabili ad alcun altro oggetto esistente.

Le statistiche citate dalla pronuncia confermano che l'ampia maggioranza dei cittadini statunitensi adulti utilizza regolarmente tali dispositivi, rendendosi così vulnerabile a violazioni della sfera di riservatezza della vita privata ben più frequenti e intrusive di quanto potesse accadere fino a soltanto due decenni fa. La pronuncia sottolinea con veemenza tali controindicazioni, facendo anche presente che il frequente ricorso all'archiviazione di dati in *cloud* complica ancora maggiormente le cose, rendendo molto difficile distinguere quali informazioni si trovino effettivamente sul dispositivo in questione e quali invece siano consultate tramite accesso a server localizzati altrove.

Roberts cassa, uno dopo l'altro, i vari criteri suggeriti dall'amministrazione per consentire, in date circostanze, tali perquisizioni senza mandato, argomentando che diversamente si sarebbe aperta la strada a una discrezionalità degli agenti impossibile da verificare e limitare. Pur nella consapevolezza delle eventuali difficoltà che la decisione della Corte potesse implicare per la raccolta degli elementi di prova, la pronuncia ribadì l'imprescindibile necessità di ottenere un apposito mandato, sempre potendosi ricorrere, ove ne sussistessero le condizioni, alla teoria delle *exigent circumstances*. Peraltro Alito, nella sola e breve *concurring opinion* di questo caso, coerentemente con quanto già affermato due anni prima, rivolse un appello al legislatore affinché legiferasse espressamente sul tema, senza lasciare che fosse il giudiziario a dover effettuare tale bilanciamento, avendo a disposizione soltanto il dettato del IV Emendamento.

3.4.4. Quali limiti alla third party exception nell'era digitale?

Ad oggi, l'ultimo capitolo di questa saga che ha visto la Corte Suprema confrontarsi con l'applicazione del IV Emendamento alle nuove tecnologie è la contrastata decisione in *Carpenter v. US*[522]. In questo caso, il *Chief Justice* Roberts e l'ala liberal hanno ribadito, di misura (5-4), l'obbligo di ottenere un mandato per poter ottenere da una compagnia telefonica informazioni relative agli spostamenti effettuati da una determinata utenza, desumibili dai dati raccolti dagli stessi fornitori di tali servizi attraverso i segnali scambiati dalle celle telefoniche.

La maggioranza ha escluso che la *third party doctrine* si possa applicare a tali dati, sancendo che un singolo mantiene una legittima aspettativa di riservatezza nella registrazione dei suoi movimenti tramite il sistema di localizzazione che passa dalle celle telefoniche. Ciò implica che la richiesta e l'ottenimento di tali informazioni sia qualificabile come perquisizione, perciò sottoposta all'obbligo di mandato a norma del IV Emendamento. Il collegio ha argomentato che questo tipo di tracciamento è ben più invasivo di quello del caso *Jones* che si limitava, per così dire, al mero veicolo e non a un dispositivo che il singolo porta con sé in ogni luogo e spostamento. L'emissione di onde che sono captate dalle celle telefoniche non può pertanto considerarsi come rinuncia volontaria alla segretezza di tale informazione tale da svincolare la richiesta di ottenimento della stessa dall'obbligo di ottenere un mandato.

La decisione della maggioranza ha offerto l'occasione ai giudici in minoranza per un corposo e differenziato dissenso, a partire da *Justice* Kennedy, il quale ha sottolineato come la localizzazione tramite celle telefoniche sia ben più imprecisa di quanto non lo sia quella tramite GPS e, ciononostante, possa costituire una prova indiziaria significativa della presenza di un sospetto nei pressi di un luogo ove sia stata commessa una condotta di reato, in grado di corroborare delle dichiarazioni testimoniali (era questo il caso in *Carpenter*). Kennedy basava la sua opinione dissenziente sulla *third party doctrine*, ricostruendo come dai casi *Miller e Smith* si desumesse che in assenza di analogie con il diritto proprietario affini a quella costruita dalla Corte nel caso *Katz*, non sussistono pari aspettative di riservatezza (l'utente

[522] 138 S. Ct. 2206 (2018).

telefonico non può accampare alcuna pretesa proprietaria su tali dati). Inoltre, l'amministrazione pubblica può ricorrere a strumenti coercitivi per obbligare i privati a esibire o consegnare documenti o altri elementi di prova nella propria disponibilità. Marcando la differenza tra il mandato e la cd. *subpoena*, che è una richiesta affinché sia il soggetto stesso a consegnare o presentare l'elemento di prova, Kennedy ha ricordato che la stessa Corte Suprema ha già stabilito che tali richieste possono riguardare anche dati commerciali contenenti informazioni personali, poiché si tratta di beni di proprietà dei fornitori del servizio e non degli utenti, venendo così a difettare quel nesso che consente di lamentare un'interferenza con una *reasonable expectation of privacy*.

La *dissenting opinion* di Kennedy critica altresì la lettura che la maggioranza fa dei due precedenti sulla *third party exception*, eccependo che non si tratta di stabilire un bilanciamento con riferimento a quelle informazioni che, se cedute a terzi, perdono la propria pretesa di riservatezza, bensì di un criterio netto, basato sulla volontaria rinuncia alla segretezza di tali informazioni. Quand'anche fosse questa la lettura da adottare, prosegue Kennedy, è difficile concordare che la posizione approssimativa e gli spostamenti di una persona siano meritevoli di una tutela sotto il profilo della riservatezza maggiore rispetto a quella delle comunicazioni telefoniche e delle transizioni bancarie, attraverso le quali si potrebbero ricostruire gli acquisti e molti spostamenti nel dettaglio di ciascun individuo. In conclusione, il criterio adottato dalla maggioranza inibirebbe l'uso di un utile strumento alle agenzie di *law enforcement* e aprirebbe serie questioni di prevedibilità delle informazioni per le quali sarebbe necessario ottenere un previo mandato.

L'opinione dissenziente di *Justice* Thomas è stata l'occasione per un attacco frontale al criterio della *reasonable expectation of privacy* di *Katz*, ricostruendo come la formulazione del IV Emendamento non testimoni alcuna intenzione di riferirsi alla *privacy* (men che meno a una ragionevole aspettativa della stessa), essendo invece la garanzia asseritamente radicata nella titolarità del diritto reale sul bene oggetto di perquisizione o ispezione.

Justice Alito ha ripreso quanto anticipato da Kennedy, vergando un'opinione dissenziente mirata a dimostrare come la decisione della maggioranza ignori le

differenze fra un ordine di esibizione di documenti o oggetti, che consente al destinatario di selezionare e produrre soltanto ciò che sia pertinente a quanto richiesto dalla pubblica autorità, e una perquisizione condotta dalla forza di pubblica sicurezza. Tale confusione porterebbe così la Corte a contraddire la propria consolidata giurisprudenza, a norma della quale non si può accampare alcuna ragionevole aspettativa di riservatezza su beni che appartengono a terzi, come chiarito da *Miller* e *Smith*. Inoltre, paradossalmente decidere in questi termini significherebbe riconoscere una tutela maggiore al soggetto che non è proprietario dei dati in questione rispetto al titolare degli stessi, che invece in forza di una *subpoena* dovrebbe esibirli senza la necessità di una *probable cause*. Ancora una volta, come nei casi precedenti, la soluzione di Alito è chiara quanto radicata nel canone del *judicial restraint*, sostenendo egli che debbano essere i rappresentanti eletti dal popolo a predisporre maggiori garanzie laddove i cittadini ritenessero che quelle del vigente *Telecommunications Act* non siano adeguate.

Justice Gorsuch, infine, ha espresso il proprio punto di vista criticando dapprima la *third party doctrine*, in quanto, se applicata nella sua pienezza consentirebbe alle amministrazioni pubbliche di ottenere e consultare qualsiasi informazione che dal singolo sia stata in qualche modo trasmessa a terzi. Inoltre, egli ha preso di mira anche il *reasonable expectation of privacy* test di *Katz*, perché non offrirebbe ai giudici un criterio decisionale chiaro e sarebbe esso stesso la causa della successiva giurisprudenza erratica sul tema. Il principio da applicare, secondo Gorsuch, è quello tradizionale del diritto reale (di proprietà) sul bene, declinato nel senso di escludere che il mero affidamento di determinati dati a terzi valga di per sé stesso a far cessare ogni interesse giuridico del proprietario sulla riservatezza degli stessi.

Anche qualora non soccorra la legislazione positiva (federale o statale che sia), cionondimeno egli ha sostenuto, rievocando un risalente caso relativo alla tutela del segreto epistolare[523], che esisterebbe un livello minimo di tutela riconosciuta dal IV Emendamento, al di sotto del quale nemmeno l'autorità del Congresso potrebbe spingersi. Non si possono approvare disposizioni legislative che riconoscono la

[523] *Ex parte Jackson*, 96 U.S. 727 (1878).

titolarità dei singoli sulla corrispondenza epistolare o su beni immobili a eccezione dei casi in cui le forze di pubblica sicurezza desiderino ispezionarle senza ragione. Né, proseguiva Gorsuch, tale principio potrebbe essere disinnescato semplicemente ricorrendo a un ordine di esibizione anziché a un mandato. In conclusione, l'opinione dissenziente dell'allora giudice al primo pieno *term* alla Corte Suprema sosteneva che i dati di localizzazione delle celle telefoniche potevano sì godere della tutela del IV Emendamento, con ciò implicando la necessità delle autorità governative di richiedere un mandato per ottenerli. Tuttavia, ciò non avveniva per effetto dell'applicazione del principio *Katz*, bensì in forza della loro natura di *customer proprietary network information* (come riconosciuto dalla legislazione in materia), cioè di beni sui quali sussisteva un interesse proprietario degli utenti che li avevano generati.

4. *La giurisprudenza italiana sull'utilizzo del captatore informatico.*

4.1. Il ruolo di supplenza del giudice di legittimità

Nel caso italiano il principale (e quasi esclusivo) contributo all'individuazione di limiti o requisiti per il ricorso all'uso di strumenti di sorveglianza occulta da remoto ai fini di indagini penali si deve alla giurisprudenza della Corte di cassazione in sede penale. Infatti, è tramite l'analisi di alcune pronunce della stessa che si può verificare a che esiti lo sforzo sussuntivo di tale mezzo di ricerca della prova sotto alcuno di quelli tipici sia pervenuto e quali considerazioni siano state svolte con riferimento alla legittimità costituzionale dell'uso indiscriminato di tali metodi di investigazione. D'altronde, il legislatore si è mosso in ritardo e, peraltro, limitandosi a recepire un recente orientamento della Suprema corte in materia, seppur la disciplina introdotta al termine del 2017 sia ancora in buona sostanza inapplicata in conseguenza di una lunga serie di rinvii dell'avvio dell'applicazione di tale quadro regolatorio (v. *infra*).

Non è da trascurare la riflessione dottrinaria sul tema, che è stata tuttavia finora confinata perlopiù agli studiosi della procedura penale, senza suscitare approfondite riflessioni in ambito costituzionalistico[524]. D'altronde, in assenza di una pronuncia

[524] Il tema è stato oggetto di numerosissimi studi negli ultimi anni, fra i quali si citano soltanto: G. Caneschi, *Le nuove indagini tecnologiche e la tutela dei diritti fondamentali. L'esperienza del captatore*

della Corte costituzionale su questo tema (a oggi peraltro di là da venire, essendo la disciplina di recente introdotta ancora inattuata), la funzione interpretativa e conciliatrice delle disposizioni normative con il dettato costituzionale è esercitata dalla sola giurisprudenza di legittimità.

La prima occasione in cui la Cassazione penale ha avuto modo di misurarsi con il tema in parola risale alla pronuncia del 2009 nel cd. caso Virruso[525]. Nel caso di specie era stata acquisita copia di dati digitali immagazzinati su un dispositivo informatico in uso a un soggetto indagato per reati associativi tramite inoculazione di un captatore informatico, che non solo avrebbe trasmesso le informazioni relative ai *file* presenti sul computer in un dato momento, ma avrebbe altresì consentito di acquisire informazioni anche sui nuovi file creati o modificati da quel momento per i successivi otto mesi. La doglianza del ricorrente poggiava sulle modalità con le quali l'operazione era stata autorizzata, non bastando secondo l'imputato un decreto di acquisizione di atti ai sensi dell'art. 234 c.p.p. Diversamente, sarebbe stato necessario autorizzare delle intercettazioni di comunicazioni informatiche, ai sensi dell'art. 266-bis c.p.p. La Corte d'appello dinanzi al quale la sentenza di prime cure era stata impugnata aveva concluso che tale motivo d'appello non fosse fondato, sul presupposto che ciò che era stato acquisito non era un flusso comunicativo fra soggetti, bensì un flusso unidirezionale di dati interno al sistema operativo del dispositivo in uso. Oltre all'inutilizzabilità del materiale raccolto in spregio alla legge, il ricorrente lamentava altresì l'incostituzionalità di tali elementi di prova, asseritamente raccolti in violazione del principio di inviolabilità domiciliare e della corrispondenza.

