



UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di Diritto Pubblico, Internazionale e Comunitario - DiPIC

Corso di Laurea Triennale in Diritto e Tecnologia

a.a. 2022/2023

Tesi di Laurea

INTERCETTAZIONI E PROTEZIONE DEI DIRITTI FONDAMENTALI: UN DIFFICILE BILANCIAMENTO TRA ESIGENZE REPRESSIVE E TUTELA DELL'INDAGATO

Relatore

Prof. Massimo Bolognari

Laureanda

Francesca Oriente

N° matr. 2007401

RINGRAZIAMENTI

Al termine di questo intenso percorso ringrazio, anzitutto, il prof. Massimo Bolognari, mio relatore, che con attenzione ha seguito il mio lavoro.

Ringrazio con tutto il cuore la mia famiglia che mi ha sostenuta dandomi sempre la possibilità di compiere le mie scelte in libertà.

Ma ringrazio soprattutto me stessa per non aver mai mollato nonostante le difficoltà e gli impegni che a volte hanno messo alla prova la mia audacia.

INDICE

INTRODUZIONE	1
1. LE INTERCETTAZIONI	3
1. DEFINIZIONE E GENESI STORICA	3
2. OGGETTO, PRESUPPOSTI E LIMITI DELLE INTERCETTAZIONI.....	7
3. DISCIPLINA E AMMISSIBILITÀ DELLE INTERCETTAZIONI	11
2. L’IMPATTO DELLE INTERCETTAZIONI SUL DIRITTO ALLA <i>PRIVACY</i>.....	15
1. L’EVOLUZIONE DEL DIRITTO ALLA <i>PRIVACY</i>	15
2. I LUOGHI TUTELATI DALLA <i>PRIVACY</i> A FRONTE DI INDAGINI PENALI.....	18
3. I LIVELLI DI TUTELA PREVISTI NEL NOSTRO ORDINAMENTO	20
4. L’ESPERIENZA TEDESCA COME CASO PARADIGMATICO DI PROTEZIONE RAFFORZATA DELLA <i>PRIVACY</i>	21
5. LA FASE DI STRALCIO DELLE CONVERSAZIONI INTERCETTATE A PROTEZIONE DELLA RISERVATEZZA SECONDO LA DELEGA IN MATERIA DI INTERCETTAZIONI	23
3. L’IMPATTO DELLE INTERCETTAZIONI SUL DIRITTO ALL’INVIOLABILITÀ DEL DOMICILIO.....	27
1. UN INQUADRAMENTO DEL DIRITTO ALL’INVIOLABILITÀ DEL DOMICILIO.....	27
2. L’INDIVIDUAZIONE DEI LUOGHI RIENTRANTI NELLA NOZIONE DI DOMICILIO E I LUOGHI INFORMATICI E DIGITALI.....	29
3. L’ART. 14 COST. E LA NECESSITÀ DI UN NUOVO DIRITTO	32
CONCLUSIONI	35
BIBLIOGRAFIA	37
SITOGRAFIA.....	39

INTRODUZIONE

Le tecnologie stanno trasformando il nostro modo di vivere e l'impiego di queste ultime nell'attività di repressione dei reati assume un crescente importanza. Non si tratta, però, di un'operazione agevole. Il legislatore, infatti, fatica ad adattare gli istituti tradizionali alle nuove tipologie di atti investigativi che fanno uso delle tecnologie, con la conseguenza che si creano vuoti di tutela e si verificano gravi violazioni dei diritti fondamentali. Si pensi, ad esempio, a quanto avviene con le intercettazioni mediante captatore informatico, le quali comportano significative intromissioni nella vita delle persone.

Questo elaborato è volto ad analizzare e ad approfondire l'impatto delle intercettazioni sui diritti fondamentali, prendendo in esame il diritto alla *privacy* e il diritto all'inviolabilità del domicilio.

Anzitutto, si è deciso di approfondire i vari aspetti concernenti le intercettazioni. *In primis*, dopo aver dato la definizione di tale mezzo, si è svolta un'analisi di tipo storico: dal primo uso dell'intercettazione telefonica negli ultimi anni del 1800, passando per la nota Sentenza *Katz v. United States*, sino ad arrivare all'impiego in Italia di tale strumento. L'evoluzione italiana su cui mi sono concentrata ha toccato il primo uso di intercettazioni del 1903, l'impostazione adottata dal Governo Mussolini e i cambiamenti normativi dalla redazione della Costituzione nel 1947 fino alle modifiche normative del 2017. Si sono poi approfondite le modalità captative, i limiti e i presupposti relativamente alle intercettazioni telefoniche e ambientali, concentrandomi poi in modo più esteso su quelle informatiche o telematiche.

Nel capitolo successivo si è analizzato l'impatto delle intercettazioni sul diritto alla *privacy*, ponendo l'attenzione inizialmente sul suo sviluppo storico dal XIX secolo nei Paesi di *common law*, per poi focalizzarsi sulla sua evoluzione in rapporto allo sviluppo tecnologico. Inoltre, si sono richiamate le fonti che prevedono espressamente il diritto alla *privacy*, sia a livello italiano sia internazionale. Una distinzione importante che si è approfondita è quella concernente i livelli di tutela previsti per i diversi luoghi, quando

su questi si effettuano indagini penali. Un tema ulteriore affrontato riguarda l'esperienza tedesca in relazione alla protezione della riservatezza durante le intercettazioni, come caso concreto in cui si è reso necessario compiere un bilanciamento tra l'esigenza di reprimere la criminalità e, allo stesso tempo, tutelare i diritti fondamentali dell'indagato. Infine, si sono esaminate le novità introdotte dalla legge-delega all'interno della riforma Orlando.

Nel terzo ed ultimo capitolo si è analizzato l'impatto delle intercettazioni sul diritto all'inviolabilità del domicilio, arrivando alla conclusione che, nonostante siano stati fatti passi avanti, soprattutto grazie all'interpretazione estensiva della giurisprudenza rispetto all'ambito di tutela dei diritti fondamentali, ci sono ancora eccessivi spazi di discrezionalità.

Nel paragrafo iniziale si è analizzato l'art. 14 Cost. cercando di inquadrare la nozione di domicilio. Successivamente, si è operata una distinzione tra i luoghi che rientrano nella nozione di domicilio tradizionale e dunque nell'ambito di tutela dell'art. 14 Cost., domandandosi se uno spazio digitale possa essere considerato domicilio.

Infine, ho cercato di capire se le intercettazioni debbano rientrare o meno nell'ambito della tutela previsto per il domicilio e quindi se debbano essere attuate determinate garanzie, in quanto nel comma citato l'elenco è limitato a tre atti investigativi che esulano le intercettazioni.

1. LE INTERCETTAZIONI

1.1. DEFINIZIONE E GENESI STORICA

Il nostro codice di procedura penale non fornisce alcuna definizione esaustiva del mezzo investigativo delle intercettazioni. Tuttavia, nell'opera definitoria si sono cimentate sia la giurisprudenza sia la dottrina. Quest'ultima ha cercato di colmare questo vuoto definendo l'intercettazione un mezzo di ricerca della prova, la cui caratteristica principale è di essere uno strumento occulto agli interessati per l'intero svolgimento dell'indagine¹. Dal canto suo, la Corte di Cassazione Sez. unite nella sentenza 24 settembre 2003, n. 36747 ha definito l'intercettazione «l'apprensione occulta, in tempo reale, del contenuto di una conversazione o di una comunicazione in corso tra due o più persone da parte di altri soggetti, estranei al colloquio».

L'intercettazione telefonica come mezzo investigativo ha origine e trova applicazione inizialmente in Gran Bretagna e negli Stati Uniti tra la fine del 1800 e i primi decenni del 1900². Soprattutto negli ultimi anni del suddetto periodo tale mezzo investigativo venne usato durante il c.d. Proibizionismo: il suo indiscriminato utilizzo per prevenire e reprimere la vendita e il contrabbando di bevande alcoliche rese necessario revisionare i precetti costituzionali sulle libertà civili.

Un caso giurisprudenziale di particolare importanza fu il caso *Olmstead v. United States*, 277 U.S. 438 (1928) aperto nel 1926: la Corte Federale dello Stato di Washington, basandosi su prove raccolte a seguito di intercettazioni avvenute con il telefono della polizia, condannò a 4 anni di reclusione e al pagamento di 8.000 dollari il trafficante di alcool Roy Olmstead per aver violato la legge sul divieto di fabbricazione, vendita, importazione e trasporto di alcool (*Volstead Act*). Due anni dopo, però, Roy Olmstead

¹ Scarpino, Daniele. "La Disciplina Delle Intercettazioni Telefoniche Ed Ambientali - Rivista Penale Diritto e Procedura." *Rivista Penale Diritto e Procedura*, 20 Jan. 2023, <https://www.penaledp.it/la-disciplina-delle-intercettazioni-telefoniche-ed-ambientali-2/>.

² Alfredo, Gaito. *Diritto Alla Riservatezza e Intercettazioni: Un Bilanciamento è Possibile?* Seminario; diritto alla riservatezza e intercettazioni, Facoltà di Giurisprudenza Sapienza Università di Roma, Anno accademico 2012–2013, p.7.

impugnò la decisione alla Corte Suprema degli Stati Uniti per la lesione dei diritti sanciti dal IV e dal V emendamento della Costituzione americana concernenti la difesa, sostenendo che questi erano stati conculcati dalle intercettazioni telefoniche svolte dalla polizia senza vaglio del giudice e usate come prove in giudizio. In particolare, il IV emendamento prevede «il diritto dei cittadini di godere della sicurezza personale, della loro casa, delle loro carte e dei loro beni, nei confronti di perquisizioni e sequestri ingiustificati»³ e il V garantisce il diritto al giusto processo a seguito della commissione di un reato.

La Corte respinse il ricorso per mancata violazione degli emendamenti sopra citati; tuttavia, nel 1967 nella sentenza *Katz v. United States* ribaltò la decisione del 1928 dichiarando la “prevalenza costituzionale del diritto alla *privacy* sui mezzi di ricerca della prova”⁴ ed in particolare sulle intercettazioni utilizzate in quel caso.

