QUESITI

Archivio Penale • gennaio-aprile 2020 • fascicolo 1 • anno LXXII
ISBN 978-88-3318-050-2 • DOI 10.12871/978883318050214 • pp. 177-195

Alberto Camon

Il cacciatore di IMSI

L'articolo è dedicato agli *IMSI catchers*: ne descrive il funzionamento, ripercorre le riflessioni scientifiche e le sentenze intervenute al riguardo negli Stati Uniti ed esamina criticamente il primo tentativo d'inquadramento effettuato dalla Corte di cassazione italiana.

IMSI-catchers

The essay deals with IMSI-catchers: it describes how they work, it sums up the U.S. litterature on the subject and it criticises the only decision by the Italian Corte di cassazione that tries to put the investigative tool in context.

1. Per comprendere l'impatto delle nuove tecnologie sull'indagine penale diventa sempre più importante confrontarsi con l'esperienza nordamericana: in vasti settori della tecnica, a cominciare dall'informatica, gli Stati Uniti occupano una posizione di leader, almeno nel mondo occidentale (per alcuni Paesi dell'est asiatico il discorso cambierebbe, ma con essi una comparazione giuridica sarebbe più difficile e meno proficua); inoltre, negli USA gli stanziamenti per le esigenze di sicurezza pubblica e di amministrazione della giustizia sono sempre stati cospicui (almeno a livello federale) e, dopo l'undici settembre, hanno toccato livelli senza precedenti, soprattutto per quanto riguarda le risorse destinate alla progettazione, allo sviluppo o all'acquisto di strumenti ad alto tasso tecnologico[1]. Per l'azione congiunta di questi fattori, se un nuovo mezzo d'indagine vede la luce, è probabile che lo faccia lì prima che da noi.

Così è accaduto per le riprese visive eseguite di nascosto all'interno d'un domicilio: il *leading case* statunitense è del 1984[2]; il nostro, del 1997[3]. Così è accaduto per il *thermal imaging device* (un apparecchio che misura il calore degli oggetti verso cui viene puntato): la Corte Suprema USA se n'è occupata nel 2001[4]; nel nostro ordinamento, a quanto risulta, ancora non ci sono precedenti. Così è accaduto per il captatore informatico: in America se ne parla almeno dai primi

1. Qualche cifra in Norman, *Taking the sting out of the Stingray: the dangers of cell-site simulator use and the role of the Federal communications commission in protecting privacy & security*, 68 *Fed. Comm. L.J.* (2016), 148.

2. United States v. Torres, 751 F.2d 875.

3. Cass., Sez. VI, 10 novembre 1997, Greco, in *Cass. pen.*, 1999, 1190, con nota di Camon, *Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove "incostituzionali"*.

4. Kyllo v. United States, 533 U.S. 27, 41 (2001).

anni del secolo, quando l'FBI mise a punto un *key logger* chiamato *Magic lantern*[5]; in Italia s'è iniziato a discuterne in seguito ad una sentenza del 2009[6]. E così sta accadendo per gli *IMSI catchers*.

2. Detti anche *cell-site simulators*, o *Stingray* (dal nome del modello più famoso)[7], gli *IMSI catchers* sono apparecchi portatili, delle dimensioni d'una valigetta[8], che possono essere portati a mano, caricati in macchina, installati su un drone o su un aereo. Sfruttando alcune vulnerabilità delle reti di comunicazione, in particolare quelle che adoperano lo standard GSM, fingono di essere un ponte radio, in modo da indurre i cellulari nei dintorni ad agganciarsi e carpirne i codici identificativi.

A grandi linee il meccanismo è questo: i cellulari funzionano scambiando messaggi con le stazioni base, o ponti radio, a loro volta inserite in una più ampia infrastruttura, la rete di comunicazione. Periodicamente (ogni sette secondi circa) le stazioni base lanciano nell'etere un richiamo per accertare quali cellulari si trovino nelle vicinanze e capire come raggiungerli nell'eventualità che una comunicazione debba essere indirizzata ad uno di essi. Tutti i cellulari che ricevono la richiesta rispondono, innescando una procedura di registrazione. Le reti GSM adoperano però un meccanismo d'autenticazione "a senso unico": la stazione mobile (il cellulare, lo smartphone, il laptop…) deve accreditarsi presso la stazione base, mentre non è richiesto l'inverso[9]; di qui la possibilità d'una stazione fasulla: l'*IMSI catcher*, appunto.