La quinta sezione penale della Suprema Corte ha respinto la doglianza su tutta la linea, avallando l'operato del giudice d'appello. Secondo il giudice di legittimità, ottenere copia di informazioni che siano state raccolte in *file* all'interno di un sistema

---

informatico, in *DPC*, 2/2019, 417-429; C. Peloso, *La tutela della riservatezza nell'era delle nuove tecnologie: la vicenda dei captatori informatici per le intercettazioni tra presenti nei reati di terrorismo*, in *DPC*, 1/2017, 149-161; G. Barroccu, *Il captatore informatico: un virus per tutte le stagioni*, in *Diritto penale e processo*, 3/2017, 379-390. Molti altri contributi dottrinari sono stati pubblicati a margine della pronuncia nel caso Scurato e a commento della delega al Governo in materia e dell'adozione del cd. Decreto Orlando. Sul versante pubblicistico, si segnalano S. Grieco, *L'introduzione del virus di Stato nelle intercettazioni ambientali: il trojan e le sue ricadute costituzionali*, in *Dirittifondamentali.it*, 1/2019; S. Romano-C. Sorio, *L'utilizzo dei cd.* trojan horses *nelle indagini penali e la tutela "progressiva" della libertà e segretezza delle comunicazioni*, Law and Media Working Paper Series, no. 14/2016.

[525] Cass. pen., sez. V, sent. n. 16556/2009, 14 ottobre 2009.

informatico, senza che le stesse siano oggetto (ancora) di una comunicazione non è considerato intercettazione di un flusso di comunicazioni[526]. Pertanto, non è applicabile la disciplina dettata dall'art. 266-bis c.p.p. e l'inquadramento corretto di tali mezzi di ricerca della prova sarebbe nella categoria della prova atipica. Nemmeno possono condividersi, proseguiva la Corte di cassazione, le censure di illegittimità costituzionale, non essendo stato il captatore installato in luogo di privata dimora (bensì in un dispositivo presso i locali sede di un ufficio pubblico comunale, quindi in luogo aperto al pubblico) e non avendo esso trasmesso informazioni tratte da una qualche forma di corrispondenza, poiché il contenuto di tali *file* era destinato a essere stampato e solo successivamente consegnato al destinatario.

4.2. Non così in fretta: i distinguo della sentenza Musumeci e le minacce ai diritti costituzionali dei singoli

A conclusioni differenti è giunta una diversa sezione della Cassazione qualche anno dopo nel cd. caso Musumeci[527]. Impugnando l'ordinanza del tribunale del riesame sull'applicazione della misura della custodia cautelare in carcere, un indagato per un reato associativo sosteneva che l'inoculazione del virus informatico e l'intercettazione delle comunicazioni tra presenti svolta tramite l'attivazione da remoto del microfono e della videocamera del dispositivo *target* avrebbe violato l'art. 8 della Conv. EDU, per effetto della captazione di tutti i dati della sfera privata degli utilizzatori, in violazione della rilevante disciplina sulle intercettazioni delle comunicazioni. Inoltre, l'inoculazione su un dispositivo mobile renderebbe la captazione di carattere ambientale e ne consentirebbe l'esperimento anche in luoghi di privata dimora, senza previa indicazione degli stessi nel decreto di autorizzazione del Gip.

La Corte non ha esitato a qualificare l'attivazione del microfono tramite l'uso dello *spyware* come una forma di intercettazione tra presenti (anche nota come intercettazione ambientale). Sulla base di tale presupposto, essa ha tratto dalla disposizione che disciplina questo atto d'indagine (art. 266, c.2 c.p.p.) il corollario che,

[526] Sul significato di tale locuzione si veda Cass. SS.UU., sent. n. 6/2000, 23 febbraio 2000.
[527] Cass. pen., sez. VI, sent. n. 27100/2015, 26 maggio 2015.

nell'autorizzare l'intercettazione di una disposizione tra presenti, il giudice debba indicare nel decreto i luoghi nei quali tale operazione si debba svolgere. Inferire diversamente, argomentava la sesta sezione, violerebbe il portato dell'art. 15 Cost., aprendo la strada a intercettazioni ambientali in ogni luogo. L'obbligo di disporre con atto motivato dell'autorità giudiziaria e solo nei casi stabiliti dalla legge la deroga all'inviolabilità di ogni comunicazione imporrebbe infatti la stretta interpretazione delle disposizioni che disciplinano tali limitazioni della prerogativa costituzionale. A supporto di tale interpretazione, la pronuncia cita la precedente decisione della medesima sezione che consentiva la variazione dei luoghi in cui la captazione delle comunicazioni dovesse svolgersi solo laddove essa rientrasse nelle specificità dell'ambiente oggetto dell'intercettazione[528].

La particolare natura del monitoraggio occulto da remoto tramite virus informatico, ha sostenuto la Corte con riferimento all'attivazione del microfono, richiede che il decreto autorizzativo individui con precisione i luoghi in cui tale captazione avrà luogo, non potendo l'atto limitarsi a indicazioni indeterminate o addirittura assenti. Per quanto concerne la fotocamera, è d'uopo verificare che non siano state effettuate videoriprese all'interno di luoghi di privata dimora o con riferimento ai quali la riservatezza personale fosse tutelata, dovendosi in tal caso ritenere le stesse non utilizzabili a fini probatori[529].

4.3. Un momentaneo punto fermo: il laissez faire *della sentenza Scurato*

Una tale rigorosa impostazione non ha però retto ha lungo, come testimonia l'intervento delle Sezioni Unite l'anno successivo nel cd. caso Scurato[530]. Con tale pronuncia, la Corte di cassazione nella sua composizione più autorevole ha sì concordato con la sesta sezione sulla sussumibilità delle indagini svolte con ricorso al captatore informatico sotto la fattispecie dell'intercettazione cd. ambientale (*rectius*, tra presenti). Peraltro, nel fare ciò essa ha ricordato come sia già stata esclusa in

[528] Cass. pen., sez. VI, sent. n. 15396/2007, 11 dicembre 2007.
[529] A questo proposito la decisione rinvia a Cass. pen., SS. UU., sent. n. 26795/2006, 28 marzo 2006 (Prisco).
[530] Cass. pen., SS. UU., sent. n. 26889/16, 28 aprile 2016.

precedenza la configurabilità di vizi di illegittimità costituzionale della disciplina di tale mezzo di ricerca della prova[531].

Tuttavia, essa ha ritenuto di censurare l'opzione interpretativa secondo la quale l'esperimento di tali intercettazioni necessita di una specifica indicazione, all'interno del decreto che le autorizza, dei luoghi ove le medesime avranno luogo. Infatti, argomentano le Sezioni Unite, tale requisito non si rintraccerebbe né nel dettato normativo (il c.2 dell'art. 266 c.p.p. consente l'intercettazione di comunicazioni tra presenti negli stessi casi di cui al c.1, riferendosi all'ambiente soltanto quando tratta delle intercettazioni nei luoghi di domicilio) né nella rilevante giurisprudenza in materia, anche quella di ambito CEDU[532].

L'indicazione dei luoghi in cui l'intercettazione tramite captatore avvenga, seguita la Corte, è obbligatoria laddove si tratti di luoghi privati, ossia coperti dal principio dell'inviolabilità domiciliare, e a patto che esista un fondato motivo di ritenere che in essi abbia luogo una condotta criminosa o strumentale a essa. Inoltre, come da precedente giurisprudenza, citata anche dalla sentenza Musumeci, la variazione di luogo non rende inutilizzabile l'intercettazione se il luogo diverso rientra nella specificità dell'ambiente oggetto d'intercettazione.

Tuttavia, argomentano le Sezioni Unite, poiché per la natura dello strumento tecnologico utilizzato la previsione della presenza della persona in luogo di domicilio o privata dimora o meno è particolarmente complicata, le captazioni domiciliari in assenza di apposita autorizzazione nel decreto del giudice sono vietate, se non nei casi già previsti dalla legge.

A questo proposito, l'art.13 della l. 203/1991 (che convertiva il d.l. 152/1991) autorizza tali operazioni laddove esse siano necessarie per lo svolgimento delle indagini in relazione ad un delitto di criminalità organizzata o di minaccia col mezzo del telefono in ordine al quale sussistano meramente sufficienti indizi (e non, invece, quei gravi indizi di reato ai quali si riferisce l'art. 267 c.p.p.), aggiungendo che quando tale captazione viene disposta in un procedimento relativo a un delitto di criminalità

[531] Per l'art. 14 Cost., v. Corte cost., sent. 135/2002; per l'art. 15 Cost., v. Cass. pen., sez. I, sent. n. 3133/1997, 12 novembre 1997 (cd. caso Cuomo).
[532] *Vetter c. Francia*, no. 59842/00, Corte EDU, II sez., 31 maggio 2005; *Kennedy v. Regno Unito*, no. 26839/05, Corte EDU, IV sez., 18 maggio 2010.

organizzata che avvenga nei luoghi di domicilio o privata dimora, l'intercettazione è consentita anche se non vi è motivo di ritenere che nei luoghi predetti si stia svolgendo l'attività criminosa.

Le Sezioni Unite smontano l'interpretazione della sentenza Musumeci ancorando la propria motivazione al dato testuale della legge e sottolineando come la locuzione "intercettazioni ambientali" sia utilizzata da dottrina e giurisprudenza ma senza riscontri sotto il profilo normativo. Tale qualifica sarebbe dovuta a una concezione delle intercettazioni di comunicazioni fra presenti ancorata a una visione delle stesse come operabili soltanto attraverso l'apposizione di microspie in ambienti predeterminati, che l'avvento dei moderni *smartphone* ha messo in crisi e costringe a ripensare.

Il principio di diritto che le Sezioni Unite sanciscono in via generale è, dunque, che il decreto autorizzativo dell'attività di intercettazione di comunicazioni tra presenti deve contenere l'indicazione dei luoghi ove le stesse si svolgeranno soltanto laddove esse coinvolgano ambienti di privata dimora o domiciliari e soltanto nei casi in cui sussista un fondato motivo di ritenere che vi si stia svolgendo attività criminosa. Non sarebbe necessaria l'indicazione del luogo specifico nell'intercettazione fra presenti in luoghi diversi da quelli di cui sopra, rimanendo utilizzabile il materiale raccolto laddove il luogo non inizialmente previsto rientri nella tipologia per la quale il decreto autorizzava l'operazione. L'indicazione del luogo è rigorosamente richiesta soltanto laddove siano in gioco le limitazioni al fondamentale diritto alla tutela del domicilio, in presenza di fondato motivo di ritenere che ivi si svolga l'attività criminosa.

4.4. Il doppio binario processuale: la perimetrazione degli effetti della pronuncia

È la norma derogatrice dell'art. 13, l. 203/1991 che fonda la distinzione che le Sezioni Unite tracciano fra i casi comuni e quelli che riguardano l'esperimento delle intercettazioni fra presenti mediante l'uso di captatore informatico. Non è, infatti, tanto l'interesse del soggetto sottoposto a indagine alla tutela del proprio domicilio a rilevare in modo particolare, d'altronde ben si potrebbero effettuare operazioni di

intercettazione entro il domicilio con l'impiego di strumenti tradizionali. Ciò che merita maggiore attenzione è invece la lesione che così si viene a cagionare alla tutela del domicilio dei terzi, i quali ammettano in tali luoghi il soggetto che utilizza il dispositivo infettato e con esso discorrono.

In ogni caso, esimendo i procedimenti per reati di natura associativa dagli obblighi dettati dalla disposizione rilevante, il legislatore ha compiuto una scelta (discrezionale, ma pur sempre nella propria libera disponibilità) operando un bilanciamento fra interessi in questo caso divergenti. La segretezza delle comunicazioni e la tutela del domicilio (anche dei terzi) vengono sacrificate sull'altare della prevenzione di condotte connotate da una gravità e una pericolosità tali da minacciare l'intera collettività. È il giudice che autorizza l'esperimento dell'operazione a dover valutare se si diano i presupposti per il ricorso a questo strumento.