In Italia, invece, a causa del raro utilizzo delle intercettazioni, dovuto soprattutto all’insufficienza degli strumenti tecnici e alla scarsa consapevolezza della sua efficacia, l’approccio alla materia fu diverso: il codice del 1865 non prevedeva alcuna disciplina; inoltre, gli articoli 170 e 238 nel codice del 1913 si occupavano della materia solo in modo superficiale.

Il primo caso in cui venne in gioco l’uso delle intercettazioni risale al 1903, quando vennero registrati gli estremi di una telefonata nella quale un Ministro dell’allora Regno d’Italia del Governo Giolitti e la moglie si scambiavano informazioni di carattere finanziario. In concreto la telefonata riguardava l’approvazione del decreto finanziario che sarebbe stato promulgato il giorno successivo e il consiglio del ministro alla moglie di investire su determinati titoli. La telefonata fu ascoltata dal centralinista che, a causa dell’anomalia della conversazione, ne registrò gli estremi e tutti i dettagli provocando il rinvio del decreto; tuttavia, la conseguenza più significativa dell’evento fu l’istituzione del Servizio di Intercettazione della Polizia di Stato per la vigilanza delle personalità pubbliche⁵.

³ Citazione testuale del IV emendamento della Costituzione degli Stati Uniti d’America

⁴ Articolo di Bill Scott tratto da *The History of Prohibition*; Alfredo, Gaito. *Diritto Alla Riservatezza e Intercettazioni: Un Bilanciamento è Possibile?* Seminario; diritto alla riservatezza e intercettazioni, Facoltà di Giurisprudenza Sapienza Università di Roma, Anno accademico 2012–2013, p. 8.

⁵ Alfredo, Gaito. *Op. cit.*, p. 8.

Il Governo Mussolini promulgò il terzo codice di procedura penale, il c.d. Codice Rocco, il quale disciplinava anche le intercettazioni. In particolare, mantenne invariati gli artt. 226 e 339 del precedente codice del 1913, i quali recitavano rispettivamente: «Gli ufficiali di polizia giudiziaria, per fini del loro servizio, possono accedere agli uffici o agli impianti di pubblico servizio per trasmettere, intercettare o impedire comunicazioni prenderne cognizioni o assumere altre informazioni»⁶ e «Il giudice può accedere agli uffici o impianti telefonici di pubblico servizio e trasmettere, intercettare o impedire comunicazioni, assumere cognizione. Può anche delegare un ufficiale di polizia giudiziaria»⁷. È evidente quanto queste disposizioni fossero assolutamente prive di principi garantisti autorizzando, in particolare, un forte potere in capo alla polizia giudiziaria e al giudice. Esempio pratico sostanziale fu l'ordine dato da Mussolini al Servizio di Intercettazione di mantenere sotto controllo i telefoni di esponenti di partiti politici di opposizione, militari, giornalisti, diplomatici stranieri e avvocati, numerando le loro conversazioni ed etichettandole con i relativi interlocutori e con il carattere della conversazione⁸. Emblematica fu anche l'applicazione di tali disposizioni nel 1924 con il delitto Matteotti: furono mantenuti sotto controllo i telefoni dei giornali per monitorare costantemente le notizie.

Un simile assetto venne superato con l'avvento della Costituzione del 1947. In particolare, l'art. 15 Cost. tutela la libertà e la segretezza delle comunicazioni, consentendo una loro limitazione solo con atto motivato dell'autorità giudiziaria⁹.

Un passo successivo avvenne nel 1955 con l'emanazione della legge n. 517, la quale inserì un 4° comma all'art. 266 del c.p.p. Quest'ultimo prevedeva in capo all'autorità giudiziaria l'obbligo di motivare l'atto con cui venivano disposte le intercettazioni. I presupposti, i termini, le modalità di esecuzione delle intercettazioni e le sanzioni in caso di loro violazione, furono previsti dalla successiva legge n. 98/1974.

Con il fenomeno del terrorismo e della criminalità organizzata degli anni '80 si tornò ad un'impostazione che privilegiava le istanze repressive. Emblematica a riguardo fu la legge n. 191/1978: oltre a prevedere, ad esempio, l'uso di intercettazioni per scopi diversi

⁶ Citazione testuale dell'art. 226 del Codice Rocco

⁷ Citazione testuale dell'art. 339 del Codice Rocco

⁸ Alfredo, Gaito. *Op. cit.*, p. 8.

⁹ Alfredo, Gaito. *Op. cit.*, p. 9.

da quelli per i quali inizialmente il mezzo investigativo era stato disposto, si prevedeva anche l'uso di intercettazioni preventive.

Il sistema mutò nuovamente con il Codice di Procedura Penale in vigore dal 1989, che specificatamente nella sezione "Intercettazioni di conversazioni o comunicazioni" al Capo IV segnò il passaggio ad un sistema di tipo accusatorio, i cui pilastri sono regole certe ed eque per entrambe le parti nel processo penale¹⁰. Inoltre, le intercettazioni divennero un mezzo di ricerca della prova del pubblico ministero su autorizzazione del GIP, dunque non più nelle mani della polizia giudiziaria. In particolare, ora vige il principio del contraddittorio, l'onere della prova in capo all'accusatore e il principio di innocenza fino a prova contraria¹¹.

Successivamente alla promulgazione dell'ultimo codice, la materia delle intercettazioni ha subito molte modifiche, che verranno approfondite di seguito, proprio alla luce della necessità di adeguare la disciplina e la prassi ai cambiamenti tecnologici e allo sviluppo di nuovi sistemi informatici. Emblematica, ad esempio, è l'introduzione dell'art. 266-*bis* c.p.p. avvenuta con la l. n. 547 del 23 dicembre 1993 concernente le intercettazioni informatiche o telematiche. Nel 2017 un ulteriore passo è stato compiuto con la riforma Orlando (decreto legislativo n. 216 del 2017), la quale ha apportato importanti modifiche al codice di procedura penale in materia di intercettazioni, tra cui, ad esempio, l'inserimento di ulteriori reati tra quelli per cui è eseguibile il mezzo investigativo e l'estensione dei casi in cui è possibile utilizzare il captatore informatico (c.d. *trojan horse*).

Questa evoluzione fa notare quanto la disciplina delle intercettazioni sia sensibile alle fluttuazioni politiche, oscillando costantemente tra un'impostazione che privilegia le istanze repressive e l'esigenza di fissare presidi a tutela dell'individuo.

¹⁰ Alfredo, Gaito. *Op. cit.*, p. 9

¹¹ Alfredo, Gaito. *Op. cit.*, p. 9

1.2. OGGETTO, PRESUPPOSTI E LIMITI DELLE INTERCETTAZIONI

Dopo aver approfondito l'evoluzione storica di tale mezzo investigativo, è importante capire quali siano i presupposti e le modalità con cui questo viene attuato. Anzitutto, dal punto di vista normativo, la disciplina delle intercettazioni è prevista nel capo IV del titolo III del Libro III del codice di procedura penale. In particolare, come è già stato evidenziato, lo strumento appartiene al genere dei mezzi di ricerca della prova, utili all'individuazione di soggetti o cose dalle quali si possono trarre elementi rilevanti e utili ai fini dell'esecuzione del procedimento di accertamento di illeciti penali e, più in specifico, di un fatto-reato.

La categoria delle intercettazioni telefoniche è consentita e circoscritta dal comma 1 dell'art. 266 c.p.p.; il comma 2 dello stesso contempla le intercettazioni ambientali anche mediante captatore informatico e infine, l'art. 266-bis c.p.p. consente le intercettazioni informatiche e telematiche. L'art. 267 c.p.p. indica con precisione i presupposti e le forme del provvedimento con cui viene ordinato il mezzo investigativo, in particolare prevede che quest'ultimo debba essere disposto previa autorizzazione da parte del giudice per le indagini preliminari su richiesta del pubblico ministero. L'autorizzazione viene concessa allorché sussista il requisito dell'indispensabilità dell'intercettazione ai fini delle indagini e ci siano gravi indizi di reato. Inoltre, il decreto deve indicare i motivi per cui si è reso necessario ricorrere a tale mezzo investigativo. Nei soli casi di urgenza è lo stesso pubblico ministero a disporre l'intercettazione con decreto motivato che dovrà essere successivamente convalidato dal GIP entro 48 ore, pena l'interruzione dell'attività investigativa e l'inutilizzabilità dei risultati.

La disciplina delle intercettazioni sottopone queste ultime a due limiti: quello oggettivo/quantitativo prevede che il mezzo investigativo sia ammesso solo per i reati enucleati nel comma 1 dell'art. 266 c.p.p., e quello soggettivo, il quale vieta l'uso del mezzo per intercettare conversazioni che coinvolgono il Presidente della Repubblica, i parlamentari italiani ed europei, i giudici costituzionali e altri soggetti che verranno poi indicati al capitolo 2.

Connesso alle modalità operative è il requisito della simultaneità, necessario al fine di qualificare l'intercettazione come tale: si intende simultanea l'attività di captazione svolta tramite strumenti tecnici che consentano di apprendere il contenuto della comunicazione oggetto dell'indagine nello stesso tempo in cui essa avviene. Nel caso in cui non sussista questo requisito, l'intercettazione non potrà rientrare nel perimetro dell'art. 266 c.p.p. Ad esempio, non può considerarsi intercettazione la captazione di una registrazione di un messaggio di segreteria telefonica in quanto la prima è avvenuta in un momento successivo al colloquio originale. Nel caso di mancanza del suddetto requisito, la conversazione rientrerà nell'ambito di applicazione dell'art. 253 c.p.p. qualora sussistano i presupposti per procedere al sequestro probatorio del materiale.

In riferimento all'oggetto dell'intercettazione, questa può essere suddivisa in tre categorie: telefonica, ambientale ed informatica o telematica.