Per migliorare la qualità della comunicazione e minimizzare il consumo della batteria, i cellulari sono predisposti per connettersi automaticamente al ponte radio più potente; perciò l'*IMSI catcher* deve emettere un segnale forte, che superi quelli emanati dalle torri delle compagnie telefoniche. Quando il telefono lo riceve, si disconnette dal ponte radio "legittimo", si collega all'*IMSI catcher*, e gli manda il codice IMSI (*International Mobile Subscriber Identity*), che contrassegna la sim card. Una procedura simile può essere effettuata per farsi rilasciare il codice IMEI (*International Mobile Equipment Identity*), che contrassegna il telefono[10].

5. Woo, So, *The case for Magic Lantern: september 11 highlights the need for increased surveillance*, 15 *Harv. J. Law & Tec* (2002), 521 s.

6. Cass., Sez. V, 14 ottobre 2009, n. 16556, Virruso e altri, in *Mass. Uff.*, n. 246954-01.

7. Ma si tratta d'un dispositivo che non è più all'avanguardia. La ditta che lo produce – la *Harris Corporation* – vende già una versione più evoluta, denominata *Hailstorm*.

8. Bajak, *APNewsBreak: US suspects cellphone spying devices,* in *www.apnesnew*.

9. Federrath, *Protection in Mobile Communications*, in Müller, Rannenberg (ed.), *Multilateral Security in Communications*, München, 1999, 349 s., reperibile anche in *http://www.semper.org/sirene/publ/Fede3_99Buch3Mobil.pdf*, 6; Strobel, *IMSI Catcher*, Seminar work (Ruhr-Universitat Bochum, 2007), in *http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf*.

10. Le reti più evolute (3G, 4G) adoperano invece procedure d'autenticazione "a doppio senso". L'ostacolo non è tuttavia insormontabile: l'*IMSI catcher* può infatti "forzare" il telefono verso

Prendere i codici si mostra utile soprattutto come tappa preliminare a controlli ulteriori: per esempio, l'inoculazione d'un *trojan horse*, che, per avere qualche probabilità di successo, richiede che si conosca in anticipo il sistema operativo che "gira" sul dispositivo: un'informazione rivelata, per l'appunto, dal codice identificativo dell'apparecchio[11]. Oppure un'intercettazione, destinata a colpire un telefono di cui ancora non si conosce il numero[12]. O infine – è l'applicazione più frequente – un "pedinamento elettronico"[13]: una volta che il codice identificativo del bersaglio sia stato ottenuto, esso viene inserito nello *Stingray*, che a questo punto è in grado di seguirne gli spostamenti[14], con un margine d'errore molto basso: per alcuni dispositivi, un paio di metri. Questo significa che chi li adopera può sapere non soltanto in quale edificio si trova un individuo, ma anche in quale stanza, ed anzi in quale area di due metri quadrati all'interno di quella stanza[15].

La maggior parte dei modelli in commercio hanno anche funzioni aggiuntive (spesso vendute a parte, come softwares opzionali): possono infatti interrompere il servizio, impedendo la connessione alla rete[16]; registrare il contenuto delle comunicazioni inviate e ricevute[17]; fare chiamate o mandare messaggini per conto

una connessione 2G, cioè meno protetta (Dabrowski, Pianta, Klepp, Mulazzani, Weippl, *IMSI-catch me if you can: IMSI-catcher-catchers* (2014), reperibile in *www.researchgate.net*) e al tempo stesso obbligarlo a mostrare sul display l'informazione – a questo punto falsa – di essere ancora connesso ad una rete 3 o 4G (Norman, *Taking the sting out of the Stingray*, cit., 142 s.).

11. L'IMEI è una stringa composta da 15 cifre, suddivise in 4 parti: la prima indica la casa costruttrice e il modello del telefonino a cui il codice è associato.

12. È il caso che sarà discusso *infra*, §§ 5-8.

13. Owsley, *TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions*, 66 *Hastings L.J.* (2014), 193.

14. Brown, Leese, *Stingray devices usher in a new fourth amendment battleground*, 39 *Champion* (2015), 14; Kerr, *Applying the Fourth Amendment to Cell-Site Simulators*, *The Washington Post*, 4 aprile 2016.

15. Così, quasi testualmente, Hemmer, *Duty of candor in the digital age: the need for heightened judicial supervision of stingray searches*, 91 *Chi.-Kent L. Rev.* (2016), 300 s.

In svariate occasioni è infatti accaduto che il *cell-site simulator* abbia permesso alla polizia di individuare lo stabile, e lo specifico appartamento all'interno di quello stabile, in cui l'imputato si nascondeva: per un esempio, United States v. Lambis, No. 15-CR-724, 2016 WL 3870940 (S.D.N.Y. July 12, 2016).

16. Zetter, *Turns out police stingray spy tools can indeed record calls*, in *Wired*, (*www.wired.com/2015/10/stingray-government-spy-tools-can-record-calls-new-documents-confirm*).