La conclusione che da tale percorso argomentativo la Corte trae è che non sono contrastanti con la tutela costituzionale della segretezza delle comunicazioni e della riservatezza del domicilio le intercettazioni domiciliari tramite captatore informatico. La serietà delle minacce da parte delle organizzazioni criminali, nonché di quelle di ambito terroristico internazionale, che delle potenzialità della rete informatica si servono massicciamente, impone che l'autorità pubblica possa servirsi delle medesime strumentazioni per far fronte nel modo più efficace a tali moderne modalità di pianificazione delle condotte di reato, pur nel rispetto della legge e delle garanzie costituzionali in materia.

La Corte si pone la questione dell'eventuale lesione della dignità della persona umana, tutelata dall'art. 2 Cost., ma condivide quanto suggerito dalla Procura Generale nella memoria depositata in vista dell'udienza[533], vale a dire che a tale rischio si può porre rimedio tramite la sanzione dell'inutilizzabilità di quelle specifiche risultanze acquisite in modo lesivo della personalità dell'indagato. Inoltre, richiamando la rilevante giurisprudenza della Corte di Strasburgo, le Sezioni Unite affermano altresì che le intercettazioni tra presenti tramite il ricorso a captatore informatico non violano l'art. 8 CEDU sulla tutela della vita privata delle persone, in

[533] La memoria della P.G. è liberamente consultabile al seguente url: https://archiviodpc.dirittopenaleuomo.org/upload/1462201608Memoria%20Procura%20generale%20Trojan.pdf (ultimo accesso: 5 luglio 2020).

quanto le modalità sono ispirate al generale principio di proporzionalità delle misure limitative di una libertà. Nel sancire il rilevante principio di diritto, la Corte di cassazione pone l'accento sulla necessità che la qualificazione dell'ipotesi di reato entro i limiti del reato associativo sia basata su indizi sufficienti, sicuri e obiettivi che ne giustifichino la formulazione da parte del pubblico ministero e l'autorizzazione da parte del giudice competente.

La seconda parte della sentenza Scurato è invece dedicata proprio al tema della circoscrizione dei confini dei reati di criminalità organizzata, nei cui confronti vige una meno favorevole disciplina in tema di intercettazioni. Dopo aver passato in rassegna il dato normativo, da cui non si evince un criterio discretivo efficace, le Sezioni Unite prendono in considerazione la rilevante giurisprudenza in materia, sottolineando come sia stata adottata una nozione ampia che, pur escludendo il mero concorso di persone nel reato, valorizza la costituzione di un apparato organizzativo per la commissione di più reati, così non limitando al solo contesto delle mafie tradizionali la categoria.

Sulla base dell'ampia motivazione esposta (almeno per il contesto di un procedimento *de libertate*), le Sezioni Unite hanno respinto il ricorso dello stesso Scurato, confermando le misure cautelari applicate dai giudici di merito, in virtù della ragionevolezza e logicità della motivazione delle medesime e della non sindacabilità del merito dell'apprezzamento in sede di legittimità.

4.5. La delega parlamentare e la riforma promessa (ma sospesa)

Rinviando al Cap. V alcune considerazioni di cui la dottrina si è fatta portatrice nei mesi e anni successivi la suddetta pronuncia, giova ricordare come il legislatore italiano abbia fatto un tentativo di disciplinare il fenomeno, seppur gli effetti pratici di tale iniziativa stentino ancora a vedersi in concreto. Il Parlamento italiano ha infatti delegato il Governo, con l'emanazione della l. 103/2017[534], all'adozione di un decreto legislativo che modificasse la materia delle intercettazioni a fini di indagine, prevedendo fra l'altro che l'attivazione del microfono a opera del captatore

[534] Legge 23 giugno 2017, n. 103, art.1, cc. 82, 83 e 84, lett. a), b), c), d) ed e).

informatico potesse avvenire solo in conseguenza di un'attivazione da remoto e non automaticamente all'inoculazione del captatore. Inoltre, si raccomandava che la registrazione fosse avviata su indicazione della polizia giudiziaria, che ne determina l'orario di inizio e fine, e che l'attivazione fosse sempre ammessa laddove si proceda per reati di cui all'art. 51, cc. 3-bis e 3-quater c.p.p. oppure nei luoghi di privata dimora solo ove vi si stia svolgendo attività criminosa, comunque sempre indicando le ragioni che fondano la necessità di tali intercettazioni.

Si davano poi istruzioni affinché vi fosse il trasferimento delle registrazioni al solo server della Procura procedente e lo spegnimento del captatore senza che vi fosse possibilità di riattivarlo e si prescriveva l'utilizzo di programmi spia conformi a requisiti tecnici indicati dal Ministero e che si limitassero alle attività disposte senza porne in essere di ulteriori. Si raccomandava anche che le intercettazioni potessero essere disposte direttamente dal pubblico ministero nei casi di urgenza, ferma la necessaria convalida entro 48 ore da parte del giudice competente e che l'utilizzabilità si limitasse ai procedimenti per i reati di cui al decreto autorizzativo e ad altri procedimenti solo ove indispensabili per l'accertamento di reati per cui è disposto l'arresto obbligatorio in flagranza, vietando infine la divulgazione e pubblicazione di intercettazioni che coinvolgano occasionalmente terze parti estranee ai reati per i quali si procede.

In esercizio della suddetta delega, il Governo ha adottato il d. lgs. 216/2017, a norma del cui art. 4 è stato aggiunto un riferimento al captatore informatico nel testo dell'art. 266, c.2 c.p.p. (intercettazione di comunicazioni tra presenti). È stato inoltre inserito *ex novo* un comma 2-bis della disposizione, che dispone che "[l]'intercettazione di comunicazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile è sempre consentita nei procedimenti per i delitti di cui all'articolo 51, commi 3-bis e 3-quater".

All'articolo 267, c.1 è stata aggiunta la frase "Il decreto che autorizza l'intercettazione tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile indica le ragioni che rendono necessaria tale modalità per lo svolgimento delle indagini; nonchè, se si procede per delitti diversi da quelli di cui all'articolo 51, commi 3-bis e 3-quater, i luoghi e il tempo, anche indirettamente

determinati, in relazione ai quali è consentita l'attivazione del microfono". È stato introdotto anche il c.2-bis, che recita "Nei casi di cui al comma 2, il pubblico ministero può disporre, con decreto motivato, l'intercettazione tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile soltanto nei procedimenti per i delitti di cui all'articolo 51, commi 3-bis e 3-quater. A tal fine indica, oltre a quanto previsto dal comma 1, secondo periodo, le ragioni di urgenza che rendono impossibile attendere il provvedimento del giudice. Il decreto è trasmesso al giudice che decide sulla convalida nei termini, con le modalità e gli effetti indicati al comma 2".

All'art. 268, c.3-bis, è stata aggiunta la frase "Per le operazioni di avvio e di cessazione delle registrazioni con captatore informatico su dispositivo elettronico portatile, riguardanti comunicazioni e conversazioni tra presenti, l'ufficiale di polizia giudiziaria può avvalersi di persone idonee di cui all'articolo 348, comma 4". Un nuovo c.1-bis è stato inserito all'art. 270 e recita "I risultati delle intercettazioni tra presenti operate con captatore informatico su dispositivo elettronico portatile non possono essere utilizzati per la prova di reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione, salvo che risultino indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza".

Infine, all'art. 271 è stato introdotto il nuovo c.1-bis "Non sono in ogni caso utilizzabili i dati acquisiti nel corso delle operazioni preliminari all'inserimento del captatore informatico sul dispositivo elettronico portatile e i dati acquisiti al di fuori dei limiti di tempo e di luogo indicati nel decreto autorizzativo".

Il medesimo testo di legge ha altresì esteso ai procedimenti per i delitti contro la P.A. puniti con una pena non inferiore a cinque anni l'applicabilità dell'art.13, l. 203/1991 che consente l'intercettazione nei luoghi di privata dimora o domicilio quando sussistano meri indizi sufficienti di reato, ma esclude che si possa procedere, come avviene per i reati di criminalità organizzata, anche in assenza di alcun fondato motivo di ritenere che in tali ambienti si stia consumando un'attività criminosa (art. 6, d. lgs. 216/2017). Peraltro, quest'ultima limitazione all'uso del captatore informatico nei reati contro la P.A. è stata abrogata dopo solo un anno di vigenza (per effetto di una disposizione della cd. *Legge spazzacorrotti*[535]).

[535] Art. 1, c.3, l. 9 gennaio 2019, n. 3.

L'ultima disposizione del decreto sanciva l'applicabilità della maggioranza delle disposizioni ai provvedimenti di autorizzazione all'esperimento di intercettazioni pronunciati a partire dal centottantesimo giorno successivo all'entrata in vigore del decreto stesso. È stata proprio quest'ultima disposizione a cagionare un costante rinvio dell'applicazione di tali disposizioni, in prima istanza con l'art. 2, c.1, d.l. 91/2018, che ha posticipato il termine al 31 marzo 2019. La seconda occasione di rinvio si è manifestata con l'approvazione della cd. "Legge MilleProroghe" del dicembre 2018 (art. 1, c.1139, lett. a), n. 1, l. 145/2018), in conseguenza della quale il termine è stato rinviato al 31 luglio 2019. Un'ulteriore proroga al 31 dicembre 2019 del termine si è avuta con l'art. 9, c.2, lett. a) d.l. 53/2019. La formulazione e il termine sono stati oggetto di ulteriore modifica con l'art. 1, c.1, n. 1 d.l. 161/2019, che ha previsto l'applicazione di tali disposizioni ai procedimenti penali iscritti dopo il 29 febbraio 2020. In sede di conversione del decreto, peraltro, il termine è stato prorogato al 30 aprile 2020 (Allegato alla l. 7/2020). Ultimo in ordine di tempo, l'art. 1, c.1, lett. a) d.l. 28/2020 ha fissato l'ennesimo nuovo termine al 31 agosto 2020, che finalmente non è stato ulteriormente prorogato.

Sulla base di uno slittamento costante e continuo dell'applicazione di tali disposizioni, si potrebbe dubitare sulla reale volontà del legislatore di far applicare tali disposizioni in concreto, così limitando l'attività investigativa che fa ricorso allo strumento del captatore, il cui uso non è al momento limitato da altro che non sia quanto statuito dalla pronuncia nelle Sezioni Unite Scurato, non avendo le disposizioni del cd. Decreto Orlando potuto applicarsi finora ad alcun procedimento penale o quasi. Sulle conseguenze che tale costante posticipazione dell'applicazione delle disposizioni (e delle garanzie) dettate dalla legge possano cagionare, si rinvia alle considerazioni svolte nel capitolo conclusivo.

V. La tutela della riservatezza delle comunicazioni digitali: dai nuovi diritti all'equo bilanciamento fra valori divergenti

Sommario: 1. L'autonomia del diritto alla segretezza della corrispondenza oggi. – 2. Derogare sì, ma quando? – 3. Alla ricerca dell'equilibrio: il criterio di ragionevolezza come panacea?

1. L'autonomia del diritto alla segretezza della corrispondenza oggi

Il rapporto fra diritto e tecnologia si caratterizza per un'inevitabile asincronia, dovuta al fatto che il progresso della tecnica e le invenzioni umane precorrono l'intervento normativo, la cui necessità emerge solo dopo che un uso più o meno prolungato dei nuovi strumenti abbia dato luogo a problematiche non risolvibili in via di interpretazione sulla base degli strumenti giuridici già esistenti. Peraltro, se è pur vero che il progresso della tecnica offre uno straordinario novero di possibilità, in particolare sotto il profilo comunicativo, inimmaginabile soltanto qualche decennio fa, non si può ignorare come uno degli effetti del progresso tecnologico sia l'accrescimento dei poteri delle organizzazioni statali a scapito di quelli dei singoli individui o gruppi, potenziandone le capacità di monitoraggio e sorveglianza anche senza una presenza capillare sul territorio. Una delle tendenze identificate dalla riflessione a proposito dei mutamenti ingenerati dalla tecnica scientifica sulla società, d'altronde, è la progressiva concentrazione di un potere sempre maggiore in un numero sempre più ristretto di soggetti[536].