Nella prima rientra la captazione di comunicazioni telefoniche, le quali sono processi di trasmissione di segnali elettrici ed elettromagnetici attraverso reti di telecomunicazione che permettono a due parti di scambiarsi informazioni in tempo reale. Al fine dell'esecuzione delle intercettazioni telefoniche, è previsto che la polizia giudiziaria possa richiedere agli operatori che gestiscono le reti di telefonia generale di adempiere all'autorizzazione dell'autorità giudiziaria (GIP) mediante le loro strutture tecnologiche. In particolare, agli operatori telefonici è richiesto di duplicare le telefonate oggetto dell'intercettazione e di mandarle al c.d. Centro Intercettazioni Telefoniche della Procura della Repubblica per la successiva analisi investigativa. Di prassi le telefonate vengono protette da sistemi di cifratura a seguito della loro registrazione, in modo tale da renderle leggibili solo per chi possiede la chiave di decrittazione¹².

L'intercettazione ambientale permette di captare le conversazioni tra persone presenti principalmente grazie all'utilizzo di microspie o "cimici" facilmente installabili e occultabili nei luoghi dove si trovano gli indagati, come, ad esempio, gli abitacoli delle autovetture¹³. Le più diffuse sono le c.d. microspie UMTS, le quali sono in grado di trasmettere a distanze illimitate audio e immagini sfruttando la rete di telefonia mobile

¹² "Intercettazioni Telefoniche." *Axerta*, 3 Mar. 2019, <https://www.axerta.it/intercettazione-telefonica/>.

¹³ "Intercettazioni Ambientali: Cosa Sono e Come Funzionano." *DOGMA*, <https://www.dogma.it/it/news/intercettazioni-ambientali>.

cellulare UMTS. Tuttavia, queste riescono ad operare in un raggio d'azione limitato. Le intercettazioni vengono svolte anche attraverso l'utilizzo di microtelecamere che consentono di registrare tutto ciò che avviene nell'ambiente circostante, di registratori, di rilevatori GPS con microspia installata e di microfoni direzionali per captare le conversazioni a distanza. Una prassi diffusa consiste nell'installazione dei suddetti dispositivi in luoghi chiusi e piccoli che, grazie alla loro conformazione, permettono una captazione meno disturbata¹⁴.

Diversa natura presentano le intercettazioni informatiche o telematiche: queste permettono di «captare un flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi», come previsto dall'art. 266-bis. c.p.p. Questo tipo di attività investigativa richiede l'uso di tecnologie informatiche e telematiche, quali il captatore, chiamato anche *trojan horse*, o la tecnica del reindirizzamento.

Il captatore informatico è un *software* che viene installato all'insaputa dell'indagato nei dispositivi elettronici di quest'ultimo, quali ad esempio: cellulare, *computer*, *tablet*. L'installazione del *software* può avvenire fisicamente dalla polizia in un dispositivo sottoposto ad intercettazione, ipoteticamente quando questo si trovi incustodito, oppure in modalità remota dall'indagato stesso. In quest'ultimo caso il *software* può essere installato a seguito di un semplice 'click' su un *link* presente in una *e-mail* ricevuta o a seguito dell'installazione di un aggiornamento *software* che inconsapevolmente permette l'installazione del *malware*. Una condizione necessaria ai fini del funzionamento del captatore è il collegamento alla rete. Quanto, invece, al piano tecnico il *software* ha due componenti: un *server*, il quale è rappresentato da un programma che infetta il dispositivo elettronico, e il *client* in cui risiede l'applicazione che lo monitora¹⁵.

Il captatore permette di svolgere molteplici operazioni sul dispositivo. In particolare, può visualizzare e monitorare le immagini che appaiono sullo schermo, o tutto ciò che viene digitato sulla tastiera; per di più capta e registra i suoni provenienti dal microfono¹⁶. È

¹⁴ “Intercettazioni Ambientali: Cosa Sono e Come Funzionano.” *DOGMA*, <https://www.dogma.it/it/news/intercettazioni-ambientali>.

¹⁵ Oliviero, Mazza. *Le Nuove Intercettazioni*. G Giappichelli Editore, 2018, p.102.

¹⁶ Oliviero, Mazza. *Op. cit*, p. 102.

rilevante il vantaggio per cui, essendo il captatore azionabile da remoto, esso non richiede l'intrusione fisica degli operatori.

Un'altra possibile funzione è l'*online search*, che consente di copiare i dati, le informazioni e la memoria del dispositivo¹⁷; ulteriore potenziale del *trojan* è la capacità di captare i flussi di informazioni tra le periferiche di un dispositivo (microfono, schermo, tastiera) e il suo microprocessore¹⁸. Tale funzione viene denominata *online surveillance*.

La seconda modalità con la quale possono essere svolte le intercettazioni informatiche o telematiche è la tecnica del reindirizzamento. Quest'ultima permette di captare i flussi comunicativi tra più sistemi informatici o telematici prima che tali dati arrivino al destinatario. Ciò è permesso necessariamente dalla collaborazione con il *provider*¹⁹. A sua volta il reindirizzamento può captare *e-mail*, video, messaggi, audio oppure comunicazione vocali tramite *Internet*. Nel primo caso si presuppone che tutto avvenga in modo sincrono, ovvero che la captazione si attivi nel momento in cui il flusso avviene, e che la comunicazione sia effettuata tra due o più persone²⁰. Nel secondo caso, invece, vengono captate le comunicazioni digitali attraverso il protocollo VoIP (*Voice over Internet Protocol*). In questo contesto un problema che assume rilievo è la protezione crittografica che spesso presentano le comunicazioni VoIP: nel caso in cui questa sia attiva, l'attività investigativa è possibile solo tramite la decrittazione, le cui chiavi sono in possesso esclusivamente dei gestori del servizio di comunicazione, oppure tramite il *trojan*. Nel caso opposto, invece, l'intercettazione si configura come captazione diretta del contenuto comunicativo²¹.

¹⁷ Oliviero, Mazza. *Op. cit.*, p. 102.

¹⁸ Oliviero, Mazza. *Op. cit.*, p. 102.

¹⁹ Silvia, Signorato. *Le Indagini Digitali. Profili Strutturali Di Una Metamorfosi Investigativa*. G. Giappichelli Editore, 2018, p. 249

²⁰ Silvia, Signorato. *Op. cit.*, p. 250

²¹ Silvia, Signorato. *Op. cit.*, p. 253

1.3. DISCIPLINA E AMMISSIBILITÀ DELLE INTERCETTAZIONI

Gli interventi del legislatore al fine di disciplinare il mezzo investigativo analizzato sono molteplici: in una caotica produzione normativa caratterizzata da decreti legislativi, leggi, decreti legge e leggi di conversione, si è reso necessario determinare quale sia l'effettiva disciplina applicabile. Tra i provvedimenti principali si possono identificare il d.lgs. 29 dicembre 2017, n. 216 (la c.d. Riforma Orlando) analizzata di seguito, la legge 9 gennaio 2019, n.3 (legge Spazzacorrotti) e il d.l. 30 dicembre 2019, n. 161 convertito dalla legge n. 7 del 2020 (c.d. riforma Bonafede).

Il primo, in particolare, oltre a introdurre il reato di diffusione di riprese e registrazioni fraudolente, si dedica prevalentemente di intercettazioni di comunicazioni²².

La c.d. Legge Spazzacorrotti, dal canto suo, apporta variazioni alla disciplina delle intercettazioni: da un lato modifica l'art. 6 d.lgs. n. 216 del 2017 eliminando il requisito dello svolgimento di un'attività criminale nei luoghi di privata dimora nei casi di reati contro la pubblica amministrazione, dall'altro lato inserisce l'art. 267 co. 2-*bis* c.p.p., il quale prevede i casi in cui è autorizzato l'inserimento del captatore informatico su un dispositivo elettronico portatile, e l'art. 267 co. 1 terzo periodo c.p.p. che sancisce cosa deve prevedere il decreto autorizzativo.

La successiva riforma Bonafede del 2019 rivede la disciplina delle intercettazioni telefoniche e si applica ai procedimenti penali iscritti successivamente al 31 agosto 2020.

La disciplina delle intercettazioni ambientali risulta differente rispetto a quella delle intercettazioni telefoniche o informatiche/telematiche; infatti, per le prime risulta necessario un fondato motivo di ritenere che in quel determinato luogo si stia svolgendo un'attività criminosa²³. Di conseguenza, l'atto autorizzativo dovrà indicare i motivi e le esigenze concrete di repressione dei reati: in particolare, all'art. 267 c.p.p. è previsto che

²² Glauco, Giostra, e Renzo, Orlandi. *Revisioni Normative in Tema Di Intercettazioni*. G. Giappichelli Editore, 2020, p. 158.

²³ Citazione testuale dell'art. 266, co. 2, c.p.p.

l'autorizzazione debba essere concessa quando vi siano gravi indizi di reato e quando l'intercettazione risulta indispensabile ai fini della prosecuzione delle indagini²⁴.

Le intercettazioni informatiche o telematiche svolte in particolare attraverso il captatore informatico sono state per lungo tempo al centro di dibattiti giurisprudenziali e politico-legislativi²⁵, a causa del carattere estremamente invasivo sui diritti fondamentali dell'individuo. Al riguardo, risultano di particolare interesse la Sentenza Scurato (Cass., Sez. Un., 28 aprile 2016) e il già citato d.lgs. n. 216 del 2017 (c.d. Riforma Orlando). Dalla sentenza Scurato emergeva come l'impiego del captatore informatico dovesse essere sottoposto ad un duplice limite: il suo uso era strumentale alle intercettazioni ambientali ed esclusivamente ai reati di criminalità organizzata. Fondante questi limiti era il dubbio della Corte sulla legittimità delle intercettazioni di conversazioni tra presenti mediante captatore anche in luoghi di privata dimora a prescindere dall'attuale svolgimento di un'attività criminosa²⁶. A questa perplessità consegue la disciplina delle intercettazioni per i reati di criminalità organizzata, secondo la quale le captazioni sono possibili anche nei luoghi di privata dimora, sia pur non singolarmente individuati, senza che ci sia un fondato motivo di ritenere che ivi si stia svolgendo attività criminosa. Quest'ultima condizione, al contrario, è prevista dall'art. 266 co.2 c.p.p (novellato dalla riforma Orlando) per i reati comuni.