17. Lye, *In Court: Uncovering Stingrays, A Troubling New Location Tracking Device*, in *www.aclu.orgn*; Pagliery, *FBI lets suspects go to protect «Stingray» secrets*, in *money.cnn.com/2015/03/18/technology/security/police-stingray-phone-tracker/*; Pell, Soghoian, *A Lot More than a Pen Register, and Less than a Wiretap*, 16 *Yale J.L. & Tech* (2014), 143, nota 20, 146 e 148, nota 46; in re *application of the United States of America for an order authorizing the use of a cellular telephone digital analyzer*, 885 F. Supp. 197 (C.D. Cal. 1995).

del telefono "in ostaggio"; cambiare il contenuto dei messaggi inviati[18]; esplorare e registrare quanto è archiviato nel dispositivo sotto controllo[19].

Per fare tutto ciò, l'*IMSI catcher* posa simultaneamente da ponte radio (ingannando il cellulare) e da cellulare (ingannando il ponte radio "vero")[20]. L'indagine in tal caso si prolunga nel tempo, ed è allora importante che il cellulare non si disconnetta dall'*IMSI catcher*, come potrebbe accadere se si allontanasse. Ebbene, per agevolare le "transizioni" fra i ponti radio ed evitare interruzioni del servizio, generalmente le stazioni base inviano ai cellulari una lista delle stazioni vicine, con l'indicazione della potenza del rispettivo segnale, in modo da informare il cellulare in movimento sulle torri alle quali agganciarsi per non perdere la linea; allo scopo di tenere prigioniero il telefono sotto controllo, l'*IMSI catcher* gli può mandare una lista vuota, oppure un elenco che contiene soltanto stazioni tecnicamente non disponibili, o infine alterare l'indicazione della potenza del segnale emesso dalle varie torri[21].

Come sempre succede in questi casi, si stanno diffondendo anche le contromisure: smarthpones più protetti (*Cryptophone*, *Stealth Phone*, *Blackphone*…); o soluzioni informatiche (hardware o software) che smascherano gli *IMSI catchers*: il loro nome inglese – *"IMSI catcher catchers"*[22] – evoca brillantemente la competizione fra spionaggio e controspionaggio. L'antidoto più efficace è anche il più semplice: spegnere il telefono, o metterlo in "modalità aereo"; ma naturalmente non è sempre possibile.

3. Si sa che negli U.S.A. le agenzie di *law enforcement* (federali, statali e locali) li usano da almeno venticinque anni[23], forse di più; dal 2010 sono anche adoperati a bordo di piccoli aerei che sorvolano i centri abitati, aumentando così a dismisura il numero dei soggetti monitorati[24].

18. Hemmer, *Duty of candor*, cit., 296 s.

19. Norman, *Taking the sting out of the Stingray*, cit., 141 s.

Per una descrizione di caratteristiche, funzioni, prezzi di alcuni apparecchi (peraltro un po' datata; sono passati sei anni, e in questo campo non sono pochi) si può vedere Gallagher, *Meet the machines that steal your phone's data*, in *https://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/2/*.

20. Meyer, Wetzel, *On the Impact of GSM Encryption and Man-in-the-Middle Attacks on the Security of Interoperating GSM/UMTS Networks*, in *Proceedings of the 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2004, reperibile anche in *https://www.cs.stevens.edu/~swetzel/publications/pubtopic.html*, p. 2876.

21. Dabrowski, Pianta, Klepp, Mulazzani, Weippl, *IMSI-catch me*, cit., 4.

22. Dabrowski, Pianta, Klepp, Mulazzani, Weippl, *IMSI-catch me*, cit., 1.

23. Pell, Soghoian, *A Lot More than a Pen Register*, cit., 142; Zetter, *Florida Cops' Secret Weapon: Warrantless Cellphone Tracking*, in *Wired*, 3 marzo 2014 (*http://www.wired.com/2014/03/stingray/*).

24. Pagliery, *U.S. planes spy on American phones*, in *https://money.cnn.com/2014/11/13/technology/security/federal-planes-spy/?iid=EL*.

I casi in cui i giudici se ne sono occupati, tuttavia, non sono tanti; questi metodi d'indagine diventerebbero meno efficaci se diventassero di pubblico dominio, perché i bersagli potrebbero imparare a modificare i loro comportamenti per eludere la sorveglianza; s'è perciò sviluppata una sinergia fra case produttrici, *prosecutors* e agenzie di *law enforcement*: al momento dell'acquisto degli *Stingray*, di solito venditore e compratore sottoscrivono anche un accordo di riservatezza, in forza del quale i rappresentanti dell'accusa sono tenuti a rivelare il meno possibile al riguardo, anche rinunciando ad incriminare, abbandonando processi già iniziati o offrendo *plea bargains* molto generosi pur d'evitare il rischio di *leaks*[25].