La lettura del dettato legislativo e costituzionale in senso più o meno ampio e aperto si dimostra così particolarmente significativa per poter tempestivamente fare fronte alle questioni che l'interprete trova dinanzi a sé. In questo contesto, si palesano le virtù di un dialogo fecondo fra i vari formanti presi in considerazione (v. *Introduzione*), in particolare in considerazione del fatto che l'autorità giudiziaria si trova prima o poi a dover rendere una decisione sui casi devoluti alla sua cognizione

[536] B. Russell, *L'impatto della scienza sulla società*, [ed. orig. *The Impact of Science on Society*, 1952], trad. it. di G. Meineri, Roma, Newton & Compton, 2005, 49 ss.

e, a differenza del legislatore, non può rimanere inerte e limitarsi a rispondere "*non liquet*".

L'operazione sussuntiva sottostante a ogni applicazione di regole astratte a fattispecie concrete è resa vieppiù complicata in ambito costituzionale dal fatto che i testi sono spesso ben più statici nella loro formulazione di quanto non siano le disposizioni legislative, almeno per quanto riguarda la disciplina dei diritti individuali. Questa situazione può rivelarsi favorevole ai singoli, poiché una parcellizzazione della tutela in tante situazioni giuridiche soggettive l'una distinta dall'altra offre, in ipotesi, una maggior possibilità di trovare il corretto inquadramento della prerogativa difesa e ottenerne una protezione sicura. D'altro canto, la frammentazione della garanzia dei diritti in una pluralità di posizioni giuridiche ne determina inevitabilmente una differenziazione sotto il profilo della tutela, che può essere associato sia a una scelta esplicita del testo costituzionale (la previsione – o meno – di una riserva di legge o di giurisdizione per esempio), sia a un'opzione adottata in un testo legislativo nell'esercizio della discrezionalità che contraddistingue l'operato del decisore politico, sia infine all'interpretazione che le corti ne danno in sede di applicazione concreta[537].

Nello schema del costituzionalismo europeo liberale e della prima metà del Novecento si è visto che la tutela della segretezza del contenuto di una comunicazione si è progressivamente emancipata dalla salvaguardia della libertà personale e dalla protezione della sfera domiciliare, andando ad assumere una posizione autonoma e ben distinta dalle altre due prerogative, tanto che la sua disciplina è in parte diversa da quella di libertà personale e domiciliare sia nella Costituzione italiana del 1948 che nella Legge Fondamentale tedesca del 1949. Tale differenza, curiosamente, si declina in direzioni opposte, poiché apparentemente nel caso italiano è una distinzione più garantista, nel senso che vige un divieto tassativo e assoluto di deroga, anche temporanea, al segreto delle comunicazioni senza l'autorizzazione del giudice (art. 15 Cost. It.), laddove nel caso della libertà personale e del domicilio sono ammesse restrizioni anche in mancanza di provvedimento giurisdizionale, anche se devono poi

[537] Sulla formulazione analitica della Carta costituzionale repubblicana in opposizione all'eccessiva genericità della tutela dei diritti nelle costituzioni di epoca liberale v. P. Caretti-G. Tarli Barbieri, *I diritti fondamentali. Libertà e diritti sociali*, Torino, Giappichelli, 2017, 86-87.

essere tempestivamente convalidate (artt. 13-14 Cost. It.). Nel caso tedesco, invece, la tutela del segreto epistolare ha subito una significativa *deminutio* in corrispondenza della revisione della Legge Fondamentale che ha introdotto la cd. *Costituzione d'emergenza* nel 1968[538], tanto che la protezione assai ampia e generale del testo originale è stata 'oscurata' dall'apertura alle limitazioni al diritto, pur temperata da una riserva di legge rinforzata per contenuto, e dalla previsione della possibilità di derogare al diritto alla tutela giurisdizionale altrimenti riconosciuto per tutte le altre posizioni giuridiche (art. 10 GG).

Diverso è il caso statunitense, ove il testo costituzionale è assai più risalente nonché molto complicato da modificare, ragion per cui il materiale con il quale i giudici si devono confrontare tendenzialmente non muta nel tempo, ma si arricchisce dell'elaborazione giurisprudenziale precedente, integrato dal *corpus* di principi elaborati nel patrimonio di *common law*. In particolare, la protezione del segreto delle comunicazioni dall'interferenza del potere pubblico si è potuta affermare in modo chiaro e inequivoco quando l'interpretazione delle garanzie del IV Emendamento ha virato da un'ottica meramente reale, orientata alla protezione di determinati beni[539], a una prospettiva personale, che tutela la sfera immateriale e morale della persona sia nella sua manifestazione concreta che in astratto[540].

Da questo punto di vista, il caso statunitense è un esempio di sostanziale coincidenza fra le due posizioni giuridiche, tale per cui la tutela della segretezza del contenuto delle comunicazioni si inserisce in un più ampio diritto alla riservatezza della vita privata (che si potrebbe intendere come quel *right to be let alone* invocato da Warren e Brandeis, seppur allora desunto non dalla disposizione costituzionale bensì dalla tradizione di *common law*, v. *supra* Cap. III, §3.3). Questa posizione giuridica soggettiva gode di una tutela variabile, i cui limiti non sempre si palesano chiaramente e possono oscillare sulla base della valutazione caso per caso delle corti, che vagliano la ragionevolezza dell'esistenza di un'aspettativa di riservatezza che sia soggettivamente genuina e oggettivamente legittima e tollerata.

---

[538] 17esima l. rev. Cost. 26 giugno 1968 (BGBL. I, S. 709).
[539] *Olmstead v. United States*, 277 U.S. 438 (1928).
[540] *Katz v. United States*, 389 U.S. 347 (1967).

Anche nei due Paesi dell'Europa continentale presi in considerazione in questa trattazione il quadro costituzionale postbellico originario è stato innovato in via di interpretazione da due giudici costituzionali invero particolarmente attivi e vivaci. L'apertura alla tutela di 'nuovi diritti', che possono venire alla luce come risultato del combinato disposto di altre disposizioni del testo costituzionale (è questo il caso del diritto alla riservatezza della vita privata in Italia[541]), è una delle vie tramite le quali si può offrire un'adeguata protezione a interessi che siano emersi in un momento successivo a quello della redazione di un catalogo di diritti. Tuttavia, il rischio della proliferazione di diritti a copertura costituzionale ma differenziati, per quanto in modo limitato, nella natura (si pensi al diritto all'autodeterminazione informatica[542] e al diritto all'integrità e confidenzialità dei sistemi informatici in Germania[543]) corre il rischio di rendere più incerto il quadro giuridico e non garantire una tutela efficace ai singoli.

Una possibile alternativa a tale approdo potrebbe consistere nel 'rispolverare' la categoria omnicomprensiva dei diritti della personalità[544], limitandosi a questa qualificazione generale delle posizioni giuridiche soggettive e lasciando all'apprezzamento dell'interprete nel caso concreto il vaglio sull'esistenza di un legittimo interesse al mantenimento della segretezza di una determinata informazione o di un determinato fatto. Peraltro, questa ipotetica convergenza verso una fonte comune delle prerogative attinenti alla sfera della personalità avrebbe il merito di consentire di adottare standard analoghi per informazioni e dati che, pur diversi per natura, potrebbero essere considerati meritevoli di analoga protezione (si pensi, pur nell'intrinseca differenza, ai dati archiviati su un dispositivo elettronico e al contenuto di una comunicazione telematica).

Si tenga a mente come la concentrazione del fascio dei diritti della personalità entro una matrice comune e unitaria potrebbe trarre ispirazione dall'approccio generale adottato dalla giurisprudenza della Corte EDU, in forza del contenuto

---

[541] Corte cost., sent. n. 38/1973, desunto dagli artt. 2, 3, c.2 e 13, c.1 Cost.
[542] BVerfG, Primo Senato, 15 dicembre 1983, 1 BvR 209/83.
[543] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07.
[544] Sulla riconducibilità della libertà e segretezza della corrispondenza a un unico disegno sistematico del Costituente italiano attinente ai diritti della persona v. P. Caretti-G. Tarli Barbieri, *I diritti fondamentali*, *op. cit.*, 375.

dell'art. 8 della Convenzione che tutela espressamente la vita privata e familiare accanto al domicilio e alla corrispondenza, facendoli soggiacere a una medesima regolazione e sottoponendoli agli stessi limiti.

Questa impostazione sembra poter essere maggiormente appropriata a proteggere in modo efficace la sfera della personalità individuale in quanto gli strumenti insidiosi di ricerca della prova dei quali si è dato conto nel Cap. IV hanno un potenziale ben più penetrante di quelli che i costituenti europei avrebbero potuto avere in mente a metà del secolo scorso (ciò vale a maggior ragione per i *Founding Fathers* statunitensi). Se si legge questo elemento insieme all'evidente dato sociale del sempre maggior affidamento che gli individui fanno su dispositivi elettronici di varia natura per l'intero spettro – o quasi – delle proprie attività quotidiane, si apprezza immediatamente il potenziale lesivo di questi strumenti, specie in ragione della capacità degli stessi di operare in modalità occulta e quindi all'insaputa del destinatario. L'accesso indiscriminato a questi strumenti informatici rende l'intera vita privata della persona suscettibile di essere svelata, non limitandosi a operare come una normale intercettazione che capta le sole comunicazioni orali (o scritte) *pro futuro*. Al contrario, le preoccupazioni manifestate dal *BundesVerfassungsGericht* sull'accesso indiscriminato alle informazioni e ai dati che su un dispositivo di questo genere siano archiviati mostrano i limiti della tutela del segreto delle comunicazioni, rendendo quantomeno legittimo interrogarsi sull'opportunità di concepire tale diritto in maniera unitaria, così da non parcellizzarne il godimento tramite la sottoposizione a regimi diversi.

Ciò non significa che il diritto a mantenere riservato il contenuto di una comunicazione privata non debba avere una sua piena autonomia con riferimento a quelle forme di comunicazione tradizionale che siano poste sotto sorveglianza con strumenti non in grado di avere pieno accesso ai dispositivi *target*, poiché in questi casi non viene minacciata la personalità dell'individuo in senso più ampio, ma la potenziale lesione rimane circoscritta all'ambito della cognizione del contenuto delle conversazioni a soggetti ai quali il destinatario non voleva che esso fosse noto.

2. *Derogare sì, ma quando?*

Accanto all'identificazione della più appropriata qualificazione dell'interesse di respiro costituzionale sotteso alle attività in questione, diviene di primaria importanza la riflessione sulle ipotesi entro le quali la deroga al principio generale possa essere disposta. Se alle garanzie idonee da predisporre in caso di eccezione alla regola si accennerà *infra*, è di indubbio interesse lo sforzo di tracciare un perimetro delle situazioni di fatto che giustifichino interventi limitativi del godimento del diritto a mantenere riservato il contenuto delle proprie comunicazioni.

In tutti i casi trattati l'interferenza statale con il segreto delle comunicazioni è ammessa con riferimento a un catalogo chiuso, per quanto esteso, di fattispecie di reato, richiedendo quindi il raggiungimento di una soglia di gravità tale da esigere un sacrificio tanto significativo sotto il profilo costituzionale. L'identificazione dei fini perseguiti, che coincide in buona sostanza con la protezione di altri interessi a rilevanza costituzionale, si pone quindi come presupposto alla definizione delle modalità con le quali la limitazione viene posta in essere in concreto.

Uno sforzo in questa direzione emerge per esempio dalla giurisprudenza costituzionale tedesca: il Tribunale di Karlsruhe ha ritenuto che la restrizione dei diritti protetti dalla Legge Fondamentale sia ammessa solo in presenza di elementi di fatto che testimonino un pericolo concreto a beni giuridici che abbiano una rilevanza fondamentale nell'architettura costituzionale, indicando specificamente la vita, l'integrità fisica e la libertà personale. Accanto a questi, tuttavia, vi sono altresì altri interessi la cui protezione può essere legittimamente perseguita per mezzo di una compressione del diritto al segreto della corrispondenza, che sono quelli che presiedono al buon funzionamento delle strutture pubbliche che assicurano un sostegno alla vita dei cittadini[545].