Tale scelta del legislatore, secondo la logica del doppio binario processuale, risultava conciliare le potenzialità invasive dello strumento investigativo, ovvero il sacrificio dei diritti individuali come la libertà e la segretezza delle comunicazioni, con gli scopi investigativi, vedendo così rispettato il principio di proporzionalità.

È proprio in questo contesto che il legislatore è intervenuto con la riforma Orlando, la quale ha novellato l'art. 266 c.p.p. prevedendo la possibilità di inoculare il captatore in dispositivi elettronici portatili. Inoltre, come anticipato precedentemente, ha previsto la necessità di un fondato motivo di ritenere che si stia svolgendo un'attività criminosa come requisito per le intercettazioni eseguite in luoghi di privata dimora, menzionati all'art. 214 c.p. La riforma ha poi stabilito che per i reati previsti dall'art. 51, commi 3-bis e 3-quater

²⁴ Citazione testuale dell'art. 267, co. 1, c.p.p.

²⁵ Silvia, Signorato. *Op. cit.*, p. 240.

²⁶ Glauco, Giostraco, e Renzo, Orlandi. *Op. cit.*, p. 258.

c.p.p. le intercettazioni siano sempre eseguibili. Viene, infine, stabilito all'art. 267 c.p.p. che il decreto autorizzativo debba indicare «i luoghi e il tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono»²⁷. Inoltre, va evidenziato come la riforma sia intervenuta solo in ambito di intercettazioni su dispositivi mobili all'art. 266 c.p.p. dedicato alle intercettazioni di conversazioni o comunicazioni e non nel contesto dell'art. 266-bis dedicato alle intercettazioni di comunicazioni informatiche o telematiche²⁸ tramite *Internet*. Questa limitazione della Riforma non considera le particolarità tecniche dell'intercettazione, la quale consente di captare, oltre alle voci dell'ambiente in cui si trova il dispositivo su cui il *software* è installato, anche le comunicazioni telefoniche effettuate con quel dispositivo e allo stesso tempo le comunicazioni tramite *Internet*. Il problema è che nel momento in cui si installa il captatore non si può sapere che tipo di comunicazione verrà intercettata; di conseguenza, quando il pubblico ministero dovrà richiedere al giudice per le indagini preliminari l'autorizzazione a disporre un'intercettazione, non potrà sapere se richiederla ai sensi dell'art. 266 c.p.p. o dell'art. 266-bis c.p.p.

Un altro aspetto problematico riguarda poi la previsione secondo la quale il decreto autorizzativo deve indicare i luoghi e il tempo in cui si effettua l'intercettazione. In riferimento soprattutto ai primi, è importante rilevare la molteplicità dei luoghi in cui si può trovare il dispositivo e la difficoltà, soprattutto, di predeterminarli²⁹. Una possibile soluzione che possa risolvere il problema è considerare il dispositivo stesso come luogo, in quanto il luogo dove viene installato il captatore non corrisponde ai luoghi in cui si sposta il dispositivo. Di conseguenza nel decreto ci si può limitare all'indicazione dello specifico dispositivo informatico.

Un ulteriore importante profilo della riforma Orlando concerne le captazioni sonore, in particolare l'attivazione del microfono tramite captatore, previsione attuale contenuta nell'art. 267 co. 1 c.p.p.: si stabilisce che esso venga attivato solo successivamente ad un apposito comando inviato da remoto, in linea con il principio di proporzionalità e con la necessità di evitare che il captatore possa giungere a risultati ulteriori rispetto alle originali previsioni. Questo limite alle intercettazioni sorge alla luce della pervasività dei mezzi

²⁷ Silvia, Signorato. *Op. cit.*, p. 241

²⁸ Silvia, Signorato. *Op. cit.*, p. 242

²⁹ Silvia, Signorato. *Op. cit.*, p. 245.

elettronici e informatici di cui le persone sono costantemente in possesso: grazie a questa sarebbe possibile per gli investigatori controllare ed intercettare l'individuo in qualsiasi momento e luogo, compreso quello privato, senza dover affrontare i limiti di un'eventuale microspia tradizionale.

L'art. 270 co. 1-*bis* c.p.p., introdotto dal d.lgs. n. 216/2017, sancisce che il materiale captato a seguito di intercettazioni su dispositivi elettronici portatili non possa essere utilizzato come prova di reati diversi da quelli per i quali è stato emesso il decreto preventivo di autorizzazione, ad eccezione del caso in cui il materiale sia necessario per accertare reati per i quali è obbligatorio l'arresto in flagranza³⁰. Questa previsione, al contrario, non si applica nel caso in cui le intercettazioni siano tradizionali: la giurisprudenza ritiene che il materiale intercettato possa essere utilizzato anche per reati giuridicamente qualificati in modo diverso.

Sono state poi previste cautele ulteriori per circoscrivere e limitare l'utilizzo delle intercettazioni informatiche: l'art. 5 del d.lgs. n. 216/2017 prevede che dal punto di vista tecnico si debbano utilizzare obbligatoriamente programmi informatici conformi a standard tecnici prestabiliti e l'art. 7 obbliga a un controllo costante dell'integrità informatica al fine di assicurare l'immodificabilità dei dati intercettati e registrati³¹, coerentemente con i principi di affidabilità, sicurezza ed efficacia. Ulteriore vincolo prevede che il controllo, l'avvio e la cessazione delle operazioni di intercettazione siano svolti da personale qualificato che abbia le competenze tecniche necessarie e funzionali.

A seguito di questa analisi normativa, si nota quanto frammentata sia la disciplina a causa dei numerosi interventi riformatori che gradualmente hanno modificato il quadro normativo in linea con i principi e le finalità dello Stato. Questo conduce a un problema da risolvere al fine di individuare in modo corretto la disciplina da applicare alla fattispecie concreta tra le varie leggi spesso in conflitto tra loro.

³⁰ Oliviero, Mazza. *Le Nuove Intercettazioni*. G Giappichelli Editore, 2018, p.126.

³¹ Silvia, Signorato. *Op. cit.*, pp. 246-247.

2. L'IMPATTO DELLE INTERCETTAZIONI SUL DIRITTO ALLA *PRIVACY*

2.1. L'EVOLUZIONE DEL DIRITTO ALLA *PRIVACY*

Il rapporto tra diritto penale e *privacy* risulta essere molto complesso, in quanto quest'ultima è un concetto relativamente recente e, soprattutto, costituito da componenti assai complesse e frammentate a causa dello sviluppo della tecnologia: la riservatezza e la vita privata. Recente è anche il tentativo di ancorare al concetto di *privacy* un interesse giuridico suscettibile di tutela penale, in quanto sono rilevanti le tensioni che sussistono tra questo nuovo diritto e la materia penale: è difficile plasmare quest'ultima su questo nuovo diritto sempre in evoluzione che si sta spostando sempre più verso la protezione dei dati personali. Di conseguenza, è di fondamentale importanza, prima di tutto, comprendere l'evoluzione concettuale e storica del diritto alla *privacy* per poi analizzarne l'ambito di applicazione.

Il diritto alla *privacy* si è affermato nel XIX secolo, nonostante la necessità di una tale protezione fosse comunque radicata sin dall'antichità: si pensi che nel mondo greco, spazio pubblico (*polis*) e dimensione privata (*oikos*) erano considerati necessariamente distinti.

Tuttavia, l'esistenza di un diritto autonomo ha faticato ad affermarsi. Infatti, per lungo tempo esso veniva considerato come una declinazione del diritto di proprietà. L'evoluzione del diritto alla *privacy* è emersa quando l'uomo ha iniziato a considerarsi individuo singolo e indipendente dalla sfera pubblica, cominciando a percepire la necessità di vedere protetta la sua vita personale dalle ingerenze pubbliche³².

Il diritto alla *privacy* è stato riconosciuto, in primo luogo, nei Paesi di *common law*, dove la proprietà era considerata un diritto inviolabile. In particolare, nel saggio «*The Right to Privacy*» dell'anno 1890, Samuel D. Warren e Louis D. Brandeis hanno modellato il

³² Silvia, Signorato. *Le Indagini Digitali. Profili Strutturali Di Una Metamorfosi Investigativa*. G. Giappichelli Editore, 2018, p.73.

concetto di *privacy*, che viene inteso come diritto ad essere lasciati soli. In questo articolo veniva contestata l'ingerenza della stampa nella vita privata al fine di creare scandalo: la famiglia di Warren apparteneva all'alta borghesia ed era solita intrattenere costose feste nella propria casa che diventava bersaglio di paparazzi. La denuncia deriva proprio dalla violazione della proprietà, luogo in cui neanche le autorità pubbliche possono accedere senza un legittimo motivo, come un ragionevole sospetto basato sulla legge.

Questa è la ragione per cui inizialmente la *privacy* acquisisce una nozione negativa, indicativa di un diritto a non subire interferenze altrui privando gli altri della conoscenza di sé³³.

In Italia il termine giuridico *privacy* è stato introdotto nel 1970 dall'art. 8 dello Statuto dei lavoratori, il quale vieta "al datore di lavoro di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore"³⁴. La ricerca dei tratti fondamentali di tale diritto ha condotto all'elaborazione della nozione di riservatezza coincidente proprio con la *privacy* intesa come diritto di escludere tutti (*ius excludendi alios*) dalla propria sfera privata. Questo concetto è stato enucleato tra i diritti fondamentali dell'uomo come un diritto "ad una vita intima"³⁵.

Lo sviluppo della tecnologia ha fatto conoscere il bisogno di ulteriori tutele che hanno gradualmente fatto abbandonare il significato di *privacy* come diritto ad essere lasciati soli, per ancorarlo al diritto di poter controllare i propri dati e impedirne anche la circolazione. Il motivo di fondo è che le nuove tecnologie permettono di raccogliere ed elaborare un'elevata mole di dati, mettendo questi ultimi a rischio di eventuali perdite (*data losses*) o violazioni di accesso (*data breaches*) da parte di persone non autorizzate. Il baricentro della tutela ora è diventato proprio la consapevolezza dell'utente rispetto alla corretta gestione dei propri dati personali.

³³ Citazione testuale art. 12 della Dichiarazione universale dei diritti dell'uomo; Silvia, Signorato. *Op. cit.*, p.75.

