

## **La lotta al terrorismo e i limiti della violazione della sfera privata individuale: il caso delle intercettazioni abusive di massa.**

**Sommario:** Introduzione. 1. La questione decisa dal Giudice Distrettuale di Detroit. 2. I compiti della National Security Agency e la violazione del FISA (Foreign Intelligence Surveillance Act). 3. L'opposizione del segreto di Stato da parte del NSA. 4. Le violazioni della Costituzione americana 5. La Class Action Tash Hepting v. AT&T 6. Il problema della tutela della riservatezza delle comunicazioni in Europa. 7. La normativa in materia di intercettazioni delle comunicazioni in materia di terrorismo internazionale. 7.1 Le intercettazioni abusive di massa in Italia. 8. Conclusioni: verso la società della sorveglianza?

### **ABSTRACT:**

Il contributo che segue si inserisce nel più vasto dibattito di diritto comparato sulla tutela della riservatezza delle conversazioni telefoniche, telematiche o elettroniche a seguito di una importante decisione della Corte Distrettuale di Detroit sulla legalità del *Terrorism Surveillance Program* attraverso il quale la *National Security Agency* intercettava senza autorizzazioni giudiziarie le conversazioni telefoniche ed elettroniche dei cittadini americani con l'estero. Successivamente, lo sguardo comparatistico si rivolge al contesto europeo in generale ed italiano in particolare, a seguito della nota vicenda delle intercettazioni telefoniche abusive di massa poste in essere da una rete di intelligence parallela senza autorizzazione giudiziaria.

### *Introduzione.*

La decisione che si analizza riguarda uno dei casi più controversi della recente storia americana con molteplici risvolti di diritto costituzionale, separazione tra i poteri dello Stato, tutela della riservatezza e protezione della sicurezza nazionale. Ci si riferisce alla decisione *American Civil Liberties Union v. National Security Service* emanata dal giudice distrettuale di Detroit Anna Diggs Taylor il 17 agosto 2006 sul fenomeno delle intercettazioni abusive di massa. Presupposto della decisione è la *war on terrorism* che gli Stati Uniti d'America hanno mosso contro quella entità terroristica internazionale multilivello conosciuta come Al Qaeda a seguito dei noti tragici attentati dell'11 settembre 2001 che videro alcuni aerei dirottati lanciati contro il *World Trade Center* ed il Pentagono provocando migliaia di morti. L'impatto emotivo provocato da questi avvenimenti sull'opinione pubblica e sulla classe politica americana ha avuto quali conseguenze una serie di profondi mutamenti nell'architettura normativa degli Stati Uniti. Queste si sono concretizzate nella promulgazione di alcuni atti legislativi che hanno modificato l'intero apparato di tutela dei diritti dei cittadini e dei non cittadini residenti negli Stati Uniti<sup>1</sup>. Tra questi i più clamorosi sono stati il *Patriot Act*<sup>2</sup>, la creazione del carcere di Guantánamo

---

<sup>1</sup> K. R. Kusick, *Thwarting Ideological Terrorism: Are We Brave Enough To Maintain Civil Liberties In The Face Of Terrorist Induced Trauma?*, 35 Case W. Res. J. Int'l L. 55, (2003), p. 83; T. Topper Gonzales, *Individual Rights Versus Collective Security: Assessing The Constitutionality Of The Usa Patriot Act*, (2003), p. 75; R. A. Copeland, *War On Terrorism Or War On Constitutional Rights? Blurring The Lines Of Intelligence Gathering In Post-September 11 America*, 35 Tex. Tech L. Rev. 1, (2004), p. 1; G. Hafner, *The Definition of the Crime of Terrorism*, in AA. VV., *International Cooperation in Counter-Terrorism*, (eds. G. Nasi), Aldershot – Burlington, 2006, p. 33.

<sup>2</sup> Il nome esteso di questo provvedimento emanato dal legislatore americano sette settimane dopo gli attentati dell'11 settembre 2001 è *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (Patriot Act). Dottrina e giurisprudenza statunitensi ed europee hanno molto dibattuto sulla natura e costituzionalità di queste norme così invasive nel quadro dei diritti personali, sia dei cittadini americani, sia da parte di coloro che pur non essendo cittadini sono legalmente residenti negli USA. Tuttavia va sottolineato il momento emotivo della promulgazione di questa normativa: sembrava che tutti i cittadini fossero concordi nel rinunciare ad alcune loro libertà e tutele in cambio di maggiore sicurezza. Per la ricostruzione di questo percorso sia sociale sia legislativo, B. A. Howell, *Seven Weeks: The Making Of The Usa Patriot Act*, in 72 *Geo. Wash. L. Rev.* 1145 (2004). In seguito, è stato elaborato un nuovo provvedimento legislativo noto come "Patriot Act II", di notevole invasività in diversi aspetti della vita privata di qualsiasi cittadino americano. Al di là delle peculiarità legate all'entrata in vigore della prima legge e alla volontà governativa di mantenere il più possibile segreta la seconda si sottolinea come le modifiche da esse apportate alle norme precedenti siano sostanziali: è stata radicalmente mutata la disciplina delle

Bay<sup>3</sup> e il dibattito su di esso di fronte alla Corte Suprema degli Stati Uniti<sup>4</sup>, nonché il contenzioso tra Stati Uniti ed Unione Europea per quanto concerne la disponibilità a favore delle autorità pubbliche nordamericane dei dati personali dei passeggeri che effettuano voli transatlantici<sup>5</sup>.

*1. La questione decisa dal Giudice Distrettuale di Detroit: il fenomeno delle intercettazioni abusive di massa.*

Oltre alle citate attività contro il terrorismo rese pubbliche, vi sono state anche altre strategie occulte poste in essere dall'esecutivo senza la conoscenza da parte dell'opinione pubblica ovvero del nulla osta dell'autorità giudiziaria o del potere legislativo. Tra queste la più eclatante di cui si è avuta notizia è l'attività di intercettazione elettronica da parte della *National Security Agency* di centinaia di migliaia di telefonate e di e-mail di cittadini statunitensi senza il nulla osta dell'autorità giudiziaria, ma con la sola autorizzazione del Presidente degli Stati Uniti<sup>6</sup>. A darne la notizia fu il *New York Times* nel dicembre 2005<sup>7</sup>. Dopo che il fatto divenne pubblico, l'*ACLU (American Civil Liberties Union)* intraprese

---

comunicazioni personali, le quali divengono di dominio pubblico, il Governo e la polizia federale possono ottenere informazioni riguardanti la stretta personalità di ogni individuo ed il Governo può porre in stato di detenzione sospetti terroristi (M. Bellazzi, *I "Patriot Acts" e la limitazione dei diritti costituzionali negli Stati Uniti*, in *Politica del diritto*, 2004, p. 681; A. Uyeda, *The Usa Patriot Act May Infringe On Civil Liberties In Cyberspace*, 2002 *UCLA J. L. & Tech. Notes* 1; J. B. Perrine, *The Usa Patriot Act: Big Brother Or Business As Usual?*, 19 *Notre Dame J.L. Ethics & Pub. Pol'y* 163, (2005); J. M. Hannigan, *Playing Patriot Games: National Security Challenges Civil Liberties*, 41 *Hous. L. Rev.* 1371, (2004).