La giurisprudenza del *BundesVerfassungsGericht* è senz'altro influenzata dalla ricca elaborazione giurisprudenziale della Corte EDU in materia, che poggia sull'interpretazione del requisito della necessità di una misura, nel contesto di una società democratica, alla sicurezza nazionale, alla sicurezza pubblica, al benessere

[545] BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07, § 247.

economico collettivo, al mantenimento dell'ordine pubblico, alla prevenzione dei reati, alla tutela della salute, della morale o di diritti e libertà di altri soggetti. Il requisito della necessità poggia sul doppio accertamento dell'esistenza di un'esigenza sociale di perseguimento di un determinato interesse (fra quelli menzionati dalla disposizione) e della strumentalità e proporzionalità della limitazione del diritto adottata ad assicurare il godimento del suddetto interesse[546]. Il dominio di fini astrattamente perseguibili delineato dal testo della Convenzione è al contempo ampio e stringente. Ampio perché si fa menzione di un novero consistente di circostanze e finalità, che non si limitano alla mera tutela della vita e dell'integrità fisica dei cittadini ma si spingono anche al perseguimento del benessere economico e della tutela della morale. Si tratta quindi di uno spazio assai esteso e variegato entro il quale le autorità pubbliche possono muoversi per addurre le opportune giustificazioni alla limitazione del diritto in questione. Stringente perché lo scrutinio che viene effettuato è rigoroso e non si accontenta dell'allegazione di rischi presunti sulla base di massime d'esperienza ma esige una dimostrazione concreta della sussistenza della minaccia caso per caso.

Se il margine di apprezzamento riconosciuto agli Stati firmatari della Convenzione EDU rimane di una certa ampiezza, residua in capo alla Corte di Strasburgo la supervisione sulla legislazione nazionale nonché sulla sua applicazione in concreto da parte delle autorità investigative e di pubblica sicurezza[547]. Questo perché l'obiettivo dello scrutinio della Corte EDU è anche quello di evitare che, celandosi dietro il paravento della protezione della sicurezza nazionale, si finisca con l'indebolire o addirittura demolire il concetto stesso di sistema democratico.

L'unico modo per assicurare che ciò non avvenga è prescrivere che, ogni qual volta siano poste in essere misure orientate a proteggere l'ordine pubblico e la sicurezza dei cittadini tramite la compressione del diritto alla riservatezza del contenuto delle comunicazioni, siano predisposte tutta una serie di garanzie sotto il profilo procedurale, che assicurino quello che oltreoceano chiamerebbero un *due process of law*. Risiede dunque proprio nella previsione da parte del legislatore di una rigorosa procedimentalizzazione delle operazioni di sorveglianza, che consenta alle potenziali

---

[546] *Dudgeon c. Regno Unito*, no. 7525/76, Corte EDU, Grande Camera, 22 ottobre 1981, §§ 51-53; analogamente *Z c. Finlandia*, no. 22009/93, Corte EDU, Sez. semplice, 25 febbraio 1997, § 94.
[547] *Piechowicz c. Polonia*, no. 20071/07, Corte EDU, IV Sez., 17 aprile 2012, § 212.

parti lese di sottoporre a uno scrutinio di legittimità le attività di indagine occulte altrimenti del tutto sottratte a un controllo preventivo, la chiave di volta di questo complicato bilanciamento. Tanto nell'intero sistema CEDU quanto nella giurisprudenza tedesca di cui si è detto, perciò, l'accertamento dell'esistenza di un quadro normativo conforme a tale requisito si estrinseca in una verifica della ragionevolezza dell'ampiezza delle limitazioni imposte dal legislatore in rapporto ai fini perseguiti.

Come è stato analizzato nel corso della trattazione, negli Stati Uniti d'America la questione non si pone negli stessi termini, nel senso che si ritiene largamente che la discrezionalità legislativa esercitata nella determinazione dei casi nei quali sia consentito il ricorso a forme di interferenza del tipo delle intercettazioni delle telecomunicazioni o del tracciamento dei dati non ricada oltre i limiti previsti dalla disciplina costituzionale, concentrandosi invece il contenzioso piuttosto sulla delimitazione delle fattispecie che siano tutelate dalla riserva di giurisdizione (*rectius*, dell'obbligo di ottenere un mandato) di cui al IV Emendamento[548]. D'altronde, la stessa giurisprudenza della Corte Suprema federale ha delineato una serie di eccezioni alla regola generale, che consentono di procedere alle perquisizioni e ai sequestri di cui al IV Emendamento anche senza mandato. Si tratta di ipotesi improntate pragmaticamente allo scopo di assicurare elementi di prova nei casi di intervento dell'autorità in flagranza di reato, nonché a proteggere la persona dell'agente che effettui il fermo o l'arresto[549].

Qui, il vero tema è la determinazione dell'esistenza di quella ragionevole aspettativa di riservatezza con riferimento alle indagini che interferiscano con l'utilizzo di dispositivi digitali e l'estensione della protezione degli stessi, vale a dire la soglia oltre la quale l'autorità inquirente necessiti di un mandato ben preciso per poter prendere cognizione dei dati contenuti su uno di essi.

---

[548] O.S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, *op. cit.*, 851.

[549] Per un panorama su tali ipotesi di deroga dalla generale esistenza di una *probable cause* o dall'obbligo di *warrant* a norma del IV Emendamento, v. R.W. Galloway Jr., *Basic Fourth Amendment Analysis*, in 32 *Santa Clara L. Rev.*, 1992, 737-782.

Nel caso italiano, infine, la decisione è stata nel senso di un sacrificio senz'altro rilevante della tutela del segreto delle comunicazioni e dell'inviolabilità del domicilio dei soggetti destinatari delle attività di intercettazione e captazione occulta mediante *trojan*[550], che trova giustificazione nel perseguimento dei fini di persecuzione dei reati e di prevenzione delle condotte criminose. Tuttavia, ciò che contraddistingue il nostro ordinamento è l'opzione per un doppio livello di tutela avverso tali intrusioni (anche detto 'doppio binario'[551]). Infatti, la maggior forza lesiva potenziale dei delitti attinenti all'ambito della criminalità organizzata viene ritenuta meritevole di un trattamento meno favorevole, tale da consentire un sacrificio delle prerogative in parola non del tutto bilanciato dalle garanzie procedurali che si applicano invece alle altre fattispecie di reato.

3. *Alla ricerca dell'equilibrio: il criterio di ragionevolezza come panacea?*

Il perseguimento di fini legittimi secondo la Costituzione, sia esso presuntivamente soddisfatto dal quadro legislativo o soddisfatto in quel novero di casi identificati nella prassi giurisprudenziale (come negli Stati Uniti d'America) oppure verificato caso per caso a seconda della misura posta in essere (come nel sistema del Consiglio d'Europa), non basta a dare il semaforo verde all'esperimento dell'attività di interferenza. Infatti, seppure in modo diverso, la cartina di tornasole della legittimità di una misura, che serve a identificarne la legittimità nel contesto europeo e a svincolare dall'obbligo di richiedere un mandato in quello statunitense, risiede in uno scrutinio orientato a indagare la ragionevolezza della limitazione (in Europa) o dell'aspettativa (negli Stati Uniti d'America).

Benché vi sia un'apparente identità terminologica fra i due casi, è bene distinguerli perché la natura del vaglio che si prefiggono è senz'altro diversa. Infatti, il riferimento alla ragionevolezza negli Stati Uniti d'America serve lo scopo di indagare se il soggetto può legittimamente attendersi che i dati delle proprie

---

[550] Evidenzia profili critici sotto il profilo costituzionale C. Pinelli, *Sull'ammissibilità di restrizioni alla libertà di domicilio e alla libertà di comunicazione tramite "virus di stato"*, in *Diritto Penale Contemporaneo*, 4/2017, 75-82.
[551] M. Griffo, *Il captatore informatico e la filosofia del doppio binario*, *op. cit.*

comunicazioni (siano essi quelli esteriori o il contenuto vero e proprio) possano essere conosciuti anche senza un mandato e quindi in deroga a tutte le garanzie procedurali a esso associate. In particolare, specie con riferimento ai dati esteriori delle comunicazioni o a quelli emessi da dispositivi utilizzati su base quotidiana e continua, la questione più spinosa riguarda i limiti alla *reasonable expectation of privacy*, cioè se essi siano sussumibili in un caso di *third party exception* o meno, come da ultimo ha sancito la Corte Suprema con la sofferta sentenza *Carpenter*[552].

Nel contesto europeo, diversamente, la ragionevolezza è stata intesa, specie dalla Corte EDU e dal *BundesVerfassungsGericht*, come uno scrutinio molto penetrante e severo sulla proporzionalità e adeguatezza delle limitazioni apposte ai diritti costituzionalmente sanciti. Questo ha implicato una verifica dell'idoneità dei mezzi adottati per il perseguimento dei fini di tutela dei diritti e un controllo puntiglioso sulla configurazione di tali strumenti, così da garantire che l'interferenza sia limitata al quel tanto che basta per raccogliere gli elementi sufficienti alle indagini, senza che questo vada a sopprimere del tutto il godimento del diritto in questione. Quest'ultimo profilo è particolarmente rilevante nel contesto tedesco, ove la sottolineatura esplicita del testo costituzionale che impone di non sacrificare mai il nocciolo duro (*wesensgehalt*) dei diritti fondamentali (art. 19 GG) impone una compensazione alle restrizioni alle posizioni giuridiche soggettive consistente in quelle garanzie procedurali particolarmente stringenti che il Tribunale Costituzionale Federale ha sancito nei due casi del 2008 e 2016.

Se l'intervento del giudice è considerato requisito irrinunciabile in tutti gli ordinamenti, salvo il caso, negli Stati Uniti d'America, delle circostanze in cui non sia configurabile una *reasonable expectation of privacy*, il grado di dettaglio della richiesta presentata dalle autorità procedenti al giudice e l'analiticità del provvedimento con il quale viene autorizzato l'esperimento delle operazioni diviene dirimente. In particolare, la natura intrinsecamente occulta delle attività d'indagine in questione deve essere controbilanciata dalla possibilità di sottoporre a scrutinio sulla legittimità le misure dispiegate, prevedendo una tempestiva comunicazione dell'avvenuta

[552] *Carpenter v. US*, 138 S. Ct. 2206 (2018).

restrizione a carico del destinatario non appena ciò sia possibile senza pregiudizio per l'esito delle indagini.

In tutto ciò, l'attività di captazione occulta deve essere orientata a raggiungere solo e soltanto quelle conversazioni che siano strumentali alla ricostruzione delle fattispecie di reato perseguite, facendo in modo che sia limitata al minimo possibile l'interferenza e la registrazione di dati e comunicazioni a natura personale e riservata e curandosi di eliminarle non appena ne emerga la natura estranea alle indagini.

Ciò che sembra lecito concludere, in ultima istanza, è che il giudizio sul bilanciamento operato dal legislatore, quale che esso sia fra quelli di cui si è detto, fra gli interessi in gioco può difficilmente definirsi scolpito nella pietra, poiché il giudizio sull'effettiva necessità e adeguatezza delle misure predisposte ai fini della ricerca della prova ricade sovente sull'interprete principe del diritto, vale a dire il giudice, in specie quello penale. Se si tratti di una constatazione positiva, poiché nel suo apprezzamento delle circostanze del caso concreto esso è in grado di valutare se il bilanciamento del decisore politico sia stato accorto, oppure di un elemento che mette in crisi il sistema, minacciando quel requisito della prevedibilità che non può difettare a una disciplina tanto delicata, rimane questione aperta.

Se però il legislatore nazionale continuerà ad esercitare la propria discrezionalità in maniera timida o troppo generica, peccando di inerzia come quello italiano fino a prima della riforma Orlando o di vaghezza (basti pensare alla disputa sul perimetro della categoria dei reati associativi), allora la supplenza della giurisprudenza non potrà che essere il rimedio prescelto. Peraltro, se ciò può in linea generale configurare un certo *favor* nei confronti dei destinatari ipotetici delle misure limitative della libertà personale, non può non far un po' storcere il naso sotto il profilo dell'equilibrio istituzionale. D'altronde, il giudice è sì deputato a riconoscere i diritti dei cittadini anche a fronte di eventuali abusi dell'autorità pubblica, ma quando deve intervenire per colmare lacune significative in merito all'ambito di applicazione di date discipline, come avvenuto nel caso dell'uso dei *trojans* in Italia nella storica sentenza Scurato[553], esso esorbita dalle proprie funzioni e si veste dei panni del legislatore. Questa è, tuttavia, una mera conseguenza della patologia, che risiede

[553] Cass. pen., SS. UU., sent. n. 26889/16, 28 aprile 2016.

altrove: se il legislatore abdica al proprio ruolo e rinuncia a dettare con sufficiente dovizia di particolari la disciplina in un ambito delicato come quello della limitazione dei diritti dei consociati, lo spazio non può rimanere vuoto e, giocoforza, dovrà essere occupato da un altro soggetto istituzionale, che pur investito della funzione dell'esercizio della giurisdizione si ritroverà nei panni altrui a farsi legislatore.