³⁴ Citazione testuale dell'art. 8 Statuto dei lavoratori

³⁵ Antonella, Massaro. *Diritto Penale e Privacy*. Pacini Giuridica, 2020, p. 39.

A questo riguardo, la Carta di Nizza è la fonte che attribuisce alla protezione dei dati personali una valenza autonoma rispetto al diritto alla *privacy*, dividendo queste due dimensioni tra gli artt. 7 e 8.

Un'ulteriore fonte che protegge il diritto alla *privacy* è la Dichiarazione universale dei diritti dell'uomo, la quale all'art. 12 vieta che un individuo sia sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa e nella sua corrispondenza³⁶. Una simile formulazione è rinvenibile nell'art. 17 del Patto internazionale sui diritti civili e politici. Analogamente, l'art. 8 della Convenzione europea dei diritti dell'uomo e delle libertà fondamentali garantisce il diritto al rispetto della vita privata e familiare³⁷, come l'art. 16 del Trattato sul funzionamento dell'Unione europea sancisce il diritto dei cittadini alla protezione dei propri dati di carattere personale.

Nonostante queste previsioni, la Costituzione italiana nulla prevede a riguardo, lasciando la possibilità di ricondurre tale diritto ad un fondamento costituzionale. Dalle varie teorie sviluppatesi nel tempo resta la prassi di ancorare il diritto alla riservatezza all'art. 2 Cost., il quale, però, non offre particolari garanzie. In concreto «riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo, sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale»³⁸. Di conseguenza, per definire i limiti delle attività investigative, sembra necessario fare riferimento all'art. 8 Cedu, previsione più importante in materia di *privacy*. In particolare, tutela la vita privata e familiare di un individuo, il suo domicilio e la sua corrispondenza. Eventuali deroghe devono rispettare il principio di necessità per finalità di giustizia.

In relazione proprio all'art. 8 Cedu, le attività captative svolte durante le intercettazioni integrano di per sé una violazione di questo diritto, secondo quanto specificato dalla Corte europea dei diritti dell'uomo³⁹; di conseguenza, per lo svolgimento di queste attività è necessario rispettare determinate garanzie previste dall'articolo stesso: la compressione del diritto alla *privacy* deve essere prevista da una chiara previsione di legge che

³⁶ Silvia, Signorato. *Op. cit.*, p.76.

³⁷ Silvia, Signorato. *Op. cit.*, p.77.

³⁸ Citazione testuale dell'art. 2 Cost.

³⁹ Oliviero, Mazza. *Le Nuove Intercettazioni*. G Giappichelli Editore, 2018, p. 110.

identifichi le persone intercettate allo scopo di rendere prevedibile per queste ultime l'interferenza nella loro vita privata; inoltre, deve essere necessaria per la soddisfazione delle esigenze indicate nella norma stessa e deve essere proporzionata allo scopo da perseguire⁴⁰. In relazione a quest'ultimo vincolo, la proporzionalità deve essere valutata caso per caso tenendo conto del tipo di atto investigativo, delle sue modalità e del contesto⁴¹. Un profilo critico concerne il primo vincolo, ovvero la previsione di legge come requisito per la compressione del diritto alla *privacy*: il problema si pone nella valutazione dell'ammissibilità degli atti investigativi atipici usati sempre più frequentemente ma non previste dalla legge.

2.2. I LUOGHI TUTELATI DALLA *PRIVACY* A FRONTE DI INDAGINI PENALI

Il passo successivo consiste nell'individuare i luoghi in cui, nel corso di indagini penali, deve operare almeno un'aspettativa di *privacy*. A questo scopo si devono considerare le molteplicità di forme di tutela a cui possono essere ricondotti i luoghi informatici in cui opera specificatamente il diritto alla *privacy*. Con riguardo a quest'ultimo, si possono classificare i luoghi compresi nell'ambito di tutela del diritto al rispetto alla vita privata. La distinzione principale è quella tra dati contenuti in un dispositivo informatico e dati collocati in rete. I primi, in particolare, permettono di concludere che l'accesso ad un dispositivo digitale corrisponde autonomamente ad una violazione di domicilio digitale, a meno che questo sia un dispositivo di più soggetti e non sia di destinazione di attività private della vita domestica o lavorativa⁴². Questo implica che le attività investigative svolte in un dispositivo informatico, come le intercettazioni, debbano rispettare le garanzie a presidio del domicilio digitale. Inoltre, la tutela della *privacy* viene unita a quella del domicilio nel caso in cui tali dati siano riservati.

⁴⁰ Silvia, Signorato. *Op. cit.*, p.78.

⁴¹ Silvia, Signorato. *Op. cit.*, p.79.

⁴² Silvia, Signorato. *Op. cit.*, p.80.

Più articolato è il caso in cui i dati siano immessi in rete, dove i luoghi digitali non rientrano nella tutela *ex art. 14 Cost.* secondo cui «Il domicilio è inviolabile. Non vi si possono eseguire ispezioni o perquisizioni o sequestri, se non nei casi e modi stabiliti dalla legge secondo le garanzie prescritte per la tutela della libertà personale»⁴³. Per accertare che i luoghi in rete possano essere protetti dalla *privacy*, bisogna valutare il carattere riservato dello spazio in cui l'informazione risiede e non dell'informazione stessa⁴⁴. Questo deriva dal fatto che un dato può essere riservato e, allo stesso tempo, essere disponibile in un luogo accessibile da chiunque: in questo caso la tutela della *privacy* non trova applicazione. Al contrario, le indagini penali devono garantire la tutela di quest'ultima nel caso in cui le informazioni non siano riservate ma siano accessibili solo in un luogo con carattere meritevole di tutela del diritto alla riservatezza.

Riguardo all'individuazione dei luoghi in cui la *privacy* deve essere tutelata, opera l'ulteriore distinzione che proietta i luoghi fisici ai luoghi virtuali della rete. Si considerano luoghi pubblici gli spazi in cui si accede senza previa registrazione: le informazioni, comprese quelle personali, contenute in questa categoria di luoghi potranno essere acquisite durante le indagini senza limiti e senza precedenti autorizzazioni giurisdizionali⁴⁵. Successivamente si possono individuare i luoghi aperti al pubblico, i quali nella realtà virtuale sono spazi in cui si accede previa identificazione o registrazione: anche in questo caso la tutela alla *privacy* non trova applicazione, vedendo permesse attività investigative senza autorizzazioni. L'unica categoria in cui opera, se non altro, un'aspettativa di *privacy* è quella che comprende i luoghi in cui per accedere è necessaria una doppia accettazione da parte del gestore di quel luogo digitale. In un caso simile, ai fini delle indagini, gli organi investigativi devono ottenere tale accettazione per procedere nelle loro attività senza essere soggetti alle limitazioni poste a tutela della *privacy*, in quanto si considera come nullaosta il consenso di chi gestisce il luogo a vedere violato il proprio spazio.

⁴³ Citazione testuale art. 14 Cost.

⁴⁴ Silvia, Signorato. *Op. cit.*, p.81.

⁴⁵ Silvia, Signorato. *Op. cit.*, p.82.

2.3. I LIVELLI DI TUTELA PREVISTI NEL NOSTRO ORDINAMENTO

Vagliando la garanzia del diritto alla riservatezza durante l'attività investigativa svolta in particolare tramite le intercettazioni, si possono individuare tre livelli di tutela. Il primo è riservato al Presidente della Repubblica, per il quale la Corte costituzionale prevede l'inutilizzabilità del materiale intercettato. Questa immunità viene fatta derivare dall'art. 20 Cost., il quale però prevede una deroga specificatamente per i casi di alto tradimento e di attentato alla Costituzione, reati per cui è prevista l'intercettazione solo dopo la sospensione del Capo dello Stato dalla sua carica⁴⁶.

A questo livello se ne aggiunge un secondo previsto per i parlamentari, i quali godono anch'essi di una tutela rafforzata ma parziale che viene condotta all'art. 68 co. 3 Cost., il quale prevede la necessità di un'autorizzazione della Camera di appartenenza del parlamentare intercettato. Fermo restando l'obbligo di quest'ultima nei casi in cui le conversazioni intercettate contengano una notizia di reato riguardante il parlamentare, tale previsione non opera quando nell'attività investigativa si utilizzano conversazioni di soggetti terzi che coinvolgono anche i parlamentari.

L'ultimo livello spetta ai cittadini normali a cui deve essere garantito il rispetto dei diritti inviolabili previsti dalla Costituzione in particolare dall'art. 15, secondo il quale ogni limitazione al diritto alla libertà e alla segretezza della corrispondenza e di ogni altra forma di comunicazione debba essere limitata solo attraverso un atto motivato da parte dell'autorità giudiziaria. Altro diritto inviolabile garantito è previsto dall'art. 8 Cedu, previsione già citata nel primo paragrafo di questo capitolo. Disposizioni ulteriori richiedono che siano determinati i requisiti e l'ammissibilità delle intercettazioni (artt. 266 e 267 c.p.p.), le quali devono essere autorizzate con decreto motivato quando queste siano indispensabili per le indagini⁴⁷.

⁴⁶ Alfredo, Gaito. *Diritto Alla Riservatezza e Intercettazioni: Un Bilanciamento è Possibile?* Seminario; diritto alla riservatezza e intercettazioni, Facoltà di Giurisprudenza Sapienza Università di Roma, Anno accademico 2012–2013, p. 20.

⁴⁷ Alfredo, Gaito. *Op. cit.*, p. 21.

Un discorso a sé stante concerne l'avvocato difensore, i suoi ausiliari e i suoi assistiti: per questi soggetti si tende ad applicare l'art. 103 co. 5 c.p.p., il quale prevede una tutela assoluta della riservatezza per cui le intercettazioni di dialoghi riguardanti l'attività difensiva sono vietate.

Nella realtà queste disposizioni paiono spesso di difficile applicazione, per cui si rende fondamentale se non altro un bilanciamento tra gli interessi di tutti i soggetti.