<sup>3</sup> D. M. Amann, *Guantánamo*, 42 *Colum. J. Transnat'l L.* 263, (2004); M. A. Drumbl, *Victimhood In Our Neighborhood: Terrorist Crime, Taliban Guilt, And The Asymmetries Of The International Legal Order*, 81 *N.C. L. Rev.* 1, (2002); T. Huckert, *The Undetermined Fate Of The Guantanamo Bay Detainees' Habeas Corpus Petitions*, 9 *Gonz. J. Int'l L.* 236, (2006); D. Cassell, *Defending Human Rights In The "War" Against Terror*, 4 *Regent J. Int'l L.* 223 (2006); T. D. Gill, E. van Sliedregt, *Guantánamo Bay: a Reflection on the Legal Status and Rights of "Unlawful Enemy Combatants"*, in *Security and Civil Liberties: the Case of Terrorism*, (eds. A. M. Hol, J. A. E. Vervaele), 2005, Antwerpen – Oxford, p. 1. In lingua italiana, T. E. Frosini, *Lo Stato di diritto si è fermato a Guantánamo, Diritto Pubblico Comparato ed Europeo*, 2005; p. 1645 Id., *C'è un giudice (anche) a Guantánamo, Diritto Pubblico Comparato ed Europeo*, 2006, n. 3 p. XXI.

<sup>4</sup> *Rasul v. Bush* (03-334) 542 U.S. 466 (2004); *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004); *Rumsfeld v. Padilla*, 542 U.S. 426 (2004). Per il riassunto ed il commento delle decisioni della Corte Suprema si vedano, tra gli altri, T. D. Gill, E. van Sliedregt, *Op. cit.*, p. 18.

<sup>5</sup> A partire dal 5 marzo 2003, le autorità statunitensi esigono dai vettori che operano voli da, per, o attraverso gli Stati Uniti di fornire all'Ufficio delle dogane e della protezione delle frontiere, *United States Bureau of Customs and Border Protection (CBP)* l'accesso elettronico ai dati dei passeggeri per motivi di sicurezza e di protezione del loro territorio. A carico dei vettori che non dovessero adempiere a tali richieste le sanzioni previste dalle autorità americane prevedono addirittura la perdita del diritto di atterraggio negli *States*. Il lungo contenzioso che ha visto contrapposte Unione Europea e Stati Uniti d'America sul punto si è (per il momento) concluso con la *Decisione 2006/729/PESC/GAI del Consiglio del 16 ottobre 2006 relativa alla firma, a nome dell'Unione europea, dell'accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e sul trasferimento dei dati del codice di prenotazione (Passenger Name Record, PNR) da parte dei vettori aerei al dipartimento della Sicurezza interna degli Stati Uniti*". L'attuazione dell'accordo, firmato con riserva della sua conclusione, è riveduta congiuntamente e su base periodica e ha una scadenza fissata al 31 luglio 2007, salvo proroga mediante consenso scritto di entrambe le parti. In dottrina, S. Rodotà, *Il diritto e i diritti nell'epoca dello "scontro di civiltà"*, in *Questione Giustizia*, 2005, p. 726.

<sup>6</sup> Secondo la lettera di denuncia dei giuristi americani al congresso il "NSA program involves "electronic surveillance," which is defined in FISA to mean the interception of the contents of telephone, wire, or email communications that occur, at least in part, in the United States. 50 U.S.C. §§ 1801(f)(1)-(2), 1801(n). NSA engages in such surveillance without judicial approval, and apparently without the substantive showings that FISA requires"( AA.VV., *January 9, 2006 Letter From Scholars And Former Government Officials To Congressional Leadership In Response To Justice Department Letter Of December 22, 2005*, 81 *Ind. L.J.* 1364, (2006), p. 1364).

<sup>7</sup> J. Risen, E. Lichtblau, *Bush Secretly Lifted Some Limits on Spying in U.S. After 9/11, Officials Say*, *New York Times*, 15<sup>th</sup> December 2005

due azioni legali. La prima causa a nome dei professionisti (avvocati, giornalisti e docenti) intercettati nei confronti della NSA (*National Security Agency*) per aver abusivamente intercettato le loro comunicazioni personali e professionali. La seconda causa contro la compagnie telefoniche che, partecipando al programma, hanno violato i diritti costituzionali dei cittadini e gli obblighi contrattuali verso i clienti. La decisione del giudice distrettuale di Detroit, Anna Diggs Taylor, si riferisce alla prima delle due cause.

Le domande dei ricorrenti riguardano la cessazione immediata di tale attività illegalmente autorizzata dal Presidente Bush e confermata per almeno altre trenta volte dal 2002 al momento in cui la notizia venne di dominio pubblico. Le allegazioni dei ricorrenti asseriscono che il "*Terrorist Surveillance Program*" (TSP) viola i loro diritti di libertà di manifestazione del pensiero e di associazione garantiti dal Primo Emendamento della Costituzione degli Stati Uniti, nonché il loro diritto alla riservatezza previsto dal Quarto Emendamento. Viene altresì lamentata la violazione del principio della separazione dei poteri in quanto il TSP è stato autorizzato dal Presidente in eccesso dei suoi poteri esecutivi, i quali sono regolati dall'Articolo II della medesima Costituzione. Tale eccesso ha specificamente violato la sovranità normativa e decisionale del Parlamento in materia di intercettazioni perché il provvedimento è stato emanato senza l'osservanza di nessuna delle procedure di garanzia richieste dalla Costituzione e dalla legge.

La resistente NSA, e le intervenute autorità governative federali, oppongono in causa il segreto di Stato (*State secrets privilege*) affermando di non poter rendere conto di fronte al giudice le specifiche ragioni che hanno dato origine al programma segreto di intercettazioni, in caso contrario sarebbe messa in grave pericolo la sicurezza nazionale.

Nelle motivazioni del provvedimento il giudice distrettuale sottolinea con molta veemenza come le libertà fondamentali garantite dal *Bill of Rights* siano le prime vittime a soffrire dello sbilanciamento dell'equilibrio tra i poteri dello Stato.

## 2. La violazione del Foreign Intelligence Surveillance Act (FISA) e i compiti della National Security Agency (NSA)

Scoperta l'esistenza del programma illegale di intercettazioni, l'amministrazione di Washington ha difeso il proprio operato in modo molto aggressivo<sup>8</sup>, mentre l'opinione pubblica qualificata<sup>9</sup> si è impegnata a verificare esattamente quali garanzie dei cittadini siano state infrante dall'operato della NSA, soprattutto in relazione al *Foreign Intelligence Surveillance Act (FISA)* e agli Emendamenti Quarto e Primo della Costituzione.

Il FISA è una legge firmata nel 1978<sup>10</sup>, la quale delinea la struttura legale che governa la sorveglianza elettronica all'interno degli Stati Uniti<sup>11</sup>. Essa proibisce il controllo e la

---

<sup>8</sup> Per il General Attorney Alberto Gonzales è stato il Congresso stesso ad autorizzare il Presidente ad "*use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the 9/11 attacks*". Ciò sulla base della *Authorization for Use of Military Force*, Pub. L. No. 107-40, §2(a), 115 Stat. 224, 224 (2001). Il General Attorney sostiene quindi che in occasione delle reiterate autorizzazioni al Terrorist Surveillance Program, il Presidente "stesse agendo allo zenith dei suoi poteri" (L. K. Donohue, *Anglo-American Privacy And Surveillance*, in 96 J. Crim. L. & Criminology 1059 (2006), p. 1061).