Bibliografia

Letteratura

- W. Abel-B. Schafer (trad. it. a cura di A. Piccinin), *La decisione della Corte Costituzionale tedesca sul diritto alla riservatezza ed integrità dei sistemi tecnologici d'informazione – un rapporto sul caso BVerfGE, NJW 2008, 822*, in *JEI – Jus e Internet*, 15 novembre 2009, §2, disponibile all'url: https://www.jei.it/approfondimenti-giuridici/23-la-decisione-della-corte-costituzionale-tedesca-sul-diritto-alla-riservatezza-ed-integrita-dei-sistemi-tecnologici-d-informazione-un-rapporto-sul-caso-bverfge-njw-2008-822
- W. Abel-B. Schafer, *The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems - A Case Report on BVerfG, NJW 2008, 822*, in 6 *SCRIPTed*, 1, 2009, 106-123
- R. Alexy, *Teoria dei diritti fondamentali*, Bologna, Il Mulino, 2012
- A. Amorth, *La costituzione italiana. Commento sistematico*, Milano, Giuffrè, 1948
- K.E. Aucoin, *The Spider's Parlor: Government Malware on the Dark Web*, in 69 *Hastings L.J.*, 2018, 1433-1469
- T.A. Auletta, *Riservatezza e tutela della personalità*, Milano, Giuffrè, 1978
- A. Baldassarre, *Privacy e costituzione. L'esperienza statunitense*, Roma, Bulzoni, 1974
- A. Bargi-S. Fùrfaro, *La prova per intercettazioni tra diritto interno e diritto sovranazionale*, in A. Gaito (a cura di), *Riservatezza ed intercettazioni tra norma e prassi*, Roma, Aracne, 2011, 55-116
- P. Barile, *Diritti dell'uomo e libertà fondamentali*, Bologna, Il Mulino, 1984
- P. Barile-E. Cheli, *Corrispondenza (Libertà di)*, in *Enc. del dir.*, X, Milano, 1962, 746-753
- G. Barroccu, *Il captatore informatico: un virus per tutte le stagioni*, in *Diritto penale e processo*, 3/2017, 379-390
- A. Belloc, *Les postes françaises: recherches historiques sur leur origine, leur développement, leur législation*, Paris, Firmin-Didot, 1886
- A. Belvedere, *Riservatezza e strumenti di informazione*, in N. Irti (a cura di), *Dizionari di diritto privato*, Giuffrè, Milano, 1980, I, 727-762

- P. Biscaretti di Ruffia, *Diritto costituzionale*, Napoli, Jovene, 1965
- A. Bonomo, *I nuovi strumenti di comunicazione telematica ed informatica: aspetti tecnici e questioni giuridiche*, in *Le investigazioni con l'impiego di intercettazioni di comunicazioni e di flussi informatici o telematici*, Gruppo di studio del 6 luglio 2011 ore 15,00, Incontro di studi sul tema: *Tecniche di indagine e rapporti tra p.m., polizia giudiziaria, consulenti tecnici e difensori*, Roma, 4-8 luglio 2011, Consiglio Superiore della Magistratura
- A. Brunialti, *Prefazione. La libertà nello stato moderno*, in A. Brunialti (a cura di), *Biblioteca di scienze politiche*, Vol. V, Torino, Unione tipografico-editrice, 1890
- G. Caneschi, *Le nuove indagini tecnologiche e la tutela dei diritti fondamentali. L'esperienza del captatore informatico*, in *DPC*, 2/2019, 417-429
- R. Cantagalli, *Riservatezza della vita privata e intercettazioni delle comunicazioni*, Firenze, Edizioni Laurus, 1977
- P. Caretti, *Corrispondenza (Libertà di)*, in *Dig. disc. pubbl.*, vol. IV, Torino, 1989, 200-205
- P. Caretti-G. Tarli Barbieri, *I diritti fondamentali. Libertà e diritti sociali*, Torino, Giappichelli, 2017
- F. Carnelutti, *Diritto alla vita privata (contributo alla teoria della libertà di stampa)*, in *Riv. trim. dir. pubbl.*, 1955, 3-18
- C. Caruso, *La libertà e la segretezza delle comunicazioni nell'ordinamento costituzionale*, in *Forum di Quaderni costituzionali*, 21 ottobre 2013
- G. Cerrina Feroni-T.E. Frosini-A. Torre (a cura di), *Codice delle Costituzioni*, Torino, Giappichelli, 2009
- G. Cerrina Feroni, *Forme di Stato*, in P. Carrozza-A. Di Giovine-G.F. Ferrari (a cura di), *Diritto costituzionale comparato*, Roma-Bari, Laterza, 2009, 674-704
- C.D. Classen-A. Gaillet, *Allemagne : la lutte antiterroriste sans régime d'exception*, in *Annuaire international de justice constitutionnelle*, 32-2016, 2017, *Migrations internationales et justice constitutionnelle - Référendums et justice constitutionnelle*, 15-27

- D. Coduti, *Libertà e segretezza della corrispondenza dei detenuti nella sentenza n. 20 del 2017 della Corte costituzionale*, in *federalismi.it*, Focus Human Rights N.2, 28 luglio 2017
- M. Comba, *Gli Stati Uniti d'America*, in P. Carrozza-A. Di Giovine-G.F. Ferrari (a cura di), *Diritto costituzionale comparato*, Roma-Bari, Laterza, 2009, 127-157
- T.M. Cooley, *The Elements of Torts*, Chicago, Callahan, 1878
- S. Cooper, *The Ultimate Guide to Port Mirroring*, disponibile all'url: https://www.comparitech.com/net-admin/ultimate-guide-to-port-mirroring/
- W.J. Cuddihy, *The Fourth Amendment. Origins and Original Meaning 602-1791*, Oxford, Oxford University Press, 2009
- B. Cupa, *Trojan horse resurrected - On the legality of the use of government spyware*, in C. Webster-R. William, *Living in surveillance societies: The state of surveillance,* Proceedings of LiSS conference 3. 978-1484049082: CreateSpace Independent Publishing Platform, 2013, 419-428, disponibile all'url: https://www.zora.uzh.ch/id/eprint/81157/1/Cupa_Living_in_Surveillance_Societies_2012.pdf
- A. De Cupis, *I diritti della personalità*, Milano, Giuffrè, 1950
- A. De Cupis, *Il diritto alla riservatezza esiste*, in *Foro it.*, 1954, 4, 89-97
- A. De Cupis, *Il diritto all'onore e il diritto alla riservatezza*, Milano, Giuffrè, 1948
- R. Dieter, *You've Got Mail: FBI Hacking in* United States v Lough *and Why It Is a Fourth Amendment Search*, in 63 *Vill. L. Rev. Online*, 2018, 101-125
- J. Eberle, *Human Dignity, Privacy, and Personality in German and American Constitutional Law*, in *Utah L. Rev.*, 1997, 963-1056
- L. Elia, *Il Parlamento italiano 1861-1988*, Vol. XIV, 1946-1947, Milano, Nuova CEI, 1988, 125-139
- M. Ferrara Santamaria, *Il diritto alla illesa intimità privata*, in *Riv. dir. priv.*, 1937, I, 168-191
- G.F. Ferrari, *«Civil law» e «common law»: aspetti pubblicistici*, in P. Carrozza-A. Di Giovine-G.F. Ferrari (a cura di), *Diritto costituzionale comparato*, Roma-Bari, Laterza, 2009, 645-673
- G.F. Ferrari, *Le libertà. Profili comparatistici*, Torino, Giappichelli, 2011

- C. Fiorio, *Intercettazioni telefoniche e diritti costituzionalmente garantiti fra frammenti di storia parlamentare e prospettive* de iure condendo, in A. Gaito (a cura di), *Riservatezza e intercettazioni tra norma e prassi*, Roma, Aracne, 2011, 283-297
- R. Flor, *Brevi riflessioni a margine della sentenza del BundesVerfassungsGericht sulla cd. Online Durchsuchung*, in *Riv. Trim. Dir. Pen. Econ.*, 3, 2009, 695-716
- R. Flor, *La sentenza del* BundesVerfassungsGericht *del 27 febbraio 2008 sulla cd.* online durchsuchung, in *Riv. trim. dir. pen. econ.*, 3, 2009, 679-694
- C. Gabrielli, *Dall'esecuzione di operazioni di ascolto all'acquisizione delle captazioni rilevanti*, in G. Giostra-R. Orlandi (a cura di), *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, Torino, Giappichelli, 2018, 3-30
- R.W. Galloway Jr., *Basic Fourth Amendment Analysis*, in 32 *Santa Clara L. Rev.*, 1992, 737-782
- E. George, *UK Computer Misuse Act – The Trojan Virus Defence. Regina v Aaron Caffrey, Southwark Crown Court, 17 October 2003*, in 1 *Digital Investigation*, 2, 2004, 89
- G. Giampiccolo, *La tutela giuridica della persona umana e il c.d. diritto alla riservatezza*, in *Riv. trim. dir. e proc. civ.*, 1958, 458-475
- P. Giocoli Nacci, *Libertà di corrispondenza*, in G. Santaniello (a cura di), *Trattato di diritto amministrativo*, vol. XII, *Libertà costituzionali e limiti amministrativi*, Padova, 1990, 107-132
- G. Giostra, *Il segreto estende i suoi confini e la sua durata*, in G. Giostra-R. Orlandi (a cura di), *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, Torino, Giappichelli, 2018, 115-135
- G. Giostra, *Prima lezione sulla giustizia penale*, Bari-Roma, Laterza, 2020
- F. Giunchedi, *La motivazione dei decreti autorizzativi nell'interpretazione delle Sezioni Unite*, in A. Gaito (a cura di), *Riservatezza ed intercettazioni tra norma e prassi*, Roma, Aracne, 2011, 141-147
- P.G. Gosso, *Intercettazioni telefoniche*, in *Enc. dir.*, XXI, 1971, 889-900
- V. Grevi, *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche*, in *Giur. Cost.*, 1973, 317-342

- S. Grieco, *L'introduzione del virus di Stato nelle intercettazioni ambientali: il trojan e le sue ricadute costituzionali*, in *Dirittifondamentali.it*, 1/2019
- M. Griffo, *Il captatore informatico e la filosofia del doppio binario*, Napoli, ESI, 2019
- D. Grimm, *La Costituzione di Weimar vista nella prospettiva del Grundgesetz*, in *Nomos. Le attualità nel diritto*, 2/2012
- E. Hobsbawm, *Age of Extremes. The Short Twentieth Century 1914-1991*, Londra, Michael Joseph, 1994 (trad. it. a cura di B. Lotti, Milano, BUR, 1994)
- E.A. Imparato, *Diritti fondamentali e principio di proporzionalità: dalla "tirannia dei valori" alla tirannia dei giudici nell'esempio tedesco*, in E.A. Imparato (a cura di), *Diritti o giudizi? Le libertà tra regole e casistica interna ed europea in una riflessione comparata*, Napoli, uniorPress, 2014, 31-51
- F. Iovene, *Le c.d. perquisizioni online tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *DPC*, 3-4/2014, 329-342
- V. Italia, *Libertà e segretezza delle comunicazioni e della corrispondenza*, Milano, Giuffrè, 1963
- O.S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, in 102 *Mich. L. Rev.*, 2004, 801-888
- D.P. Kommers, *The Basic Law: A Fifty Year Assessment*, in *German Law Journal*, 20, 2019, 571–582
- N.E. La Rocca, *L'utilizzo di impianti esterni alla Procura e l'ascolto "remotizzato"*, in A. Gaito (a cura di), *Riservatezza ed intercettazioni tra norma e prassi*, Roma, Aracne, 2011, 149-163
- F. Lanchester, *Le costituzioni tedesche da Francoforte a Bonn. Introduzione e testi*, Milano, Giuffrè, 2002
- B. Lawson, *What Not to Ware: As Congress Struggles against Spyware, the FBI Develops Its Own*, in 35 *Rutgers Computer & Tech. L.J.*, 2008, 77-103
- S. Lonati, *I criteri direttivi contenuti nella delega in materia di intercettazioni di conversazioni e comunicazioni*, in O. Mazza (a cura di), *Le nuove intercettazioni*, Torino, Giappichelli, 2018, 1-26
- G. Maranini, *Le origini dello Statuto albertino*, Firenze, Vallecchi, 1926