2.4. L'ESPERIENZA TEDESCA COME CASO PARADIGMATICO DI PROTEZIONE RAFFORZATA DELLA *PRIVACY*

Di particolare rilievo in materia di protezione rafforzata della *privacy* in relazione all'uso di forme investigative altamente tecnologiche ma lesive dei diritti fondamentali dell'individuo si pone l'esperienza tedesca, in quanto la Germania è il primo Paese in Europa ad aver dubitato della liceità delle forme di captazione mediante strumenti di controllo a distanza⁴⁸, dopo averle lei stessa autorizzate.

La sentenza del 20 aprile 2016 della Corte costituzionale ha affrontato il tema delle intercettazioni svolte con strumenti informatici particolarmente invasivi dal punto di vista della riservatezza, in quanto permettono la captazione di dati da remoto. In particolare, nella sua pronuncia la Corte ha dichiarato l'incostituzionalità di alcune disposizioni della legge federale che non rispettavano il principio di proporzionalità nell'autorizzare queste misure di sorveglianza occulte⁴⁹. Un'importante e precedente sentenza si colloca nel 2008, quando è stato riconosciuto per la prima volta il diritto alla garanzia dell'integrità e della riservatezza dei sistemi informatici. Nello specifico, la Corte è stata chiamata a valutare la legittimità dell'art. 5, co. 2, n. 11 della "Legge sulla protezione della Costituzione del *North Rhein Westfalia*", il quale non poneva sufficienti garanzie a tutela della segretezza delle comunicazioni e dell'inviolabilità del domicilio in violazione del

⁴⁸ Oliviero, Mazza. *Op. cit.*, p. 110.

⁴⁹ Oliviero, Mazza. *Op.cit*, p. 110.

principio di proporzionalità. In concreto, la legge permetteva l'uso di strumenti per intercettare comunicazioni via *Internet*, accedere in modo occulto a qualsiasi sistema informatico collegato in rete e copiare i dati per la loro valutazione. Tale attività invasiva veniva giustificata dalla finalità di lotta contro le attività illegali di particolare gravità⁵⁰. Tuttavia, i ricorrenti di questo caso giudiziario che erano stati sottoposti alle intercettazioni non erano soggetti ad indagini penali, di conseguenza il trattamento era assolutamente ingiustificato.

A seguito della pronuncia è stato riconosciuto per la prima volta il diritto alla garanzia dell'integrità e della riservatezza dei sistemi informatici, inteso come «protezione dei titolari dall'accesso statale a dispositivi tecnologici di informazione nel loro complesso»⁵¹. A guidare questa impostazione è l'aspettativa di riservatezza in capo ad ogni utente anche sui propri dati e l'esigenza di un'analogia tutela di riservatezza del domicilio informatico rispetto a quello ordinario, in quanto anche il primo è inteso come luogo in cui il singolo sviluppa la propria personalità.

Pertanto, la Corte, nella sua pronuncia, ha posto l'attenzione sulla necessità di effettuare un bilanciamento trovando un punto di equilibrio tra il ricorso alle forme tecnologiche di intercettazioni che seguono la necessità di rilevare forme di criminalità e la tutela dei diritti inviolabili dell'uomo.

⁵⁰ Francesca, Besemer. *Un Nuovo Diritto Costituzionale in Germania? Quale Status per Il "Diritto Alla Riservatezza Ed Integrità Dei Sistemi Tecnologici d'informazione"?* 25 Nov. 2010, <https://www.diritticomparati.it/nuovo-diritto-costituzionale-in-germania-diritto-alla-riservatezza-ed-integrita-dei-sistemi-tecnologici-dinformazione-1/>.

⁵¹ Oliviero, Mazza. *Op.cit*, p. 111.

2.5. LA FASE DI STRALCIO DELLE CONVERSAZIONI INTERCETTATE A PROTEZIONE DELLA RISERVATEZZA SECONDO LA DELEGA IN MATERIA DI INTERCETTAZIONI

La riforma Orlando contiene una legge-delega in materia di intercettazioni dove il Parlamento ha delineato criteri per una maggiore tutela della riservatezza in linea con le linee-guida adottate dalle principali Procure della Repubblica⁵². Fermo restando i criteri e i limiti di utilizzabilità tuttora vigenti, l'intervento tenta di operare soprattutto sul problema di partenza delle conversazioni inutilizzabili o irrilevanti. In concreto, è prevista in capo al pubblico ministero una prima valutazione e selezione delle conversazioni intercettate che siano utili e utilizzabili. Per di più, si delinea una fase successiva di stralcio delle intercettazioni inutilizzabili o irrilevanti anche in fase di contraddittorio⁵³. Sostanzialmente, la delega prevede l'obbligo di redazione dei c.d. brogliacci che fungono da prima selezione delle conversazioni che possono diventare inutilizzabili. Per comprendere meglio, questi ultimi contengono il riepilogo delle conversazioni intercettate nel corso del procedimento. Questo filtro diventa indispensabile a tutela della *privacy* dei soggetti sottoposti ad indagine. In particolare, permette che solo le conversazioni rilevanti vengano riportate e quindi utilizzate, ovvero che vengano poi pubblicate o riprodotte nei provvedimenti del giudice⁵⁴, i cui atti non sono coperti dal segreto investigativo e dal divieto di pubblicazione, come al contrario è previsto per gli atti del pubblico ministero e della polizia giudiziaria. In sintesi, le conversazioni che non possono essere riportate sono quelle che presentano le seguenti caratteristiche: contengono dati sensibili, non sono pertinenti all'accertamento della responsabilità di quel determinato reato, non sono rilevanti in quanto contengono fatti estranei⁵⁵. Questo potere di valutazione e selezione spetta di norma al pubblico ministero, ma la prassi dimostra che ci sia un dialogo tra il primo e la polizia giudiziaria, la quale finisce per

⁵² Carlotta, Conti. *La Riservatezza Delle Intercettazioni Nella "Delega Orlando."* Vol. Diritto penale contemporaneo, rivista trimestrale, Nov. 2017, p. 79.

⁵³ Carlotta, Conti. *Op. cit.*, p. 79.

⁵⁴ Carlotta, Conti. *Op. cit.*, p. 80.

⁵⁵ Carlotta, Conti. *Op. cit.*, p. 81.

gestisce tale operazione che può risultare, di conseguenza, inadeguata, incompleta e fraintendibile.

Un altro rilievo spinoso è l'ampiezza dei concetti di pertinenza e rilevanza e la discrezionalità che offre la loro valutazione; la soluzione pare essere quella di usare criteri meramente oggettivi stando ad un approccio tecnico, il quale prevede *in primis* la valutazione di pertinenza al fine di giudicare un dato come irrilevante. Dunque, «un dato può essere irrilevante ogniqualvolta, ancorché pertinente rispetto ad un tema, risulti inidoneo a portare un'informazione utile; pertanto, le intercettazioni che riguardano fatti o circostanze estranei alle indagini appaiono “non pertinenti” prima e piuttosto che irrilevanti»⁵⁶.

Un altro profilo controverso riguarda se la selezione debba comprendere intere conversazioni o solo parti di esse, considerando, però, che estrapolare parti dell'intera conversazione risulta di difficile messa in pratica.

Inoltre, la legge-delega nulla dice sulla possibilità di ripescare conversazioni precedentemente escluse nella fase di stralcio. Il caso può verificarsi quando la rilevanza emerga successivamente, ad esempio quando è la stessa difesa a prendere l'iniziativa di ripescare conversazioni. Tuttavia, questo può essere impedito dal fatto che nel brogliaccio le conversazioni escluse sono identificate solo da alcuni elementi: la data, l'ora e l'apparato trasmittente. Il tutto rende estremamente difficile per la difesa comprendere quali possano essere le conversazioni che assumono rilevanza. L'unica soluzione che si prospetta, ma che sembra a dir poco infattibile, consiste nell'ascoltare interamente le conversazioni indicate solo da quei pochi elementi identificativi⁵⁷.

Il Consiglio Superiore della Magistratura, dal canto suo, ha proposto di inserire nei brogliacci perlomeno l'indicazione di dati aggiuntivi come l'identità dei conversanti, l'orario e l'oggetto del colloquio, in modo tale da dare la possibilità alla difesa di cogliere subito le conversazioni per lei rilevanti senza procedere ad un ascolto integrale. Questo permette di tutelare il diritto alla prova, anche se bisogna tener conto che il rischio di diffusione all'esterno, in tal modo, non viene scongiurato. Un altro diritto che viene

⁵⁶ Citazione testuale di C. Conti. *Op. cit.*, p. 83.

⁵⁷ Carlotta, Conti. *Op. cit.*, p. 84.

esposto a rischio dal solo fatto di conoscere i soggetti della conversazione e l'oggetto è proprio il diritto alla riservatezza⁵⁸.

A seguito di questa analisi si nota che l'obiettivo di tutelare la riservatezza in questa legge-delega presenta molte complessità a causa dell'ampiezza dei termini utilizzati dalle linee-guida e dalla conseguente discrezionalità nelle mani dei soggetti inquirenti. D'altro canto, si considera comunque un punto di partenza al fine di selezionare alla base delle indagini le conversazioni e i dati che, oltre ad essere irrilevanti e non pertinenti, possono anche ledere il diritto alla riservatezza dell'indagato.

⁵⁸ Carlotta, Conti. *Op. cit.*, p. 84.

3. L'IMPATTO DELLE INTERCETTAZIONI SUL DIRITTO ALL'INVIOLABILITÀ DEL DOMICILIO

3.1. UN INQUADRAMENTO DEL DIRITTO ALL'INVIOLABILITÀ DEL DOMICILIO

Per capire l'inquadramento del diritto all'invioabilità del domicilio, sancito dall'art. 14 Cost., si deve tenere in considerazione la sua origine: strumentale ad altri diritti, esso connetteva la protezione della sfera intima all'interno della propria casa con la protezione della proprietà e della sicurezza personale⁵⁹. Costituzionalmente tale connessione si è attenuata portando alla concezione di tale diritto come unico e non strumentale ad altri. D'altro canto, però, esso incorpora molte esigenze, quali la tutela del diritto alla libertà personale, il diritto alla libertà e alla segretezza di ogni forma di comunicazione e il diritto alla riservatezza⁶⁰. Sono proprio gli artt. 8 Cedu e 7 della Carta dei diritti fondamentali dell'Unione europea a confermare l'impostazione secondo la quale si considera il diritto all'invioabilità autonomo. Rispettivamente gli articoli citati sanciscono che «ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza»⁶¹ e «ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni»⁶².