<sup>9</sup> AA.VV., *January 9, 2006 Letter From Scholars*, cit., p. 1364; D. Cole, M. S. Lederman, *The National Security Agency's Domestic Spying Program: Framing The Debate*, 81 Ind. L.J. 1355, (2006), p. 1357; J. C. Sims, *What Nsa Is Doing... And Why It's Illegal*, 33 Hastings Const. L.Q. 105, (2006), p. 107.

<sup>10</sup> 50 U.S.C. 1801. L. K. Donohue, *Op. cit.*, p. 1058; K. Wong, *The NSA Terrorist Program*, 43 Harv. J. on Legis. 517, (2006), p. 518; A. Burton, *Fixing Fisa For Long War: Regulating Warrantless Surveillance In The Age Of Terrorism*, 4 Pierce L. Rev. 381, (2006), p. 389.

<sup>11</sup> T. W. Morrison, *Constitutional Avoidance In The Executive Branch*, 106 Colum. L. Rev. 1189, (2006), p. 1251.

sorveglianza dei cittadini americani<sup>12</sup> da parte del potere esecutivo<sup>13</sup>, mentre impedisce la raccolta di informazioni da parte dei servizi di *intelligence* stranieri<sup>14</sup> negli Stati Uniti onde prevenire minacce alla sicurezza nazionale<sup>15</sup>.

La sezione 215 del *Patriot Act* modifica alcune disposizioni del FISA<sup>16</sup>, ed autorizza l'accesso a registrazioni e l'acquisizione di oggetti da parte del governo presso coloro che ne sono custodi, comprese istituzioni educative o finanziarie, Internet Service Providers ovvero biblioteche, tuttavia previo provvedimento giurisdizionale<sup>17</sup>. In questo senso, il *Terrorist Surveillance Program*, autorizzato dal Presidente e realizzato dalla *National Service Agency*, va oltre e contravviene il FISA sotto un duplice aspetto. Da un lato viola la proibizione di controllo delle comunicazioni elettroniche dei cittadini americani. Dall'altro per ciò che si riferisce alle procedure e alle modalità con le quali ciascun atto di sorveglianza può essere legittimamente posto in essere.

Per quanto concerne il primo aspetto, va osservato che molti degli attori sospettano di essere stati intercettati nelle loro conversazioni private e professionali. In conseguenza di ciò avrebbero subito danni irreparabili relativi all'esercizio dei diritti:

- a) di difesa tra cliente e avvocato, con la violazione dell'indispensabile confidenzialità delle conversazioni tra difensore ed assistito ed a scapito di un effettivo di difesa ed una efficace rappresentanza in giudizio delle ragioni dell'imputato;
- b) di cronaca tra il giornalista e le sue fonti, specie quando queste si trovano in aree delicate del mondo, quali Medio Oriente, Asia e Africa;
- c) di libertà della ricerca scientifica e di conseguenza della manifestazione del pensiero, quando le materie di studio concernevano, ancora, argomenti interenti al Medio Oriente, Asia e Africa.

Per quanto riguarda il secondo aspetto va sottolineato che l'azione presidenziale è stata attuata senza il rispetto minimo delle garanzie costituzionali o legislative a favore dei cittadini, ovvero senza autorizzazioni giurisdizionali o legislative né preventive né successive<sup>18</sup>. Tra le garanzie legislative previste a favore dei cittadini, violate dal TSP, il FISA istituisce la *Foreign Intelligence Surveillance Court* (FISC) al fine di supervisionare la legittimità e l'attinenza ai requisiti previsti dalla legge delle richieste in tema di sorveglianza domestica<sup>19</sup>.

---

<sup>12</sup> Ai sensi del 50 U.S.C. § 1801 (h)(4)(i) la locuzione "United States person" indica un cittadino degli Stati Uniti, uno straniero legittimamente e permanentemente residente negli Stati Uniti, una associazione non riconosciuta che conti tra i suoi membri cittadini statunitensi ovvero non cittadini ma legittimamente permanentemente residenti negli stati uniti, ovvero una società che sia registrata negli Stati Uniti e che non rappresenti un potere straniero.

<sup>13</sup> L. K. Donohue, *Op. cit.*, p. 1059.

<sup>14</sup> Secondo la definizione prevista dal 50 U.S.C. § 1801(a)(4) un agente di un potere straniero è chiunque non sia cittadino americano, e che ponga in essere attività di raccolta di informazioni per fini di sabotaggio o attività terroristiche o preparatorie di atti terroristici su incarico di poteri stranieri. Sempre ai sensi del § 1801(b)(2)(C) si definisce "terrorismo internazionale" l'attività che incorpora tre elementi: a) che si tratti di atti pericolosi per la vita umana e in violazione della legge penale; b) abbiano lo scopo di influenzare la politica governativa ovvero intimidire o coercire la popolazione civile; c) si tratti di atti che, nel caso avvengano al di fuori degli Stati Uniti o dei confini nazionali appaiano indirizzati all'intimidazione o alla coercizione dell'autorità locale o nell'ottenimento del diritto di asilo.

<sup>15</sup> D. Cole, M. S. Lederman, *Op. loc. cit.*; L. K. Donohue, *Op. cit.*, p. 1094.

<sup>16</sup> Il § 215 del Patriot Act è rubricato *Access to Records and Other Items Under the Foreign Intelligence Surveillance Act*

<sup>17</sup> S. N. Herman, *The Usa Patriot Act And The Submajoritarian Fourth Amendment*, 41 Harv. C.R.-C.L. L. Rev. 67, (2006), p. 75.

<sup>18</sup> K. Wong, *Op. cit.*, p. 520.

<sup>19</sup> Ai sensi del 50 U.S.C. § 1803 il NSA può condurre indagini di sorveglianza domestica fino ad una durata di settanta due ore senza autorizzazione di un giudice o se l'Attorney General dichiara che si tratta di

Al contrario di quanto previsto dalla legge, va evidenziata l'assoluta segretezza del programma di controllo, del quale il Presidente ha reiterato l'autorizzazione per almeno trenta volte dall'ottobre 2002 e con l'intenzione di rinnovarlo astrattamente all'infinito<sup>20</sup>.

### 2.1 L'opposizione del segreto di Stato da parte del NSA

Prevedibilmente la guerra al terrorismo ha contribuito ad incrementare una già consistente giurisprudenza in tema di opposizione di segreto di stato<sup>21</sup> da parte dell'amministrazione statunitense<sup>22</sup>. In questo specifico caso, è stato eccepito il segreto di stato onde impedire alla giustizia ordinaria di verificare in una pubblica *disclosure* le reiterate violazioni della riservatezza dei cittadini statunitensi. Le ragioni addotte riguardano soprattutto la fase processuale della *discovery*, la quale avrebbe reso note l'identità degli individui ovvero delle organizzazioni sottoposte ad intercettazioni, il contenuto delle comunicazioni acquisite dal NSA e avrebbe permesso la divulgazione dei metodi e delle tecniche utilizzate nelle operazioni di intercettazione.

La Corte distrettuale di Detroit ha accolto in parte le difese dei resistenti. Più volte pubblicamente la Presidenza degli Stati Uniti ha ripetuto che vi sono solide basi legali per l'accoglimento pieno del segreto di Stato sull'operato del NSA<sup>23</sup>. Invece, la Corte afferma che è possibile valutare la legittimità del programma di intercettazioni senza entrare nello specifico delle informazioni raccolte<sup>24</sup>. Seppure il contenuto delle conversazioni è protetto dal segreto di Stato, ciò non influenza l'indagine sulla illegalità del programma del NSA relativo alle intercettazioni delle comunicazioni tra cittadini americani e stranieri nel suo complesso.