Malgrado ciò, si può comunque registrare una significativa evoluzione: nella seconda metà degli anni Novanta, il *Department of Justice* cerca di sostenere che i *cell-site simulators* possono essere usati senza limiti, facendo leva soprattutto sul fatto che la polizia non se ne serve – così almeno si dichiara – per controllare il contenuto delle comunicazioni[26]. Questa posizione viene avallata da una delle poche pronunce pubblicate[27].

Col passare del tempo, stampa, associazioni di tutela delle libertà civili (da *American Civil Liberties Union* a *Electronic Privacy Information Center*), giuristi, prendono coscienza del meccanismo e alzano il livello d'attenzione. Pressato da queste sollecitazioni, il *Department of Justice* muta indirizzo e raccomanda ai *prosecutors* di munirsi preventivamente d'una autorizzazione giurisdizionale, sulla base della disciplina del *Pen/Trap statute*[28]. Si tratta d'una sezione (§§ 3121-3127) dell'*E-*

Prescrizioni specifiche per l'«*use of a cell-site simulator on an aircraft*» sono dettate dal *Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology*, 2015, 4 (*https://www.justice.gov/opa/file/767321/download*).

25. La questione è affrontata in Brown, Leese, *Stingray devices*, cit., 13 s.; Hazen, *Upholding citizens' privacy in the use of stingray technology: is new york behind?*, 37 *Pace L. Rev.* (2016), 359 s.; Kelly, *Cellphone data spying: It's not just the NSA, USA today*, 8 dicembre 2013, *http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsapolice/3902809/*; Kim, *The fourth amendment implications on the real-time tracking of cell phones through the use of "Stingrays"*, 26 *Fordham Intell. Prop. Media & Ent. L.J.* (2016), p. 1009; McCandless, *Stingray Confidential*, 85 *Geo. Wash. L. Rev.* (2017), 993 s.; Owsley, *TriggerFish, StingRays, and Fourth Amendment*, cit., 199; Pell, Soghoian, *Your secret Stingray's no secret anymore: the vanishing government monopoly over cell phone surveillance and its impact on national security and consumer privacy*, 28 *Harvard Journal of Law & Technology* (2014), 33 s.; Powers, *Surveillance remedies: Stingrays and the exclusionary rule*, 96 *Or. L. Rev.* (2017), 341 s.
Alcuni *non-disclosure agreements* sono stati raccolti dal *Center for Human Rights and Privacy* e possono essere consultati in *https://www.cehrp.org/non-disclosure-agreements-between-fbi-and-local-law-enforcement/*.

26. Executive Office for United States Attorneys, *Electronic Investigative Techniques, Usa Bulletin*, Sept. 1997, in *http://www.justice.gov/usao/eousa/foia_reading_room/usab4505.pdf*), 14 s. e 23.

27. In re *application of the United States of America for an order authorizing the use of a cellular telephone digital analyzer*, cit.

28. Electronic Surveillance Unit, *Electronic Surveillance Manual: Procedures and Case Law Forms*, *U.S. Dep't of Justice* 40 (2005), reperibile anche online (*http://www.justice.gov/criminal/foia/*

lectronic Communications Privacy Act del 1986, che si occupa dei dispositivi volti a registrare i dati di traffico delle comunicazioni: in particolare, *pen registers* e *trap and trace devices*; i primi, una volta collegati alla linea telefonica, memorizzano i numeri chiamati; i secondi, i numeri chiamanti. Formalmente, la nuova interpretazione patrocinata dal *Department of Justice* poggia su una modifica portata nel 2001 dal *Patriot Act*, che ha allargato la definizione legislativa dei *pen registers* e dei *trap and trace devices*, per renderla applicabile anche alle comunicazioni di tipo elettronico; sostanzialmente, è l'effetto della vigilanza e delle critiche portate avanti da più fronti verso la vecchia dottrina[29].

Ad ogni modo, ottenere un *pen-trap order* non è particolarmente difficile, perché non occorre *probable cause*; basta mostrare che le informazioni cercate sono pertinenti ad un'indagine in corso: uno standard talmente basso che la funzione del giudice chiamato a rilasciare l'autorizzazione è considerata «*ministerial in nature*»[30]. Si spiega, così, come questo modesto innalzamento della tutela non risulti del tutto tranquillizzante; non per caso, qualche giudice cassa il nuovo inquadramento giuridico: il *Pen/Trap statute* – si dice – riguarda meccanismi diversi, sotto alcuni aspetti meno intrusivi (e comunque insuscettibili d'essere allargati)[31].