Nonostante questi articoli diano una valenza autonoma a tale diritto, quello che risulta difficile è stabilire a cosa si riferisca il termine domicilio. Il diritto processuale penale non fornisce alcuna definizione, di conseguenza si rende necessario analizzare la Costituzione, la quale all'art. 14 sancisce: «Il domicilio è inviolabile. Non vi si possono eseguire ispezioni o perquisizioni o sequestri, se non nei casi e modi stabiliti dalla legge

⁵⁹ Silvia, Signorato. *Op. cit.*, p.50.

⁶⁰ Silvia, Signorato. *Op. cit.*, p.50.

⁶¹ Citazione testuale art. 8 Cedu

⁶² Citazione testuale art. 7 Carta di Nizza

secondo le garanzie prescritte per la tutela della libertà personale»⁶³. Come si può notare, anche quest'ultimo articolo non riporta alcuna definizione di domicilio. La soluzione a cui si ricorre è valutare se la definizione possa essere costruita sulla base civilistica o penalistica.

Relativamente all'ambito civilistico, fin dalla seconda metà dell'800 (periodo durante il quale era in vigore lo statuto albertino) la dottrina si è occupata a lungo di questa definizione cercando di far coincidere quella costituzionale con la nozione rientrante nell'art. 43 c.c. secondo il quale «il domicilio di una persona è nel luogo in cui essa ha stabilito la sede principale dei suoi affari e interessi»⁶⁴. In tale intento la dottrina ha negato la coincidenza dei due concetti.

Tuttavia, un altro orientamento conduce la nozione *ex art. 14 Cost.* all'ambito penalistico, il quale all'art. 614 c.p. prevede la reclusione per chi viola il domicilio inteso come abitazione, luogo di privata dimora o luogo nelle appartenenze di essi. Di conseguenza, si deduce che nella definizione di abitazione possano rientrare i luoghi in cui una persona svolge la vita domestica e nel termine privata dimora possa rientrarvi la nozione di luogo diverso dall'abitazione ma in cui si svolgono azione tipiche della vita domestica⁶⁵. Un nesso tra i due ambiti, penalistico e costituzionale, deriva dalla collocazione dell'art. 614 c.p. tra i delitti contro la libertà individuale e dell'art. 14 Cost. tra le libertà personali. Tuttavia, tale impostazione può essere confutata dal fatto che fonti collocate in diversi livelli all'interno della gerarchia possono variare gli stessi contenuti in modi altrettanto differenti.

Anche secondo la giurisprudenza le distanze tra gli ambiti penale e costituzionale tendono ad attenuarsi, infatti la stessa Corte costituzionale cerca, nella prassi, di allargare la definizione costituzionalmente orientata nell'ambito penale. Lo stesso fa la Corte europea dei diritti dell'uomo, la quale conduce il diritto all'inviolabilità del domicilio non solo al perimetro degli spazi fisici, ma anche in quello del godimento degli stessi. La Corte arriva addirittura a comprendere in tale diritto anche le sedi sociali, le filiali e altri locali professionali⁶⁶. Fermo restando che all'interpretazione della Corte costituzionale si

⁶³ Citazione testuale dell'art. 14 Cost.

⁶⁴ Citazione testuale dell'art 43 cod. civ.

⁶⁵ Silvia, Signorato. *Op. cit.*, p.52.

⁶⁶ Silvia, Signorato. *Op. cit.*, p.54.

devono attenere anche i giudici nazionali, sarà necessario per tutti procedere ad un'interpretazione altrettanto estensiva della nozione di domicilio, anche se a questo può conseguire l'attenuazione del requisito del carattere riservato delle attività svolte⁶⁷.

In sintesi, non risultando una definizione di domicilio né dalla Costituzione né dal diritto processuale penale, si ricorre all'estensione dell'interpretazione dell'art. 614 c.p.

3.2. L'INDIVIDUAZIONE DEI LUOGHI RIENTRANTI NELLA NOZIONE DI DOMICILIO E I LUOGHI INFORMATICI E DIGITALI

Ciò che bisogna sottolineare è che nell'individuazione dei luoghi che godono della protezione del diritto all'inviolabilità del domicilio, è necessario riconoscere alcune caratteristiche che i luoghi devono presentare in modo congiunto e non alternativo.

Anzitutto, si possono ravvisare tre categorie di luoghi: quelli che non rientrano nella definizione di domicilio non godendo nemmeno della protezione della *privacy*, i luoghi che rientrano solo nell'ambito di tutela della *privacy* e i luoghi che, oltre a godere della protezione della *privacy*, rientrano nell'ambito di tutela dell'inviolabilità del domicilio.

La dottrina ha sottolineato che nessun luogo è domicilio in quanto luogo fisico, ma è tale per il fatto che ha una relazione con la persona⁶⁸.

La prima caratteristica che un luogo in quanto domicilio deve avere è lo *ius includendi*, il quale indica il diritto di poter entrare, rimanere ed uscire da quel luogo. Per precisare, è sufficiente essere titolari di tale diritto, senza esercitarlo in modo effettivo. Inoltre, non è necessario che ci sia la proprietà su quel luogo.

Segue la seconda caratteristica, secondo la quale sul luogo definibile domicilio la persona deve essere titolare anche del diritto di far entrare o di escludere altri soggetti; espressioni che rappresentano rispettivamente tali diritti sono lo *ius admittendi alios* e lo *ius*

⁶⁷ Silvia, Signorato. *Op. cit.*, p.55.

⁶⁸ Silvia, Signorato. *Op. cit.*, p.56.

excludendi alios. Anche in questo caso prescinde dalla titolarità di un diritto di proprietà sul luogo ed è indifferente che la persona sia fisica o giuridica.

L'ultima e la più importante caratteristica che deve essere compresa è che questo luogo sia idoneo per poter svolgere attività tipiche della vita domestica anche provvisoriamente, ovvero attività lavorative.

Un tratto problematico è proiettare queste caratteristiche ai luoghi informatici e digitali, i quali mancano del requisito intrinseco della corporeità: un luogo definito domicilio è dotato di materialità e di confini circoscritti, caratteristiche che non si possono attribuire ad esempio al *Cloud* o alla rete. Tuttavia, un dispositivo informatico si può dire essere materiale e dotato di confini, in quanto all'interno dello spazio occupato dallo stesso sono contenuti dei dati. Di conseguenza, i dispositivi informatici possono rientrare senza perplessità nei luoghi su cui svolgere indagini penali, comprese le intercettazioni.

Più critico è far rientrare nell'alveo di questi luoghi la rete e il *Cloud*, in cui ciò che manca è la fisicità necessaria che si contrappone allo spazio virtuale, e il concetto di confine; infatti, la loro caratteristica principale è la possibilità di ampliare illimitatamente lo spazio dove memorizzare i dati proprio grazie all'assenza di limiti. Alla luce di queste criticità, diventa difficile comprendere questi spazi digitali nella nozione di luogo e, di conseguenza, poter effettuare indagini penali all'interno di essi, avendo notato che forma e materia sembrano essere requisiti inscindibili a ciò che può essere definito luogo.

Al contrario, in settori diversi da quello processuale penale classico sono stati identificati come luoghi anche gli spazi potenzialmente idonei a comprendere qualcosa⁶⁹, senza specificare confini e materia. Tale valutazione, dunque, sembra comprendere anche la rete e il *Cloud*, la cui funzione corrisponde totalmente a quest'ultima considerazione. Di conseguenza, a questi spazi sono applicabili le norme processuali penali e, di conseguenza, sono eseguibili le indagini penali. Oltre a questo, anche le misure cautelari e precautelari potrebbero essere applicate, ad esempio ad un imputato potrebbe essere vietato (ai sensi degli artt. 282-ter e 384-bis c.p.p) di avvicinarsi a determinati luoghi informatici frequentati dalla persona offesa come conseguenza alla prescrizione di allontanamento dalla casa familiare⁷⁰. Il motivo di fondo è che tale prescrizione mira

⁶⁹ Silvia, Signorato. *Op. cit.*, p.59.

⁷⁰ Silvia, Signorato. *Op. cit.*, p.60.

non solo alla protezione dell'incolumità fisica della persona offesa, ma anche a quella psichica, messa a rischio dalla violazione di eventuali spazi virtuali.

Dopo aver compreso che rete e *Cloud* possono rientrare nella nozione di luogo digitale, bisogna capire se i requisiti che un luogo deve avere per rientrare nella nozione di domicilio possono essere proiettati anche ai luoghi digitali, e, di conseguenza, se si possa parlare di domicilio digitale.

Nel nostro ordinamento spesso si è fatto riferimento a tale nozione per fini amministrativi, civili e penali.

Anzitutto, nel contesto amministrativo nell'art. 4 d.l. 18 ottobre 2012, n. 179, si è fatto riferimento ad un indirizzo di posta elettronica certificata definendo quest'ultimo domicilio digitale. La stessa associazione è stata fatta dall'art. 14 d.l. 21 giugno 2013, n. 69. Questa posta elettronica (c.d. pec) è uno spazio che permette di inviare e ricevere *e-mail* che acquisiscono validità giuridica.

Il diritto penale sostanziale, in particolare all'art. 615-ter c.p., punisce in modo specifico chi «si introduce ad un sistema informatico e telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo»⁷¹. In questo caso il domicilio tradizionale a cui si riferisce l'art. 614 c.p. è proiettato proprio in ambito digitale.

Nel diritto processuale penale sembra che la proiezione del domicilio tradizionale su quello digitale sia valido solo se sussistono gli stessi requisiti elencati in precedenza. Riguardo al primo, allo *ius includendi se*, il punto critico è capire se ci debba essere il requisito che tale luogo sia protetto da misure di sicurezza nel momento dell'accesso. Nonostante questo sia previsto in modo chiaro dall'art. 615-ter c.p., si ritiene non sia rilevante il limite descritto, in quanto costituirebbe una disparità di trattamento proteggere solo gli spazi protetti da *password* o da altri sistemi di sicurezza⁷².