### 3. Le violazioni della Costituzione americana

Alla *National Security Agency* sono state contestate anche gravi violazioni costituzionali. Innanzitutto in merito alla violazione del *Fourth Amendment*<sup>25</sup> per quanto concerne gli abusi del potere esecutivo nella violazione del diritto alla riservatezza dei cittadini senza che vi fossero state necessità conseguenti ad un processo penale in corso<sup>26</sup>, nonché in mancanza

---

un'emergenza. Questi è tuttavia tenuto a informare la Corte FISC, il quale deve emanare un provvedimento autorizzativo o denegativo entro alter 72 ore (K. Wong, *Op. cit.*, p. 518).

<sup>20</sup> ACLU v. NSA, 06-CV-10204, p. 22.

<sup>21</sup> Sulle problematiche sorte in tema di segreto di Stato e sulle proposte di modifica della disciplina, A. Rapa, *When Secrecy Threatens Security: Edmonds V. Department Of Justice And A Proposal To Reform The State Secrets Privilege*, 37 Seton Hall L. Rev. 233 (2006), p. 233.

<sup>22</sup> Per quanto riguarda le decisioni più risalenti: *Totten v. United States* 92 U.S. 105 (1875); *United States v. Reynolds* 345 U.S. 1 (1953); *Halkin v. Helms*, 598 F.2d (D.C. Cir. 1978); *Halkin v. Helms*, 690 F.2d 977; *Ellsberg v. Mitchell*, 709 F.2d 51 (D. C. Cir. 1983); *Kasza v. Browner*, 133 F.3d 1159 (9<sup>th</sup> Cir. 1998); *Tenenbaum v. Simonini*, 372 F.3d 776 (6<sup>th</sup> Cir. 2004); *El-Masri v. Tenet*, 2006 WL1391390; *Hepting v. AT&T Corp.* 2006 WL 2038464;

<sup>23</sup> in un discorso radiofonico, il 17 dicembre 2005, il Presidente Bush affermò: "Nelle settimane successive agli attacchi terroristici alla nostra Nazione, autorizzai la *National Security Agency*, nel rispetto delle leggi e della Costituzione, di intercettare le comunicazioni internazionali delle persone delle quali si era a conoscenza avessero dei collegamenti con Al Qaeda e con altre organizzazioni terroristiche". Discorso reperibile sul sito web <http://www.whitehouse.gov/news/releases/2005/12/20051217.html>.

<sup>24</sup> ACLU v. NSA, 06-CV-10204, p. 14.

<sup>25</sup> Il Quarto Emendamento della Costituzione degli Stati Uniti afferma che: *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.*

<sup>26</sup> ACLU v. NSA, 06-CV-10204, p. 30.

della preventiva autorizzazione giudiziaria<sup>27</sup>, garanzia riconosciuta dalla giurisprudenza della Corte Suprema<sup>28</sup>.

Per quanto concerne la violazione della libertà di parola e del diritto di associazione tutelati dal *First Amendment*<sup>29</sup>, la Corte Distrettuale di Detroit osserva che un'azione governativa per controllare le comunicazioni elettroniche e telefoniche dei cittadini potrebbe essere giustificata soltanto dimostrando interessi governativi inoppugnabili. Ciò non è avvenuto in questo caso, data la acclarata legittimità delle conversazioni intercettate, inerenti ad attività legali e tutelate dalla medesima Costituzione. Inoltre, va considerato che il FISA esplicitamente ammonisce che nessun cittadino degli Stati Uniti può essere considerato un agente di un servizio straniero esclusivamente sulla base di attività protette dal *First Amendment* della Costituzione degli Stati Uniti<sup>30</sup>.

Infine, il Giudice Anne Diggs Taylor censura il grave sbilanciamento dei poteri dello Stato federale a favore della Presidenza perpetrato con la reiterata e occulta riconferma del *Terrorism Secret Program*. A questo proposito, occorre osservare che il Presidente ha autorizzato il TSP abusando del suo potere esecutivo attribuitogli dall'Articolo II della Costituzione<sup>31</sup> perché ha agito oltre i limiti formali posti a garanzia di ogni procedura prevista dalla Costituzione medesima<sup>32</sup> ovvero dalle leggi<sup>33</sup> nonché senza l'autorizzazione del Congresso<sup>34</sup>. Tale obiezione non può essere superata neppure in considerazione del fatto che gli Stati Uniti sono attualmente un Paese in stato di guerra<sup>35</sup>, in quanto anche l'*Authorization for Use of Military Force* (AUMF), creato per licenziare il FISA, è sottoposto alla Costituzione e non può considerarsi una fonte di diritto superiore<sup>36</sup>.

##### 5. La Class Action *Tash Hepting v. AT&T*

---

<sup>27</sup> K. Wong, *Op. cit.*, p. 523; D. A. Jordan, *Decrypting The Fourth Amendment: Warrantless NSA Surveillance And The Enhanced Expectation Of Privacy Provided By Encrypted Voice Over Internet Protocol*, 47 B.C. L. Rev. 505, (2006), p. 515. Per una ricostruzione storico-sistematica del problema in merito all'entrata in vigore del FISA, si veda M. A. Di Sabatino, *Annotation, Construction and Application of "National Security" Exception to Fourth Amendment Search Warrant Requirement*, 39 A.L.R. FED. 646, § 2a (1978).

<sup>28</sup> *Katz v. United States*, 389 U.S. 347, 359 (1967).

<sup>29</sup> Il Primo Emendamento della Costituzione degli Stati Uniti statuisce che: *Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.*

<sup>30</sup> *ACLU v. NSA*, 06-CV-10204, p. 33. In dottrina, J. C. Sims, *Op. cit.*, p. 109; L. K. Donohue, *Op. cit.*, pp. 1070-1139; S. N. Herman, *Op. cit.*, p. 70;

<sup>31</sup> L'Articolo II della Costituzione degli Stati Uniti dispone che: « §1. *The executive Power shall be vested in a President of the United States of America.* (...) §3. (...) *he shall take Care that the Laws be faithfully executed* (...). Sull'esercizio dei poteri esecutivi del Presidente degli Stati Uniti d'America, in dottrina: N. Kinkopf, *The Statutory Commander In Chief*, 81 Ind. L.J. 1169 (2006), p. 1169;

<sup>32</sup> Il giudice distrettuale di Detroit cita a questo proposito un notissimo passaggio della sentenza della Corte Suprema *Yungstown Sheet & Tube v. Sawyer*, 343 U.S. 579 (1952), la quale afferma che "*The founders of this Nation entrusted the law-making power to the Congress alone in both good and bad times. It would do no good to recall the historical events, the fears of powers and the hopes for freedom that lay behind this choice. Such a review would but confirm our holding that this seizure order cannot stand.*"

<sup>33</sup> In particolare, in riferimento alle già analizzate disposizioni del FISA.

<sup>34</sup> *ACLU v. NSA*, 06-CV-10204, p. 37.