Gli svolgimenti posteriori – prevalentemente incentrati su un particolare impiego dello *Stingray*, ossia la localizzazione di chi adopera il dispositivo sotto controllo – proseguono il cammino. L'interesse degli studiosi s'alza ancora: nel complesso, reclamano maggiori tutele[32] e acquisiscono una più ferma consape-

docs/elec-sur-manual.pdf), 46. Si ricordi comunque che i provvedimenti del DoJ valgono per l'FBI e per altre agenzie federali, ma non a livello statale o locale (sul punto, Hazen, *Upholding citizens' privacy*, cit., 355 s.); inoltre, essi dettano le linee d'una *policy* interna all'ufficio, ma non possono di per sé creare diritti tutelabili in giudizio.

29. Cfr. Winner, *From historical cell-site location information to imsi-catchers: why Triggerfish devices do not trigger fourth amendment protection*, 68 *Case W. Res. L. Rev.* (2017), 261.

30. United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995).

31. In re *application of the United States of America for an order authorizing the installation and use of a pen register and trap and trace device*, 890 F. Supp. 2d 747, 748 (S.D. Tex. 2012).

32. Benway, *You can run, but you can't hide: law enforcement's use of "stingray" cell phone trackers and the fourth amendment*, 42 *S. Ill. U.L. J.* (2018), 287 s.; Brown, Leese, *Stingray devices*, cit., 14 s.; D'Amico, *Cellphones, Stingrays, and searches! An inquiry into the legality of cellular location information*, 70 *U. Miami L. Rev.* (2016), 1298 s.; Gee, *Almost gone: the vanishing fourth amendment's allowance of Stingray surveillance in a post-Carpenter age*, 28 *S. Cal. Rev. L. & Social Justice* (2019), p. 430 s.; Hampton, *From smartphones to Stingrays: can the fourth amendment keep up with the twenty-first century?*, 51 *U. Louisville L. Rev.* (2012), 173 s.; Harris, *The backdoor that leads to the trap door: the unusual effects of 18 U.S.C. § 2703(d) and Stingrays*, 45 *S.U. L. Rev.* (2017), 145 s.; Jonassen, *StingRays, Triggerfish, and Hailstorms, oh my! The fourth amendment implications of the increasing government use of cell-site simulators*, 33 *Touro L. Rev*. (2017), 1156 s.; Kim, *The fourth amendment implications*, cit., 1033 s.; Maleska, *Stinging the Stingray: the need for strong state-level anti-surveillance legislation*, 52 *Val. U.L. Rev.* (2018), 664 s.; Owsley, *TriggerFish, StingRays, and Fourth Amendment*, cit., 218 s.; Sullivan, *Is your smartphone conversation private? the Stingray device's impact on privacy in States*, 67 *Cath. U.L. Rev.* (2018), 388 s.;

volezza delle differenze rispetto a *pen registers* e *trap and trace devices*. Per esempio: la ragione per la quale questi ultimi strumenti non pretendono un *warrant* si riallaccia alla cosiddetta *third-party doctrine*[33]: in buona sostanza, chi volontariamente comunica ad un terzo determinate informazioni – per esempio, l'abbonato che fa una chiamata, ben sapendo che i numeri digitati sulla tastiera dell'apparecchio vengono trasmessi al gestore del servizio – accetta il rischio che il terzo le diffonda, e non può dunque invocare una *reasonable expectation of privacy*. Ma questo ragionamento fatica ad essere applicato agli *IMSI catchers*[34]: da un lato, essi non raccolgono passivamente un dato accessibile ma sollecitano, in modo attivo, a fornirlo; dall'altro, il rilascio dell'informazione da parte dell'interessato non è consapevole, perché lo scambio di segnali fra cellulare e ponte radio avviene automaticamente, senza bisogno che venga intrapresa alcuna azione.

Insieme all'attenzione della dottrina giuridica, cresce anche la consapevolezza degli intellettuali (lo *Stingray* occupa una scena di *Zero Dark Thirty*, un film che racconta la caccia a Osama bin Laden) e, di riflesso, dell'opinione pubblica. Si muovono i legislatori: progetti di legge vengono presentati al Congresso[35]; vari Stati (Colorado, Florida, Illinois, Indiana, Maine, Maryland, Minnesota, Montana, New Hampshire, New Jersey, Tennessee, Utah, Virginia, Washington, Wisconsin…) approvano *Statutes* in forza dei quali il tracciamento è una *Fourt amendment search* e richiede perciò un *warrant* e una *probable cause*[36]. Nella stessa direzione si schierano le corti, dalla *District Court of Arizona*[37] alla *Court of special appeals del Maryland*[38],

Vaysman, *Who's pinging your phone? Exploring the fourth amendment ramifications of Stingray devices*, 12 *Seventh Circuit Rev.* (2017), 407 s.