- S. Marcolini, *Le cosiddette perquisizioni on line (o perquisizioni elettroniche)*, in *Cass. Pen.*, 7-8, 2010, 2855-2868
- D. McCullagh, *Feds use keylogger to thwart PGP, Hushmail*, disponibile all'url: https://www.cnet.com/news/feds-use-keylogger-to-thwart-pgp-hushmail/
- R.A. Miller, *A Pantomime of Privacy: Terrorism and Investigating Powers in German Constitutional Law*, in 58 *B.C. L. Rev.*, 2017, 1545-1628
- L. Montanari, *Le tecniche di adattamento alla Cedu come strumento di garanzia dei diritti: un'analisi comparata delle soluzioni adottate negli ordinamenti nazionali*, in Atti del Colloquio biennale dell'Associazione italiana di diritto comparato tenutosi a Messina-Taormina, 31 maggio-2 giugno 2001, *I diritti fondamentali in Europa*, Milano, Giuffrè, 2002, 522-557
- C. Mortati, *La Costituzione di Weimar*, Milano, Giuffrè, 2019 (ed. orig. C. Mortati, *Introduzione a La Costituzione di Weimar*, Firenze, Sansoni, 1946)
- F. Nicolicchia, *I limiti fissati dalla Corte costituzionale tedesca agli strumenti di controllo tecnologico occulto: spunti per una trasposizione nell'ordinamento italiano*, in *Archivio penale*, 2, 2017, disponibile all'url: http://www.archiviopenale.it/File/DownloadArticolo?codice=a6b3ff73-ab8a-40ba-9fb1-422ebfd12304&idarticolo=15150
- F. Nicolicchia, *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, in *Diritto Penale Contemporaneo*, 2, 2018, 177-189
- A.M. Ogilvie, *The Rise of the English Post Office*, in *The Economic Journal*, Vol. 3, No. 11 (Sett. 1893), 443-457
- A. Pace, *Problematica delle libertà costituzionali*, *Parte speciale*, Padova, CEDAM, 1992
- A. Pace, *Art. 15*, in G. Branca-A. Pizzorusso (a cura di), *Commentario della Costituzione*, Bologna, Zanichelli, 1977, 80-113
- F. Palmiotto, *Le indagini informatiche e la tutela della riservatezza informatica*, in *La legislazione penale*, 1 luglio 2019, 3, disponibile all'url: http://www.lalegislazionepenale.eu/wp-content/uploads/2019/06/Palmiotto-rubrica-speciale-Finale.pdf

- L. Parlato, *Il legislatore tedesco approfitta di una più ampia riforma per disciplinare le perquisizioni* online, in *Cass. pen.*, 2, 2019, 854-872
- L. Parlato, *Problemi insoluti: le perquisizioni* on-line, in G. Giostra-R. Orlandi (a cura di), *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, Torino, Giappichelli, 2018, 289-323
- G. Parodi, *La Germania e l'Austria*, in P. Carrozza-A. Di Giovine-G.F. Ferrari (a cura di), *Diritto costituzionale comparato*, Roma-Bari, Laterza, 2009, 196-241
- C. Peloso, *La tutela della riservatezza nell'era delle nuove tecnologie: la vicenda dei captatori informatici per le intercettazioni tra presenti nei reati di terrorismo*, in *DPC*, 1/2017, 149-161
- C. Pinelli, *Sull'ammissibilità di restrizioni alla libertà di domicilio e alla libertà di comunicazione tramite "virus di stato"*, in *Diritto Penale Contemporaneo*, 4/2017, 75-82
- L. Pistorelli, *Accesso difensivo alle registrazioni delle intercettazioni, tra limiti normativi ed evoluzione tecnologica*, 15 gennaio 2012, nota a Cass. pen., sez. VI, 9 novembre 2011 (dep. 24 novembre 2011), n. 43654, Pres. De Roberto, Rel. Petruzzellis, ric. Aga e a Tribunale di Trani, ord. 16 giugno 2011, Pres. Carone, Est. Gadaleta, disponibile all'url: https://archiviodpc.dirittopenaleuomo.org/d/1172-accesso-difensivo-alle-registrazioni-delle-intercettazioni-tra-limiti-normativi-ed-evoluzione-tecno
- F. Racioppi-A. Brunialti, *Commento allo Statuto del Regno*, II, Torino, UTET, 1909
- A. Ravà, *Istituzioni di diritto privato*, Padova, CEDAM, 1938
- A. Ravà, *I diritti sulla propria persona nella scienza e nella filosofia del diritto*, Torino, Fratelli Bocca, 1901
- P. Ridola, *Preistoria, origini e vicende del costituzionalismo*, in P. Carrozza-A. Di Giovine-G.F. Ferrari (a cura di), *Diritto costituzionale comparato*, Roma-Bari, Laterza, 2009, 21-58
- P. Rivello, *Il procedimento acquisitivo delle intercettazioni e l'archivio riservato presso il pubblico ministero*, in O. Mazza (a cura di), *Le nuove intercettazioni*, Torino, Giappichelli, 2018, 55-100
- S. Rodotà, *La "privacy" tra individuo e collettività*, in *Politica del diritto*, 5, ottobre 1974, 545-563

- S. Romano-C. Sorio, *L'utilizzo dei cd.* trojan horses *nelle indagini penali e la tutela "progressiva" della libertà e segretezza delle comunicazioni*, Law and Media Working Paper Series, no. 14/2016
- G. Romeo, *La Corte Suprema e l'approccio minimalista alle nuove tecnologie*, in *Diritti Comparati*, 8 marzo 2012, disponibile all'url: https://www.diritticomparati.it/la-corte-suprema-e-lapproccio-minimalista-alle-nuove-tecnologie/
- G. Romeo, *Time is (finally) ripe: la Corte Suprema degli Stati Uniti ridefinisce il bilanciamento tra il diritto alla privacy e le nuove tecnologie*, 3 luglio 2014, disponibile all'url: https://www.diritticomparati.it/time-is-finally-ripe-la-corte-suprema-degli-stati-uniti-ridefinisce-il-bilanciamento-tra-il-diritto/
- C. Rossi, *Il rispetto della corrispondenza nella Convenzione europea dei diritti dell'uomo. Le intercettazioni nella legislazione italiana*, in *Riv. int. dir. uomo*, 1994, 64-71
- B.R. Ruiz, *Privacy in telecommunications. A European and an American approach*, L'Aja, Kluwer Law International, 1997
- B. Russell, *L'impatto della scienza sulla società*, [ed. orig. *The Impact of Science on Society*, 1952], trad. it. di G. Meineri, Roma, Newton & Compton, 2005
- R. Sacco, *Introduzione al diritto comparato*, Torino, UTET, 1992
- R. Sacco, *Legal Formants: A Dynamic Approach to Comparative Law (Installment I of II)*, in *The American Journal of Comparative Law*, Vol. 39, No. 1. (Winter, 1991), 1-34
- S.J. Schulhofer, *More essential than Ever: The Fourth Amendment in the Twenty First Century*, Oxford, Oxford University Press, 2012
- S. Signorato, *La localizzazione satellitare nel sistema degli atti investigativi*, in *Rivista italiana di diritto e procedura penale*, 2, 2012, 580-607
- S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, Giappichelli, 2018
- P. Tonini, *Manuale di procedura penale*, XX ed., Milano, Giuffrè, 2020
- M. Torre, *Il* virus *di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali*, in *Diritto penale e processo*, 9, 2015, 1163-1172
- C. Troisio, *Corrispondenza (libertà e segretezza della)*, in *Enciclopedia giuridica Treccani*, IX, 1988

- T.M. Ubertazzi, *Il diritto alla privacy. Natura e funzioni giuridiche*, Padova, CEDAM, 2004
- G. Vaciago, *Remote Forensics and Cloud Computing: An Italian and European Legal Overview*, in 8 *Digital Evidence & Elec. Signature L. Rev.*, 2011, 124-129
- E. Vaille, *Le cabinet noir*, Paris, Presses universitaires de France, 1950
- A. Valastro, *Libertà di comunicazione e nuove tecnologie. Inquadramento costituzionale e prospettive di tutela delle nuove forme di comunicazione interpersonale*, Milano, Giuffrè, 2001
- G. Varraso, *Le intercettazioni e i regimi processuali differenziati per i reati di "grande criminalità" e per i delitti dei pubblici ufficiali contro la pubblica amministrazione,* in O. Mazza (a cura di), *Le nuove intercettazioni*, Torino, Giappichelli, 2018, 139-161
- A. Venegoni-L. Giordano, *La Corte costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici*, in *Diritto Penale Contemporaneo*, 8 maggio 2016, ora disponibile all'url: https://archiviodpc.dirittopenaleuomo.org/d/4703-la-corte-costituzionale-tedesca-sulle-misure-di-sorveglianza-occulta-e-sulla-captazione-di-conversa
- S.D. Warren-L.D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, Vol. 4, No. 5. (Dec. 15, 1890), 193-220
- R.L. Weaver, *Privacy in an Age of Advancing Technology*, in 82 *Miss. L.J.*, 2013, 975-996
- A. Wiebke, *Agents, Trojans and tags: The next generation of investigators*, in 23 *International Review of Law, Computers & Technology*, 1-2, 2009, 99-108
- R. Zaccaria, *Il «fermo» della corrispondenza ha ancora finalità censorie?*, in *Foro It.*, 1970, 7/8, 1980-1987

Giurisprudenza

Italia

Giurisdizione ordinaria

- Trib. Roma, 14 settembre 1953 (caso Caruso), in *Foro it.*, 1954, 1, 115-133
- Cass. civ., Sez. I, sent. n. 4487/1956, 22 dicembre 1956, (ancora sul cd. caso Caruso), in *Foro It.*, 80, 1, 4-11, 1957

- Cass. civ., Sez. II, sent. n. 1149/1963, 10 maggio 1963, in *Foro It.*, 86, 5, 1963, 874-877
- Cass. civ., Sez. I, sent. n. 3593/1969, 30 ottobre 1969
- Cass. civ., Sez. I, sent. n. 2129/1975 (cd. caso Soraya), 27 maggio 1975, in *Foro It.*, 99, 1, 1976, 2895-2907
- Cass. pen., Sez. I, sent. n. 4141/1992, 2 dicembre 1992
- Cass. pen., Sez. I, sent. n. 9370/1994, 31 agosto 1994
- Cass. pen., Sez. I, sent. n. 1367/1995, 10 febbraio 1995
- Cass. pen., Sez. I, sent. n. 1904/1996, 17 febbraio 1996
- Cass. pen., Sez. VI, sent. n. 7/1997, 4 marzo 1997
- Cass. pen., Sez. I, sent. n. 3901/1997, 28 aprile 1997
- Cass. pen., Sez. II, sent. n. 2873/1997, 10 ottobre 1997
- Cass. pen., Sez. I, sent. n. 3133/1997, 12 novembre 1997 (Cuomo)
- Cass. pen., Sez. VI, sent. n. 4397/1998, 21 gennaio 1998
- Cass. pen., Sez. VI, sent. n. 5156/1998, 21 gennaio 1998
- Cass. pen., Sez. I, sent. n. 22/1998, 4 aprile 1998
- Cass. pen., Sez. I, sent. n. 1495/1998, 4 maggio 1998
- Cass. pen., Sez. II, sent. n. 1831/1998, 10 giugno 1998
- Cass. pen., Sez. I, sent. n. 3458/1999, 17 marzo 1999
- Cass. pen., Sez. I, sent. n. 2505/1999, 17 giugno 1999
- Cass. pen., Sez. VI, sent. n. 8645/1999, 7 luglio 1999
- Cass. pen., Sez. I, sent. n. 4561/1999, 27 luglio 1999
- Cass. pen., Sez. VI, sent. n. 4057/1999, 6 ottobre 1999
- Cass. pen., Sez. III, sent. n. 2780/1999, 13 ottobre 1999
- Cass. pen., Sez. I, sent. n. 5239/1999, 4 novembre 1999
- Cass. pen., Sez. I, sent. n. 3541/1999, 2 dicembre 1999
- Cass. pen., Sez. VI, sent. n. 3067/1999, 14 dicembre 1999
- Cass. SS.UU., sent. n. 6/2000, 23 febbraio 2000
- Cass. pen., Sez. V, sent. n. 776/2000, 9 marzo 2000
- Cass. pen., Sez. II, sent. n. 2539/2000, 25 maggio 2000
- Cass. pen., Sez. I, sent. n. 3732/2000, 26 giugno 2000
- Cass. pen., SS.UU., sent. n. 17/2000, 21 settembre 2000