<sup>35</sup> Successivamente ai tragici avvenimenti dell'11 settembre 2001, il Congresso ha attribuito in data 18 settembre 2001 al Presidente l'*Authorization for Use of Military Force* (AUMF), la quale dispone quanto segue: *That the President is authorized to use all the necessary and appropriate force against those nations, organizations, or person he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons*" (*Authorization for Use Military force*, Pub. L. No. 107-40, §2(a), 115 Stat. 224 (Sept. 18, 2001).

<sup>36</sup> *ACLU v. NSA*, 06-CV-10204, p. 39.

La sentenza *ACLU v. NSA* del giudice distrettuale di Detroit si riferisce principalmente alla tutela dei diritti costituzionali dei cittadini contro le intercettazioni illegali. Questo è un aspetto del problema relativo all'intercettazione illecita di comunicazioni elettroniche personali. Un altro elemento della complessa questione del fenomeno delle intercettazioni abusive di massa riguarda quelle compagnie di comunicazioni che hanno messo a disposizione dell'amministrazione le proprie apparecchiature e conoscenze tecnologiche onde attuare il *Terrorism Surveillance Program* violando i diritti costituzionali dei cittadini e gli obblighi contrattuali verso i clienti.

Una di queste azioni legali è quella intrapresa da alcuni cittadini, appoggiati dalla EFF (*Electronic Frontier Foundation*)<sup>37</sup> contro il gigante delle telecomunicazioni AT&T. La causa è attualmente pendente presso la Nona Corte Distrettuale di San Francisco. I ricorrenti lamentano una violazione dei loro diritti costituzionali tutelati dal First e dal *Fourth Amendment* della Costituzione degli Stati Uniti perchè la compagnia telefonica AT&T ha messo a disposizione della *National Security Agency* personale e strumenti tecnici adatti alle intercettazioni illegali, diffusione ovvero divulgazione delle medesime. La compagnia telefonica ha contestato le rivendicazioni degli attori chiedendo al giudice la dismissione della causa. Tale dismissione è stata rifiutata dal giudice californiano<sup>38</sup> sulla base delle gravi violazioni costituzionali addotte dai ricorrenti. Nel frattempo si è costituita l'amministrazione onde chiedere lo stralcio della causa ovvero l'applicazione del *Secret State Privilege*, mozione rigettata dal giudice<sup>39</sup>.

Quale reazione alle azioni legali, la maggioranza repubblicana<sup>40</sup> del legislatore statunitense ha presentato due proposte di legge. Questa strategia ha due obiettivi principali: garantire l'immunità per il passato alle compagnie telefoniche che abbiano collaborato alle intercettazioni abusive di massa<sup>41</sup> e modificare il FISA in alcune sue parti rilevanti in merito alle intercettazioni occulte<sup>42</sup>.

In sintesi, la Section 2 §a) del *Protecting Consumer Phone Records Act*<sup>43</sup>, in corso di discussione presso il legislatore statunitense, prevede che in generale sia proibito a chiunque acquisire informazioni dalle comunicazioni elettroniche o telefoniche senza il consenso scritto dell'interessato, anche in forma elettronica ai sensi dell'*Electronic Signatures in Global and National Commerce Act* (15 U.S.C. 7001 et seq.), agire con un artifici all'ottenimento delle informazioni attraverso l'uso di un falso consenso all'accesso, accedere illegalmente al sistema raccolta dei dati di un service provider ovvero di un gestore di telecomunicazioni; vendere od offrire in vendita informazioni relative ai clienti e alle loro comunicazioni per conto proprio o di terzi.

---

<sup>37</sup> La Electronic Frontier Foundation (EFF) è stata fondata nel 1990 con lo scopo di tutelare il libero pensiero, la riservatezza, l'innovazione e i diritti dei consumatori su Internet attraverso battaglie legali per il riconoscimento dei diritti digitali nel pubblico interesse (tratto da [www.eff.org](http://www.eff.org)).

<sup>38</sup> *Tash Hepting v. AT&T*, C-06-672 VRW, *Order* del 8 agosto 2006.

<sup>39</sup> Con la decisione del 20 luglio 2006 (Case 3:06-CU00672VRW), il Chief Judge W. R. Walker, della *United States District Court for the Northern District of California*, ha rigettato la mozione di stralcio della class action *Tash Hepting v. AT&T Corp.* fondata sulla sul solo segreto di stato.

<sup>40</sup> Maggioranza capovolta a favore del Partito Democratico in occasione delle elezioni di metà mandato del 7 novembre 2006 (Mid Term Election 2006).

<sup>41</sup> Risultato ottenibile attraverso l'introduzione del *Protecting Consumer Phone Records Act* (Bill S 2389, presentato al Senato degli Stati Uniti l'8 marzo 2006, il quale è modificativo del Communications Act of 1934 che proibiva l'acquisizione illegale e l'uso illegittimo delle comunicazioni dei clienti delle compagnie telefoniche.

<sup>42</sup> Si tratta Bill S 3874 "Terrorist Surveillance Act of 2006" depositato al Senato degli Stati Uniti il 7 settembre 2006 e consultato su <http://thomas.loc.gov/>

<sup>43</sup> Rubricata presso al Senato degli Stati Uniti come S2389, <http://thomas.loc.gov>

È di particolare interesse, perchè redatto con l'intento di bloccare le class actions dei cittadini intercettati, la Section 2 b) del citato progetto di legge<sup>44</sup>. In essa viene affermato che il *Protecting Consumer Phone Records Act* non interdice al gestore di reti di comunicazioni, ovvero agli Internet Service , o ad altra parte, l'uso di informazioni la cui acquisizione non sia stata proibita dalla *Sect 222 del Communications Act 1934*<sup>45</sup>, ovvero norme che siano in accordo con le previsioni della Sect. 222, purché tali norme siano in vigore il giorno prima della data di entrata in forza del *Protecting Consumer Phone Records Act*.

Per quanto riguarda il progetto di legge *Terrorist Surveillance Act 2006* di modifica del FISA, il legislatore interviene soprattutto sul titolo 18, relativo alle intercettazioni o raccolta di comunicazioni. In sintesi, secondo tali modifiche, il Presidente, su proposta dell'Attorney General, può autorizzare un programma di sorveglianza elettronica per un periodo di 45 giorni qualora ricorrano alcune condizioni. Queste riguardano cittadini o ovvero interessi statunitensi da proteggere all'interno dei confini degli Stati Uniti, come all'esterno; qualora ci sia probabile ragione di credere che un individuo soggetto a sorveglianza sia un agente ovvero un membro di un organizzazione terroristica o di una affiliata qualora esista una fondata possibilità di ottenere informazioni relativi ad una intelligence straniera. Nonostante una così forte incidenza del potere esecutivo nella privacy delle persone fondata su requisiti molto vaghi, viene mantenuta la disposizione relativa alla proibizione di intercettazioni ovvero sorveglianza elettronica basta esclusivamente sulle attività protette dal *First Amendment* della Costituzione USA, mentre si definisce il programma elettronico di sorveglianza posto in essere dalle autorità quale "*Terrorist Surveillance Program*".

Rimane evidente come l'amministrazione del Presidente Bush sia rimasta indifferente alle critiche delle autorità giudiziarie, della dottrina e dei semplici cittadini americani che hanno rivendicato la tutela dei loro diritti attraverso l'espletamento delle citate azioni legali. Al contrario, l'amministrazione sta tentando di legalizzare quanto accaduto attraverso una mirata modifica dell'impalcatura normativa. Considerato il recente radicale cambiamento della maggioranza politica alla *House of Representative* e al Senato degli Stati Uniti bisognerà attendere e verificare se tali politiche verranno ritenute ancora valide nella lotta al fenomeno terroristico, oppure se questa strategia sarà sottoposta a critiche<sup>46</sup> e a modifiche.