33. La *third-party doctrine* risale a United States v. Miller, 425 U. S. 435, 443 (1976), ed è stata applicata ai *pen registers* da Smith v. Maryland, 442 U.S. 735, 742 (1979).

Si tratta dunque d'un ragionamento risalente, che comincia perciò a mostrare i segni del tempo e che, secondo alcuni, meriterebbe d'essere radicalmente ripensato alla luce degli sviluppi vorticosi della tecnologia: si veda per esempio la *concurring opinion* di Sotomayor a United States v. Jones, 132 S. Ct. 945, 963 (2012).

34. Fra i molti, Maleska, *Stinging the Stingray*, cit., 651 s. Si veda anche (ma senza riferimenti agli *IMSI catchers*) Carpenter v. United States, 585 U.S. (2018). *Contra*, Chapman, *The outer limits: imsi-catchers, technology, and the future of the fourth amendment*, 44 *Pepp. L. Rev.* (2017), 862 s.; Winner, *From historical cell-site location information to imsi-catchers*, cit., 269 s.

35. Cfr. Benway, *You can run, but you can't hide*, cit., 286 s.; Maleska, *Stinging the Stingray*, cit., 648 s.

36. Boyne, *2017 evolving investigative technologies and the law symposium: Stingray technology, the exclusionary rule, and the future of privacy: a cautionary tale*, 119 *W. Va. L. Rev.* (2017), 937; Danelo, *Legislative solutions to Stingray use: regulating cell site simulator technology post-Riley*, 91 *Wash. L. Rev.* (2016), 1391 s.

37. United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012).

38. State v. Andrews, 134 A.3d 324, 326 (Md. Ct. Spec. App. 2016). Per un commento alla decisione si può vedere Kerr, *Applying the Fourth Amendment*, cit.

dalla *District court del Southern district of New York*[39] alla *District of Columbia Court of appeals*[40]. Perfino il *Department of Justice* si arrende e abbandona l'idea d'un *warrantless use* dello *Stingray* (anche se, al tempo stesso, cerca di allargare il più possibile le ipotesi derogatorie nelle quali si può prescindere dal mandato)[41].

Infine l'onda lambisce la Corte Suprema: *Carpenter v. United States*[42] – una decisione molto nota anche da noi[43] – afferma che, per ottenere dalle compagnie telefoniche le registrazioni delle "celle" agganciate nel corso del tempo da un telefono, è necessario un mandato, fondato su una *probable cause*[44]. Per la verità, la Corte non prende posizione sugli *IMSI catchers*[45]; non solo, ma lascia aperta la possibilità che un mandato non sia necessario qualora – come generalmente accade quando viene adoperato lo *Stingray* – il pedinamento elettronico non duri a lungo[46]. Insomma, la posizione di chi ritiene che le questioni poste dagli *IMSI catchers* siano state definitivamente risolte[47], non pare corretta[48]; di certo, però, Carpenter contro Stati Uniti è espressione della crescente inquietudine suscitata dalle nuove forme di controllo tecnologico dell'imputato; e nella crescita di que-

39. United States v. Lambis, cit.

40. Jones v. United States, 168 A.3d 703 (D.C. 2017).

41. *Department of Justice Policy Guidance*, cit., 4 s.

42. Gia citata *supra*, nota 34.

43. Se ne occupano Fanchiotti, *Carpenter v. U.S.; si amplia la tutela contro la* global police surveillance, in *Giur. it.*, 2018, 2262 s.; Fanuele, *La localizzazione satellitare nelle investigazioni penali*, Milano, 2019, 142 s.

44. *Carpenter v. United States* sviluppa una affermazione già resa in *United States v. Jones*, cit., con riguardo alla localizzazione svolta attraverso un ricevitore GPS; in *United States v. Jones*, però, l'argomento centrale – in aderenza alla dottrina del *physical trespass*, che affonda le sue radici nel *common law* ed è stata abbracciata dalla Corte sin da *Olmstead v. United States*, 277 U.S. 438 1928 – era ancora rappresentato da una aggressione "fisica" al domicilio (in quel caso la polizia aveva infatti attaccato il ricevitore GPS alla macchina del sospettato). Carpenter si stacca da quel filone.

45. «*Our decision today is a narrow one. We do not express a view on matters not before us [such as] real-time CSLI*» (*cell-site location informations*). Su questo passaggio si può vedere Kerr, *Understanding the Supreme Court's Carpenter Decision*, in *Lawfare* (22 giugno 2018), in *http://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision*.