- Cass. pen., Sez. I, sent. n. 7671/2001, 23 febbraio 2001
- Cass. pen., SS.UU., sent. n. 42792/2001, 28 novembre 2001
- Cass. pen., Sez. IV, sent. n. 32667/2002, 1 ottobre 2002
- Cass. pen., Sez. IV, sent. n. 40790/2002, 4 dicembre 2002
- Cass. pen., Sez. VI, sent. n. 1625/2003, 15 gennaio 2003
- Cass. pen., Sez. II, sent. n. 8025/2004, 24 febbraio 2004
- Cass. pen., sent. n. 36439/2004
- Cass. pen. sent. n. 39469/2004
- Cass., SS. UU. pen., sent. n. 2737/2006, 29 novembre 2005 (Campenni)
- Cass. pen., Sez. II, sent. n. 1595/2006, 16 gennaio 2006
- Cass. SS. UU., sent. n. 26795/2006, 28 marzo 2006 (Prisco)
- Cass. pen., Sez. V, sent. n. 31135/2007, 6 luglio 2007
- Cass., SS. UU. pen., sent. n. 30347/2007, 12 luglio 2007 (Aguneche)
- Cass. pen., Sez. VI, sent. n. 15396/2007, 11 dicembre 2007
- Cass. pen., sez. II, sent. n. 16818/2008, 27 marzo 2008
- Cass. pen., SS.UU., sent. n. 36359/2008, 26 giugno 2008
- Cass. pen., Sez. VI, sent. n. 46056/2008, 12 dicembre 2008
- Cass. pen., Sez. V, sent. n. 16556/2009, 14 ottobre 2009
- Cass. pen. SS.UU., sent. n. 20300/2010, 22 aprile 2010 (Lasala)
- Cass. pen., Sez. V, sent. n. 5956/2012, 15 febbraio 2012
- Cass. pen., Sez. I, sent. n. 37212/2014, 5 settembre 2014
- Cass. pen., Sez. VI, sent. n. 27100/2015, 26 maggio 2015
- Cass. pen., SS. UU., sent. n. 26889/2016, 28 aprile 2016
- Cass. pen., Sez. V, sent. n. 1407/2017, 12 gennaio 2017
- Cass. pen., Sez. V, sent. n. 48370/2017, 20 ottobre 2017
- Cass. pen., Sez. VI, sent. n. 33046/2018, 25 gennaio 2018
- Cass. pen., Sez. IV, sent. n. 48543/2018, 24 ottobre 2018

Giurisprudenza costituzionale

- Corte Cost., sent. 100/1968
- Corte cost., sent. 34/1973

- Corte cost., sent. n. 38/1973
- Corte Cost., sent. n. 120/1975
- Corte cost., sent. 135/2002
- Corte cost., sent. 336/2008
- Corte cost., sent. 20/2017

Germania

- BVerfG, Primo Senato, 16 gennaio 1957, 1 BvR 253/56
- BVerfG, Secondo Senato, 15 dicembre 1970, 2 BvF 1/69, 2 BvR 629/68 e 308/69
- BVerfG, Primo Senato, 15 dicembre 1983, 1 BvR 209/83
- BGH, 31 gennaio 2007, StB 18/06
- BVerfG, Primo Senato, 27 febbraio 2008, 1 BvR 370/07,1 BvR 595/07
- BVerfG, Primo Senato, 20 aprile 2016, 1 BvR 966/09, 1 BvR 1140/09

Stati Uniti d'America

- *Alderman v. United States*, 394 U. S. 165 (1969)
- *Arizona v. Gant*, 556 U. S. 332 (2009)
- *Benanti v. United States*, 355 U.S. 96 (1957)
- *Berger v. New York*, 388 U.S. 41 (1967)
- *Boyd v. United* States, 116 U.S. 616 (1886)
- *Carpenter v. US*, 138 S. Ct. 2206 (2018)
- *Chimel v. California*, 395 U. S. 752 (1969)
- *City of Ontario v. Quon*, 560 U.S. 746 (2010)
- *Ex parte Jackson*, 96 U.S. 727 (1878)
- *Goldman v. United States*, 316 U.S. 129 (1942)
- *Goldstein v. United States*, 316 U.S. 114 (1942)
- *Katz v. United States*, 389 U.S. 347 (1967)
- *Letter opinion and order* nel caso *United States v. Nicodemo S. Scarfo,* 180 F.Supp.2d 572, U.S. District Court for the District of New Jersey, 26 Dicembre 2001, disponibile all'url: https://www.epic.org/crypto/scarfo/opinion.html
- *Nardone v. United States*, 302 U.S. 379 (1937)

- *Nardone v. United States*, 308 U.S. 338 (1939)
- *Olmstead v. United States*, 277 U.S. 438 (1928)
- *Pavesich v. New England Life Insurance Co.*, 122 Ga. 190, 50 S.E. 68 (1905)
- *Rakas v. Illinois*, 439 U.S. 128 (1978)
- *Riley v. California*, 573 U.S. 373 (2014)
- *Roberson v. Rochester Folding Box Co.*, 171 U. Y. 538, 64 N.E. 442 (1902)
- *Schwartz v. Texas*, 344 U.S. 199 (1952)
- *Silverman v. United States*, 365 U.S. 505 (1961)
- *Smith v. Maryland*, 442 U.S. 735 (1979)
- *Soldal v. Cook County*, 506 U. S. 56 (1992)
- *Terry v. Ohio*, 392 U.S. 1 (1968)
- *U.S. v. Chadwick*, 433 U.S. 1 (1976)
- *U.S. v. White*, 401 U.S. 745 (1971)
- *United States v. Forrester*, 495 F.3d 1041, U.S. Court of Appeals for the Ninth Circuit, 6-25 luglio 2007
- *United States v. Jones*, 565 U.S. 400 (2012)
- *United States v. Leon*, 468 U.S. 897 (1984)
- *US v. Lough*, 221 F. Supp. 3d 770, U.S. District Court for the Northern District of West Virginia, 18 novembre 2016
- *United States v. Martinez*, 498 F.2d 464, U.S. Court of Appeals for the Sixth Circuit 18 giugno 1974
- *United States v. Miller*, 425 U.S. 435 (1976)
- *United States v. Ramsey*, 503 F.2d 524, U.S. Court of Appeals for the Seventh Circuit, 6 agosto 1974
- *United States v. Robinson*, 414 U. S. 218 (1973)
- *United States v. Sklaroff*, 506 F.2d 837, U.S. Court of Appeals for the Fifth Circuit, 4 marzo 1975
- *US v. Warshak*, 631 F.3d 266, U.S. Court of Appeals for the Sixth Circuit, 14 dicembre 2010

Regno Unito

- *Huckle v. Money* (1763) 95 Eng. Rep. 768 (Common Pleas 1763)
- *Money v. Leack* (1765), 3 Burr 1742, 97 ER. 1075
- *Entick v. Carrington and Three Other King's Messengers*, 95 Eng. Rep. 807 (Common Pleas 1765)
- *Regina v. Aaron Caffrey*, Southwark Crown Court, 17 Ottobre 2003

Corte Europea dei Diritti dell'Uomo

- *A c. Francia*, no. 14838/89, Corte EDU, Camera, 23 novembre 1993
- *Amann c. Svizzera*, no. 27798/95, Corte EDU, Grande Camera, 16 febbraio 2000
- *Bărbulescu c. Romania*, no. 61496/08, Corte EDU, Grande Camera, 5 settembre 2017
- *Bykov c. Russia*, no. 4378/02, Corte EDU, Grande Camera, 10 marzo 2009
- *Campbell c. Regno Unito*, no. 13590/88, Corte EDU, Camera, 25 marzo 1992
- *Cevat Özel c. Turchia*, 19602/06, Corte EDU, II sez., 7 giugno 2016
- *Copland c. Regno Unito*, no. 62617/00, Corte EDU, IV sez., 3 aprile 2007
- *Craxi c. Italia (No. 2)*, no. 25337/94, Corte EDU, I Sez., 17 luglio 2003
- *Dragojević c. Croazia*, no. 68955/11, Corte EDU, I sez., 15 gennaio 2015
- *Dudgeon c. Regno Unito*, no. 7525/76, Corte EDU, Grande Camera, 22 ottobre 1981
- *Dumitru Popescu c. Romania (No 2)*, no. 71525/01, Corte EDU, III sez., 26 aprile 2007
- *Fernández Martínez c. Spagna*, no. 56030/07, Corte EDU, Grande Camera, 12 giugno 2014
- *Foxley c. Regno Unito*, no. 33274/96, Corte EDU, III sez., 20 giugno 2000
- *Golder c. Regno Unito*, no. 4451/70, Corte EDU, Camera, 21 febbraio 1975
- *Huvig c. Francia*, no. 11105/84, Corte EDU, Camera, 24 aprile 1990
- *Iordachi v. Moldavia*, no. 25198/02, Corte EDU, IV sez., 10 febbraio 2009
- *Karabeyoğlu c. Turchia*, no. 30083/10, Corte EDU, II sez., 7 giugno 2016
- *Kennedy c. Regno Unito*, no. 26839/05, Corte EDU, IV sez., 18 maggio 2010
- *Klass c. Germania*, no. 5029/71, Corte EDU, Grande Camera, 6 settembre 1978
- *Lebois c. Bulgaria*, no. 67482/14, Corte EDU, V sez., 19 ottobre 2017
- *Lüdi c. Svizzera*, no. 12433/86, Corte EDU, Camera, 15 giugno 1992
- *Malone c. Regno Unito*, no. 8691/79, Corte EDU, Sez. plenaria, 2 agosto 1984

- *Margareta and Roger Andersson c. Svezia*, no. 12963/87, Corte EDU, Camera, 25 febbraio 1992
- *Narinen c. Finlandia*, no. 45027/98, IV sez., 1 giugno 2004
- *Niemietz c. Germania*, no. 13710/88, Corte EDU, Camera, 16 dicembre 1992
- *Petri Sallinen c. Finlandia*, no. 50882/99, Corte EDU, IV sez., 25 settembre 2005
- *Petrov c. Bulgaria*, no. 15197/02, Corte EDU, V sez., 22 maggio 2008
- *Pfeifer e Plankl c. Austria*, no. 10802/84, Corte EDU, Camera, 25 febbraio 1992
- *Piechowicz c. Polonia*, no. 20071/07, Corte EDU, IV sez., 17 aprile 2012
- *Roman Zakharov c. Russia,* no. 47143/06, Corte EDU, Grande Camera, 4 dicembre 2015
- *S. e Marper c. Regno Unito*, no. 30562/04 e 30566/04, Corte EDU, Grande Camera, 4 dicembre 2008
- *Silver c. Regno Unito*, no. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75, Corte EDU, Camera, 25 marzo 1983
- *Szabó e Vissy c. Ungheria*, no. 37138/14, Corte EDU, IV sez., 12 gennaio 2016
- *Szuluk c. Regno Unito*, no. 36936/05 Corte EDU, IV sez., 2 giugno 2009
- *Trabajo Rueda c. Spagna*, no. 32600/12, Corte EDU, III Sez., 30 maggio 2017
- *Valenzuela Contreras c. Spagna*, 58/1997/842/1048, 30 luglio 1998
- *Vetter c. Francia*, no. 59842/00, Corte EDU, II sez., 31 maggio 2005
- *X c. Regno Unito*, no. 7308/75, Commissione EDU, 12 ottobre 1978
- *Z. c. Finlandia*, no. 22009/93, Corte EDU, Camera, 25 febbraio 1997

Corte di Giustizia dell'Unione Europea

- Cause riunite C-293/12 e C-594/12, Corte di Giustizia dell'Unione Europea (Grande Camera), 8 aprile 2014, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlanda, The Attorney General* e *Kärntner Landesregierung, M.S., C.T. e a.*
- Cause riunite C-203/15 e C-698/15, Corte di Giustizia dell'Unione Europea (Grande Camera), 21 dicembre 2016, *Tele2 Sverige AB c. Post- och telestyrelsen* e *Secretary of State for the Home Department c. T.W., P.B., G.L.*

Miscellanea

- Atti della Commissione per la Costituzione, Vol. IV
- Atti di discussione in Assemblea Costituente, Vol. III
- Explanatory Report to the Convention on Cybercrime, Budapest, 23.XI.2001, disponibile all'url: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b (ultimo accesso: 23 gennaio 2021).
- *Guide on Article 8 of the European Convention on Human Rights*, disponibile all'url: https://www.echr.coe.int/documents/guide_art_8_eng.pdf (ultimo accesso: 23 gennaio 2021)