#### 6. Il problema della tutela della riservatezza delle comunicazioni in Europa.

Il problema del rapporto tra la tutela della sicurezza in relazione alla garanzia della riservatezza delle comunicazioni telefoniche ed elettroniche in merito alle intercettazioni abusive di massa ha sollevato dubbi e questioni anche in Europa addirittura precedenti agli attentati terroristici cui si accennava. Si fa riferimento all'esistenza del sistema d'intercettazione globale per le comunicazioni private ed e commerciali "Echelon"<sup>47</sup> la cui esistenza fece molto scalpore verso la fine del Secolo scorso. In questa occasione la proposta di risoluzione del Parlamento europeo<sup>48</sup> espressamente si riferisce all'art. 8 della

---

<sup>44</sup> la quale è rubricata: *Application With Section 222 Of Communications Act Of 1934*

<sup>45</sup> (47 U.S.C. 222).

<sup>46</sup> D. Eggen, *Justice Dept. to Examine Its Use of NSA Wiretaps*, Washington Post, Novembre 28<sup>th</sup> 2006, p. 10A.

<sup>47</sup> Il sistema conosciuto come "Echelon" riguarda una rete di sorveglianza globale organizzata dalla American National Security Agency (NSA) avente sede a Menwith Hill nello North Yorkshire che automaticamente filtra il traffico delle comunicazioni attraverso il Regno Unito per mezzo di parole chiave e frasi. Il sistema era in grado di utilizzare algoritmi sofisticate per intercettare discorsi complessi e riconoscere il significato del contesto (AA.VV., *A Report on the Surveillance Society*, (ed. D. M. Wood), *For the Information Commissioner by the Surveillance Studies Network*, London, September 2006, p. 18

<sup>48</sup> Proposta di risoluzione del Parlamento europeo sull'esistenza di un sistema d'intercettazione globale per le comunicazioni private ed economiche (sistema d'intercettazione ECHELON) (2001/2098(INI)).

Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali<sup>49</sup>, affermando che le intercettazioni di comunicazioni rappresentano una "profonda ingerenza nella vita privata del singolo". Tali interferenze sarebbero permesse ai sensi dell'art.8 CEDU "solo se necessarie per salvaguardare la sicurezza nazionale, nella misura in cui le disposizioni in materia siano previste dalla legge nazionale e accessibili in generale, e stabiliscano in quali circostanze e a quali condizioni l'autorità pubblica può ricorrervi; che inoltre le ingerenze nella vita privata devono essere proporzionate rispetto all'interesse da tutelare, e quindi conformemente a quanto sancito dalla CEDU non è sufficiente che siano meramente utili o auspicabili"<sup>50</sup>. Ulteriormente, l'utilizzo permanente di tali tecniche violerebbe il principio di proporzionalità previsto dalla medesima CEDU<sup>51</sup>.

Per quanto concerne il problema inerente all'utilizzo delle intercettazioni di comunicazioni elettroniche e telefoniche atte a prevenire attacchi terroristici, istituzioni comunitarie hanno emanato dichiarazioni di principio su un piano strategico per il futuro ancora da concordare tra le istituzioni e gli stati nazionali<sup>52</sup>.

Per quanto riguarda gli aspetti specifici della tutela della riservatezza delle comunicazioni, vanno segnalati due provvedimenti del Comitato dei Ministri del Consiglio d'Europa. Il primo provvedimento è la Raccomandazione Rec 10(2005)<sup>53</sup> riguardante le tecniche investigative adottabili nelle indagini antiterroristiche, tra le quali possono includersi le intercettazioni. Il Comitato dei Ministri sottolinea che l'uso delle medesime deve essere fatto secondo il principio di proporzionalità, nonché con le garanzie di legge e le prove acquisite con tali metodi devono essere sottoposte al vaglio di un giusto processo. Nello particolare caso delle intercettazioni delle comunicazioni elettroniche, telematiche e telefoniche, il Comitato dei Ministri raccomanda che il loro uso venga fatto in concordanza con specifiche norme di legge all'uopo stabilite, le quali a loro volta rispettino le disposizioni della Convenzione europea per la salvaguarda dei diritti dell'uomo e delle

---

<sup>49</sup> Il testo dell'art. 8 CEDU riguarda il Diritto al rispetto della vita privata e familiare. 1. Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza. 2. 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 per la sicurezza nazionale, per la pubblica sicurezza, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà altrui. La Corte europea dei diritti dell'uomo ha avuto occasione di pronunciarsi sulla legittimità di intercettazioni illegali effettuate dal datore di lavoro nel caso *Halford v. United Kingdom*, del 25 giugno 1997 (consultata sul sito [www.echr.coe.int](http://www.echr.coe.int)). In questa occasione la Corte ha disposto che le chiamate telefoniche rientrano nell'ambito della nozione di "vita privata" e di "corrispondenza". In conseguenza di ciò, la loro intercettazione abusiva costituisce una violazione dell'art.8 CEDU. In dottrina, S. Nigier, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006, p.181; AA. VV. (P. Coppel, A. Sharland), *Eliciting Official Information, in Information Rights*, (eds. P. Coppel), Londra, 2004, p. 32; L. K. Donohue, *Op. cit.*, p. 1155.

<sup>50</sup> Considerando n. H della Proposta di Risoluzione del Parlamento europeo n. 2001/2098 cit.

<sup>51</sup> Considerando n.I della Proposta di Risoluzione del Parlamento europeo n. 2001/2098 cit.

<sup>52</sup> Il Consiglio Europeo nella Dichiarazione dell'Aja del 4 novembre 2004 si propone di "trovare un giusto equilibrio fra tutela della vita privata e sicurezza in sede di scambio di informazioni. Lo scambio di informazioni fra autorità di contrasto è essenziale per combattere efficacemente il terrorismo e per poter svolgere indagini relative alla criminalità transfrontaliera. L'Unione deve favorire un dialogo costruttivo fra tutte le parti interessate per trovare soluzioni equilibrate fra la disponibilità delle informazioni e il rispetto di diritti fondamentali quali la tutela della privacy e la protezione dei dati personali. Materiale consultabile sul sito [www.europa.eu.int](http://www.europa.eu.int)

<sup>53</sup> Raccomandazione Rec (2005) del Comitato dei Ministri agli Stati membri sulle tecniche speciali di investigazione in relazione a crimini gravi, inclusi gli atti di terrorismo. Adottata dal Comitato dei Ministri del Consiglio d'Europa il 20 marzo 2005 e consultabile sul sito [www.coe.int](http://www.coe.int).

libertà fondamentali, in particolare l'art. 8 CEDU, nonché la Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale<sup>54</sup>

Il secondo provvedimento del Comitato dei Ministri del Consiglio d'Europa riguarda la "Dichiarazione sulla libertà di espressione e di informazione dei mezzi di comunicazione nel contesto della lotta al terrorismo"<sup>55</sup>. In tale dichiarazione, il Comitato dei Ministri richiama gli Stati membri del Consiglio d'Europa a non imporre misure restrittive sulla libertà di informazione e di espressione al di fuori di quanto previsto dagli articoli 10<sup>56</sup> e 15<sup>57</sup> della CEDU, in quanto nella loro lotta al terrorismo gli Stati ed i loro governi devono avere cura di non adottare misure contrarie ai diritti umani e alle libertà fondamentali "inclusa la libertà di espressione, pilastro delle società democratiche che i terroristi intendono distruggere"<sup>58</sup>.