46. La proposta di riconoscere in favore delle forze di polizia una specie di franchigia per controlli temporalmente circoscritti (a seconda delle impostazioni, ventiquattr'ore o sette giorni) è stata in effetti avanzata; ma la Corte ha ritenuto di poterla accantonare, perché, nella vicenda al suo esame, il limite sarebbe comunque stato sfondato (le registrazioni consegnate all'FBI attestavano gli spostamenti di Carpenter lungo un periodo di 127 giorni).

47. Cfr. State v. Sylvestre, 254 So. 3d 986 (Fla. Dist. Ct. App. 2018) («*If a warrant is required for the government to obtain historical cell-site information voluntarily maintained and in the possession of a third party, the court can discern no reason why a warrant would not be required for the more invasive use of a cell-site simulator*»).

Prima che la Corte Suprema si pronunciasse, anche Park (*Protecting the fourth amendment after Carpenter in the digital age: what gadget next?*, 60 *Orange County Lawyer* (2018), 35) si era espresso nel senso che la decisione avrebbe inevitabilmente chiuso pure il problema degli *IMSI catchers*.

48. Nello stesso senso, Fanchiotti, *Carpenter v. U.S.*, cit., 2265 s.

sta inquietudine, gli *IMSI catchers* hanno giocato un ruolo importante.

4. Ma la riflessione statunitense non ha avuto un andamento binario, cioè non ha riguardato soltanto il dubbio intorno all'esigenza d'un mandato; molto s'è discusso anche sull'estensione del controllo affidato al giudice e sulla portata dell'autorizzazione che questi è chiamato a rilasciare.

Già sono state sottolineate alcune peculiarità delle indagini condotte con lo *Stingray*; ma l'aspetto che soprattutto le caratterizza, e che al tempo stesso vale a distinguerle sia da un'acquisizione delle *historical cell-site location informations* conservate dai providers (noi diremmo: da un'acquisizione di tabulati telefonici) sia dai *pen registers* e dai *trap and trace devices* sia dai captatori informatici, è un altro: mentre questi ultimi strumenti permettono di circoscrivere il controllo ad un bersaglio specifico, i cacciatori di IMSI registrano le informazioni provenienti da *tutti* i telefoni che si trovano in una certa area[49]. L'esatta estensione della zona scandagliata (e, di conseguenza, il numero dei telefoni che rimangono impigliati nella rete) non è nota, ma alcune fonti parlano, rispettivamente, di svariati chilometri e di migliaia[50], o decine di migliaia[51], di apparecchi.

Lo slittamento da una sorveglianza mirata ad una più ampia ed indistinta determina un salto qualitativo e apre interrogativi urgenti. A tale riguardo meritano un cenno episodi che sembrano quasi estratti dalla distopia orwelliana: lo *Stingray* è stato adoperato per controllare i partecipanti a manifestazioni politiche, con il conseguente rischio d'una schedatura su basi ideologiche. Inutile dire che ne sono nate molte proteste[52]. Su questi temi si sono affaticati giudici, agenzie di *law enforcement*, legislatori, studiosi, con proposte e soluzioni sulle quali conviene spendere qualche parola.

Partiamo da un caso del 2012: nel corso d'una lunga indagine condotta dalla

49. La differenza è sottolineata da molti; a titolo esemplificativo, Brown, Leese, *Stingray devices*, cit., 13; Harris, *The backdoor that leads to the trap door*, cit., 138 s.; Jonassen, *StingRays, Triggerfish, and Hailstorms*, cit., p. 1158; Kim, *The fourth amendment implications*, cit., 1012 s.; Owsley, *TriggerFish, StingRays, and Fourth Amendment*, cit., 185 s.; Vaysman, *Who's pinging your phone?*, cit., 371.
Non stupisce che alcuni produttori magnifichino queste potenzialità (cfr. *Tactical off-air intelligence solutions* (2013), reperibile in *http://s3.documentcloud.org/documents/885760/1278-verint-product-list-engage-gi2-engage-pi2.pdf*), 7, dove la ditta Verint mette l'accento sulla capacità dei dispositivi di «*collect mass GSM traffic over a wide area*»): ciò che, in una prospettiva attenta ai rischi per la *privacy*, è un fattore d'allarme, in una prospettiva attenta all'efficacia dell'indagine diventa un punto di forza.