Il secondo requisito prevede il diritto di far entrare o di escludere altri soggetti da quel determinato luogo. Per modulare ciò in ambito digitale, bisogna pensare a quanto sia difficile garantire l'inviolabilità del domicilio in questo contesto, in quanto gli spazi

⁷¹ Citazione art. 615-ter c.p.

⁷² Silvia, Signorato. *Op. cit.*, p.63.

virtuali permettono di caricare e scambiare dati senza limiti di tempo e di spazio; di conseguenza, lo stesso godimento del diritto di escludere o includere gli altri dallo spazio risulta difficile da mettere in pratica.

Il terzo e ultimo requisito necessario prevede che in quel determinato luogo le azioni che si compiono debbano essere tipiche della vita domestica o lavorativa. Proiettare questo requisito all'ambito digitale appare troppo restrittivo: si pensi ai *social network* dove le attività sono molteplici e riconducibili a diversi usi e finalità, che non sempre si può dimostrare rientrano tassativamente in ambito domestico o lavorativo. Si ritiene che uno spazio virtuale come questo possa godere di una tutela rafforzata della riservatezza qualora ad esempio, l'utente abbia attivato tutte le protezioni offerte del *social* in ambito *privacy* e il numero di utenti collegati verso tale profilo non sia eccessivamente alto. Nel caso contrario, anche il diritto alla tutela all'inviolabilità del domicilio non trova applicazione.

3.3. L'ART. 14 COST. E LA NECESSITÀ DI UN NUOVO DIRITTO

L'art. 14 Cost. protegge il domicilio in relazione ai soli atti di ispezione, perquisizione e sequestro: ciò che bisogna comprendere è se questo elenco sia tassativo o se possa essere oggetto di interpretazione estensiva in modo da comprendervi anche le intercettazioni effettuate tramite l'installazione di dispositivi all'interno del tradizionale domicilio da parte della polizia giudiziaria. Tuttavia, l'incognita più ampia si pone in relazione allo svolgimento delle intercettazioni informatiche o digitali, dove ad essere violato è il domicilio digitale.

L'elenco stilato nella redazione della Costituzione sembra essere tassativo, in linea con l'obiettivo di tutelare al massimo grado il domicilio riducendo i casi in cui è possibile violarlo. Tale obiettivo trova conferma dal confronto tra l'art. 14 Cost. e l'art. 13 Cost., il quale nel tutelare la libertà personale sancisce che quest'ultima «è inviolabile. Non è ammessa forma alcuna di detenzione, di ispezione o perquisizione personale, né qualsiasi altra restrizione della libertà personale, se non per atto motivato dell'Autorità giudiziaria

e nei soli casi e modi previsti dalla legge»⁷³. L'espressione "qualsiasi altra" permette un'interpretazione ampia, tale da garantire una massima protezione nell'esecuzione di qualsiasi atto. La mancanza di una simile indicazione nell'art. 14 Cost. sembrerebbe escludere le intercettazioni dal suo ambito applicativo.

Tuttavia, la conseguenza più evidente di questa impostazione restrittiva è che la libertà personale diventa un diritto comprimibile da molteplici atti; al contrario, invece, il domicilio vede un catalogo ristretto a pochi atti legittimi che possono invadere tale spazio. Pertanto, la libertà personale può diventare oggetto di numerosi atti autorizzati a violarla: differentemente, il domicilio diventa oggetto di una tutela più rafforzata.

A questa disparità la Corte costituzionale ha cercato di dare una soluzione. In primo luogo, nell'elenco degli atti nominati dall'art. 14 Cost. ha ricompreso anche quelli che esulano dai primi. In secondo luogo, ha definito non tassativo l'elenco previsto dallo stesso articolo. In queste scelte la Corte ha tenuto in considerazione lo sviluppo tecnologico non valutato nella redazione della Costituzione risolvendo così il conseguente vuoto di tutela⁷⁴.

Dopo aver compreso che i luoghi informatici possono essere fatti rientrare nell'ambito di tutela prevista dall'art. 14 Cost., si deve però notare quanto questo sia anche limitativo. Come ben si sa, la vita delle persone è transitata dall'essere tradizionale all'essere digitale; di conseguenza, questa deve essere tutelata da diritti che possano proteggere la vita digitale su più versanti. Questo è il motivo per cui il diritto all'intangibilità del domicilio pare essere limitativo: è necessario che sia protetto non solo tale spazio, ma anche la vita privata, le comunicazioni, la manifestazione del pensiero dove al centro si pone l'individuo. Il nuovo diritto conforme a queste esigenze di tutela potrebbe essere il diritto all'intangibilità della vita digitale, il quale differirebbe dal diritto alla segretezza ed integrità dei sistemi informatici, coniato dalla Corte costituzionale tedesca, in quanto quest'ultimo pone al centro lo strumento informatico. Parimenti, anche il diritto all'autodeterminazione sull'uso dei dati personali esula dal nuovo diritto, avendo il primo la funzione di tutelare i soli dati personali.

⁷³ Citazione testuale art. 13 Cost.

⁷⁴ Sentenza Corte cost. 24 aprile 2002, n. 135

Ecco che questo diritto andrebbe a proteggere tutte le attività che un individuo esegue nel mondo digitale: manifestare i propri pensieri, immettere dati, stringere relazioni. Le libertà tradizionali si proiettano nel mondo digitale e sentono l'esigenza di essere protette anche a fronte di atti investigativi.

CONCLUSIONI

Questo elaborato si è posto l'obiettivo di approfondire il tema del difficile bilanciamento tra l'interesse a reprimere i reati tramite mezzi tecnologici sempre più invasivi e, al contempo, la necessità di tutelare i diritti fondamentali dell'indagato. È stato uno studio delicato e complesso che ha condotto a diverse considerazioni.

A causa dello sviluppo tecnologico, negli ultimi decenni il diritto si sta trovando a dover disciplinare l'uso di strumenti che spesso esulano dalla portata del legislatore. Un tentativo pratico è stato fatto dalla riforma Orlando, la quale si è concentrata principalmente sull'uso del captatore informatico, *software* occulto ed estremamente invasivo dei diritti fondamentali dell'uomo. A partire da questo, si nota che la soluzione adottata dal legislatore consiste nella regolamentazione di tali strumenti intercettativi a seconda delle funzioni, dei settori e delle circostanze in cui vengono utilizzati, fermo restando il rispetto del principio di necessità e di proporzionalità.

Va poi evidenziato come la criminalità abbia preso nuove forme: gli strumenti tecnologici sono il mezzo con cui individui od organizzazioni criminali commettono illeciti grazie ad un uso più consapevole della tecnologia; si pensi alla possibilità di accedere al *Dark Web* che permette di compiere attività *online* protette dall'anonimato. Di conseguenza, diventa necessario che a forme sofisticate di utilizzo della tecnologia per scopi illeciti conseguano forme altrettanto avanzate di atti investigativi, come le intercettazioni tramite mezzi informatici. I metodi tradizionali di intercettazione risultano, infatti, inadeguati: si pensi, ad esempio, quanto difficile sarebbe intercettare e analizzare una comunicazione criptata se non fosse permesso l'uso del *trojan horse*.

Tuttavia, le potenzialità dei mezzi investigativi odierni devono essere limitate da rigidi criteri che delimitino il loro ambito e che garantiscano la tutela dei diritti fondamentali. La trasformazione apportata dal progresso tecnologico sul mondo giuridico, come evidenziato dalla Corte europea e dalla Corte di Cassazione, pone il problema di dover equilibrare l'esigenza di ricorrere a strumenti invasivi al fine dell'accertamento dei reati e la necessità di proteggere al contempo i diritti fondamentali e i valori dell'uomo.

BIBLIOGRAFIA

Conti, Carlotta. *La Riservatezza Delle Intercettazioni Nella "Delega Orlando."* Vol. Diritto penale contemporaneo, rivista trimestrale, Nov. 2017, pp. 79-84.

Gaito, Alfredo. *Diritto Alla Riservatezza e Intercettazioni: Un Bilanciamento è Possibile?* Seminario; diritto alla riservatezza e intercettazioni, Facoltà di Giurisprudenza Sapienza Università di Roma, Anno accademico 2012–2013, pp. 7-9, 20-21.

Giostra, Glauco, e Orlandi, Renzo. *Revisioni Normative in Tema Di Intercettazioni.* G. Giappichelli Editore, 2020, p. 158, p. 258.

Massaro, Antonella. *Diritto Penale e Privacy.* Pacini Giuridica, 2020, p. 39.

Mazza, Oliviero. *Le Nuove Intercettazioni.* G Giappichelli Editore, 2018, pp. 102-111.

Signorato, Silvia. *Le Indagini Digitali. Profili Strutturali Di Una Metamorfosi Investigativa.* G. Giappichelli Editore, 2018, pp. 50-63, 73-82, 240-247, 249-253.

SITOGRAFIA

Besemer, Francesca. *Un Nuovo Diritto Costituzionale in Germania? Quale Status per Il "Diritto Alla Riservatezza Ed Integrità Dei Sistemi Tecnologici d'informazione?*, 25 Nov. 2010, <https://www.diritticomparati.it/nuovo-diritto-costituzionale-in-germania-diritto-alla-riservatezza-ed-integrita-dei-sistemi-tecnologici-dinformazione-1/>. (Consultato il 31 agosto 2023).

Intercettazioni Ambientali: Cosa Sono e Come Funzionano. DOGMA, <https://www.dogma.it/it/news/intercettazioni-ambientali>. (Consultato il 31 agosto 2023).

Intercettazioni Telefoniche. Axerta, 3 Mar. 2019, <https://www.axerta.it/intercettazione-telefonica/>. (Consultato il 31 agosto 2023).

Scarpino, Daniele. *La Disciplina Delle Intercettazioni Telefoniche Ed Ambientali - Rivista Penale Diritto e Procedura.*, Rivista Penale Diritto e Procedura, 20 Gen. 2023, <https://www.penaledp.it/la-disciplina-delle-intercettazioni-telefoniche-ed-ambientali-2/>. (Consultato il 31 agosto 2023).