In materia di uso delle intercettazioni la comparazione pone in evidenza come il sistema europeo, grazie all'azione delle istituzioni comunitarie e del Consiglio d'Europa, tende ad essere più rispettoso delle garanzie della riservatezza dei cittadini rispetto a quello statunitense, soprattutto in considerazione degli espliciti richiami alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

#### *7. La normativa italiana in materia di intercettazioni delle comunicazioni in materia di terrorismo internazionale.*

La materia delle intercettazioni delle comunicazioni elettroniche, telefoniche e telematiche inerenti alla prevenzione dei reati terroristici è regolata in Italia dal Decreto Legge 27 luglio 2005, n. 144<sup>59</sup>. L'art. 4 di questo provvedimento è rubricato "nuove norme per il potenziamento dell'attività informativa" e prevede che i Direttori dei Servizi di informazione e sicurezza S.I.S.De e S.I.S.Mi possano essere delegati dal Presidente del Consiglio dei Ministri a richiedere l'autorizzazione a svolgere le intercettazioni preventive

---

<sup>54</sup> La Convenzione n. 108/1981 è stata firmata a Strasburgo il 28 gennaio 1981 ed entrata in vigore dopo cinque ratifiche il 1 ottobre 1985 ed entrata in vigore in Italia con la legge di recepimento 21 febbraio 1989, n. 98.

<sup>55</sup> Adottata dal Comitato dei Ministri del Consiglio d'Europa il 2 marzo 2005, e consultabile sul sito [www.coe.int](http://www.coe.int).

<sup>56</sup> L'art. 10 della CEDU è rubricato "Libertà di espressione" e stabilisce che 1. Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza considerazione di frontiera. Il presente articolo non impedisce agli Stati di sottoporre a un regime di autorizzazione le imprese di radiodiffusione, di cinema o di televisione. 2. L'esercizio di queste libertà, poiché comporta doveri e responsabilità, può essere sottoposto alle formalità, condizioni, restrizioni o sanzioni che sono previste dalla legge e che costituiscono misure necessarie, in una società democratica, per la sicurezza nazionale, per l'integrità territoriale o per la pubblica sicurezza, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, per la protezione della reputazione o dei diritti altrui, per impedire la divulgazione di informazioni riservate o per garantire l'autorità e l'imparzialità del potere giudiziario. In dottrina sul punto, AA. VV. (P. Coppel, A. Sharland), *Op. cit.*, p. 30 e ss.).

<sup>57</sup> L'art. 15 della CEDU riguarda eventuali deroghe in caso di stato di urgenza. 1. In caso di guerra o in caso di altro pericolo pubblico che minacci la vita della nazione, ogni Alta Parte Contraente può prendere misure in deroga agli obblighi previsti dalla presente Convenzione, nella stretta misura in cui la situazione lo richieda e a condizione che tali misure non siano in contraddizione con gli altri obblighi derivanti dal diritto internazionale. 2. La disposizione precedente non autorizza alcuna deroga all'articolo 2, salvo per il caso di decesso causato da legittimi atti di guerra, e agli articoli 3, 4 (paragrafo 1) e 7. 3. Ogni Alta Parte Contraente che eserciti tale diritto di deroga tiene informato nel modo più completo il Segretario Generale del Consiglio d'Europa sulle misure prese e sui motivi che le hanno determinate. Deve ugualmente informare il Segretario Generale del Consiglio d'Europa della data in cui queste misure cessano d'essere in vigore e in cui le disposizioni della Convenzione riacquistano piena applicazione.

<sup>58</sup> *Declaration on freedom of expression and information in the media in the context of the fight against terrorism.*

<sup>59</sup> Convertito con modificazioni nella legge 31 luglio 2005 n.155, pubblicata sulla Gazzetta Ufficiale Serie Generale n. 173 del 27 luglio 2005.

previste dall'art.266 delle disp. att. c.p.p., quando siano ritenute indispensabili per la prevenzione delle attività terroristiche o di eversione dell'ordinamento costituzionale<sup>60</sup>.

L'art. 4 del D.L. 144/2005 differisce dall'art. 226 disp. att. c.p.p. in quanto mette a disposizione dei Direttori dei Servizi di informazione e sicurezza una nuova tipologia<sup>61</sup> di intercettazioni preventive purché sussistano i seguenti requisiti:

- a) sia stata loro concessa una delega dal Presidente del Consiglio dei Ministri<sup>62</sup>;
- b) le intercettazioni siano "ritenute indispensabili per la prevenzione di attività terroristiche o di eversione dell'ordinamento costituzionale;
- c) il Procuratore generale della Corte d'appello dove si trova l'intercettando condivida le attività e le valutazioni dei richiedenti<sup>63</sup>;
- d) le intercettazioni preventive svolte dai Servizi non siano mai svolte negli Uffici della Procura della Repubblica.

La dottrina è critica con tale tipologia di intercettazioni in quanto risponde soltanto in parte, e in modo non appropriato, alle esigenze dei rapporti interistituzionali<sup>64</sup>. A questo proposito non sembra opportuno che i Procuratori della Repubblica, cui l'ordinamento assegna specifiche competenze in materia di direzione della polizia giudiziaria e di repressione dei reati, siano stati attirati nella sfera di attività "grigie" dei Servizi di Sicurezza e di Informazione<sup>65</sup>.

### 7.1. *Le intercettazioni abusive di massa in Italia.*

Recenti vicende hanno reso la tematica delle intercettazioni abusive di massa di attualità anche in Italia. Nell'ambito delle indagini relative al rapimento di un cittadino egiziano sul territorio nazionale da parte di membri di servizi segreti stranieri, la magistratura inquirente ha scoperto l'esistenza di una struttura di *intelligence* parallela che sarebbe stata creata all'interno della principale compagnia telefonica italiana dai vertici della sicurezza dell'azienda stessa<sup>66</sup>. Tale struttura avrebbe organizzato una vasta rete sistematica di intercettazioni abusive senza l'autorizzazione dell'autorità giudiziaria. Si poneva quindi il problema di come gestire e disporre della enorme quantità di informazioni raccolte abusivamente a migliaia di cittadini ignari: da importanti esponenti della vita pubblica a cittadini comuni. Il Garante della privacy aveva già in dicembre emesso un provvedimento attinente all'illegittima pubblicazione e divulgazione dei contenuti delle intercettazioni lecite<sup>67</sup>, ma esso non era considerato sufficiente per regolare la accessibilità e utilizzabilità del materiale illecitamente raccolto. Infatti il medesimo Ufficio del Garante rilevava come,

---

<sup>60</sup> G. Aliquò, *Metodologie di prevenzione contro gli atti di terrorismo*, in *Terrorismo internazionale: modifiche al sistema penale e nuovi strumenti di prevenzione*, (a cura di E. Rosi e S. Scopelliti), Milano, 2006, p. 48.

<sup>61</sup> La dottrina afferma che si tratta di una nuova tipologia in quanto manca il rinvio ovvero un'integrazione pura e semplice al citato articolo 26 (G. Aliquò, *ult. op. loc. cit.*).

<sup>62</sup> Si tratta di una delega atipica, in quanto proveniente da una fonte politica e non giudiziaria come il Presidente del Consiglio (G. Aliquò, *ult. op. loc. cit.*).

<sup>63</sup> La citata dottrina osserva come le valutazioni dei due rappresentanti istituzionali possano divergere (G. Aliquò *op. cit.*, p. 48).

<sup>64</sup> Né l'attuale disciplina in materia di segreto di Stato sembra garantire, considerato che la Corte costituzionale ha affermato che in questa materia esistono degli ambiti del segreto di Stato nei quali, al ricorrere di tutte le condizioni di legalità, non è consentito alla magistratura inquirente di intromettersi (Corte cost., 21 novembre 1968, Corte cost. 18 novembre 1970, n. 175/; Id. 14 aprile 1976, n. 82; Id., 24 maggio 1977, n. 86. In dottrina, G. Aliquò *Op. cit.*, p. 50,

<sup>65</sup> G. Aliquò, *Op. cit.*, p. 48.

<sup>66</sup> Da *La Repubblica* del 20 settembre 2006: "Intercettazioni illegali, ventuno arresti nell'indagine su security Telecom Pirelli", nonché "Intercettavano illegalmente attraverso la Telecom: molti arresti" tratto da *Wikinotizie* dello stesso giorno consultabile sul sito web [http://it.wikinews.org/wiki/Intercettavano\\_illegalmente\\_attraverso\\_la\\_Telecom:\\_molti\\_arresti](http://it.wikinews.org/wiki/Intercettavano_illegalmente_attraverso_la_Telecom:_molti_arresti)

<sup>67</sup> Provvedimento del Garante della Privacy del 15 dicembre 2005 in materia di "nuove misure di sicurezza presso i gestori per le intercettazioni", doc. web n. 1203890.

seppure la stampa abbia il diritto dovere costituzionalmente protetto di informazione, il materiale raccolto è stato "acquisito ai danni di numerose persone che hanno subito una gravissima violazione del loro diritto alla riservatezza. Il contenuto di questi atti e documenti, coperto dal segreto istruttorio, non può in alcun modo essere diffuso dai mezzi di informazione"<sup>68</sup>.

Il Legislatore ha dato una risposta *tranchant* ordinando la distruzione di tutto il materiale abusivamente archiviato, indipendentemente dal fatto che contenesse notizie di reato e quindi fosse fonte di ulteriore attività investigativa. All'uopo venne emesso il Decreto Legge 22 settembre 2006, n. 259, rubricato Disposizioni urgenti per il riordino della normativa in tema di intercettazioni telefoniche<sup>69</sup>.

Questa soluzione è stata criticata da più parti in quanto con questo provvedimento il legislatore si è esclusivamente preoccupato di cancellare il contenuto delle intercettazioni abusive senza affrontare il problema relativo al contesto in cui lo scandaloso evento è maturato. In particolare, in riferimento al numero delle persone coinvolte (sia come presunti colpevoli sia come vittime), le modalità di esecuzione degli illeciti, il clima generale di violazione della legge che traspare dalla ricostruzione della vicenda. A parere della dottrina "tutto ciò disegna un quadro di illegalità che supera l'immaginazione"<sup>70</sup>. Addirittura vi è chi vi si domanda se l'eccessiva, forse esageratamente pignola, normazione in materia di tutela della riservatezza, a partire dalla legge 675/96, caposaldo della materia, fino alle previsioni del Codice in materia di protezione dei dati personali non sia addirittura ridondante<sup>71</sup>, considerato che non ha impedito il verificarsi di un abuso enorme come quello scoperto dalla Procura di Milano.

#### 8. Conclusioni: verso la società della sorveglianza?

In un celeberrimo film, tratto da un noto libro<sup>72</sup>, veniva paventata la creazione di una società dove gli individui erano sorvegliati in ogni loro movimento da un'autorità superiore sconosciuta ed imperscrutabile. Anche se la percezione di rassomiglianze con tale fantasia letteraria è innegabile, bisognerebbe porsi il problema della tutela della riservatezza delle comunicazioni personali dalle intercettazioni abusive o illegali da un punto di vista diverso, ovvero del controllo dell'operatore della sicurezza. L'esperienza americana come il caso italiano seppur diversi nella loro analogia ripropongono l'antica questione: *quis custodiet ipsos custodes?* Soprattutto in un'epoca dove la maggioranza delle persone sembra rassegnata a perdere parte delle proprie libertà, intimità e segretezza, anche nelle conversazioni, per il bisogno di sicurezza, concetto assai vago in verità, che tuttavia sembrerebbe in grado di acquietare le paure percepite dalle persone. D'altro canto ci si potrebbe domandare se davvero la sicurezza è alternativa alla libertà, ovvero se è necessario rinunciare a parte della propria libertà per ottenere più sicurezza. A questo proposito, la Dichiarazione dei diritti dell'uomo e del cittadino del 1786 mette sul medesimo piano entrambi i concetti, riconoscendo quali diritti naturali e imprescrittibili dell'uomo la libertà, la proprietà, la sicurezza e la resistenza all'oppressione. Si potrebbe obiettare che i tempi sono grandemente mutati, tuttavia la questione di fondo pone problemi di seria natura democratica e costituzionale. Sembrerebbe che attualmente la sicurezza non possa più

<sup>68</sup> Comunicato del Garante della Privacy del 20 settembre 2006, doc. web. n. 1341009

<sup>69</sup> Pubblicato nella GU n. 221 del 22 settembre 2006 (su questa rivista, p. 555) convertito nella legge Legge n. 281 del 20 Novembre 2006, pubblicato nella G.U. n. 271 del 21 Novembre 2006.

<sup>70</sup> M. Cammarata, *Intercettazioni e dossier illegali: quis custodiet custodes?*, consultato su [www.interlex.it](http://www.interlex.it).

<sup>71</sup> M. Cammarata, *Op. cit.*

<sup>72</sup> G. Orwell, *Nineteen-Eighty-Four*. London, Secker & Warburg, (1949); Film: 1984, Regia M. Radford, interpreti principali: J. Hurt, R. Burton, S. Hamilton, C. Cusack, G. Fisher, produzione: MGM, distribuzione: Atlantic Releasing.

essere affidata alla trasparente logica democratica<sup>73</sup>, ma stia tornando ad essere appannaggio di un potere sovrano, quello esecutivo<sup>74</sup>. Oltre ad essere una forma propria in cui l'attuale società dell'informazione si manifesta, la sorveglianza sta diventando uno strumento nelle mani dell'esecutivo attraverso il quale apparentemente si tenta di governare quello si pensa essere il fine ultimo di una qualsiasi società: il mantenimento della pace sociale<sup>75</sup>. Queste dichiarate intenzioni comunque non riescono a fugare i dubbi e le perplessità che la società civile e l'opinione pubblica qualificata si pongono su questa delicata materia.

Elena Falletti

---

<sup>73</sup> K. Koufa, *The UN, Human Rights and Counter-terrorism*, in *International Cooperation*, cit., p. 54.

<sup>74</sup> S. Niger, *Op. cit.*, p. 172.

<sup>75</sup> K. Koufa, *The UN, Human Rights and Counter-terrorism*, in *International Cooperation*, cit., p. 55.