50. Cfr. Hemmer, *Duty of candor*, cit., 299.

51. Kim, *The fourth amendment implications*, cit., 1043.

52. Cfr. Boyne, *2017 evolving investigative technologies*, cit., 918 s.; Eördögh, *Evidence of "Stingray" phone surveillance by police mounts in Chicago*, in *Christian Science Monitor* (22 dicembre 2014), *http://www.csmonitor.com/World/Passcode/2014/1222/Evidence-of-StingRay-phone-surveillance-by-police-mounts-in-Chicago*; H. Gee, *Almost gone*, cit., 433 s.; Meadows, *Dead end surveillance – Stingrays and civil rights*, in *Native News Online.net* (7 ottobre 2016), in *http://nativenewsonline.net/currents/dead-end-surveillance-StingRays-civil-rights/*.

DEA, di punto in bianco sembra che il cellulare d'uno degli indagati non funzioni più; un collaboratore di giustizia riferisce che il sospettato ne ha comprato uno nuovo, ma non ne conosce il numero; allora l'*assistant attorney* chiede l'autorizzazione ad usare uno *Stingray*: adoperandolo per un certo periodo in tutti i luoghi in cui l'imputato si reca, si potrebbero registrare i dati identificativi degli apparecchi che di volta in volta si trovassero nei pressi; quello che comparisse sempre, ad ogni controllo, sarebbe l'IMSI del telefono cercato, che da quel momento in poi potrebbe essere oggetto d'una sorveglianza mirata. D'accordo, ma – si domanda il giudice – in quanti e quali luoghi sarebbe usato lo *Stingray*? Per quanto tempo? Con quale raggio d'azione? Coinvolgendo quanti malcapitati? E quale uso verrebbe fatto delle informazioni raccolte da soggetti estranei al procedimento? Sono quesiti troppo delicati per essere lasciati in sospeso; perciò l'autorizzazione viene rifiutata[53].

In una vicenda di quello stesso anno, gli organi dell'indagine si mostrano più circospetti. In quell'occasione lo *Stingray* serviva per localizzare una *aircard* (un modem portatile) adoperata dal sospettato; per farlo, era necessario raccogliere anche dati provenienti da terzi; però queste informazioni sono state immediatamente cancellate dalla memoria dello *Stingray*, e della distruzione è stata redatta e conservata idonea documentazione[54].

Un'altra decisione notevole, che testimonia una progressiva crescita di consapevolezza intorno ai problemi causati dalle tecniche di sorveglianza massive, è emessa dalla *District Court dell'Eastern District of Illinois*: il giudice autorizza, sì, l'uso dello *Stingray*, ma con una serie d'importanti limitazioni, fra le quali andrà ricordato l'obbligo della polizia di fare tutto il possibile per ridurre la cattura di segnali provenienti da terzi (ad esempio restringendo l'area sorvegliata) e il divieto d'usare i dati comunque acquisiti da soggetti estranei all'indagine[55].

Nella stessa direzione si muove il *Department of Justice*, che a sua volta spiega come minimizzare i "danni collaterali" inevitabilmente arrecati dallo *Stingray*: «*1. When the equipment is used to locate a known cellular device, all data must be deleted as soon as that device is located, and no less than once daily. 2. When the equipment is used to identify an unknown cellular device, all data must be deleted as soon as the target cellular device is identified, and in any event no less than once every 30 days. 3. Prior to deploying equipment for another mission, the operator must verify that the equipment has been cleared of any previous operational data. Agencies shall implement an auditing*

53. In re *application of the United States of America for an order authorizing the installation and use of a pen register and trap and trace device*, cit.

54. United States v. Rigmaiden, cit.

55. In re *application of the U.S. for an order relating to telephones* n. 3:15-mc-00021, 2015 WL 6871289.

program to ensure that the data is deleted in the manner described above»[56].

Spunti di qualche interesse su questi temi vengono anche dagli *Statutes*, che si fanno carico sia del bisogno di limitare il sacrificio alla *privacy* sia dell'esigenza di assicurare un controllo effettivo sul rispetto dei limiti eventualmente fissati nel *warrant*. Sotto il primo profilo andrà ricordata la legislazione di Washington, che impone al giudice d'indicare nel mandato, fra l'altro, l'area geografica che potrà essere legittimamente battuta dal *cell site simulator*[57]. Sotto il secondo aspetto, va segnalata una previsione del *California penal code*, in forza della quale il giudice che emette il mandato può nominare un esperto deputato a sovrintendere l'impiego dello *Stingray* e controllare che i paletti eventualmente fissati non siano scavalcati[58]. In una logica non molto distante, uno studioso ha proposto che l'esame dei dati raccolti sia affidato a funzionari estranei all'indagine, i quali avrebbero il compito di passare a polizia e *prosecutors* le sole informazioni pertinenti all'oggetto del *warrant*, cancellando tutte le altre[59].

5. Torniamo adesso da questa parte dell'oceano. La discussione è iniziata più tardi, però è cresciuta svelta ed ha già messo in moto i legislatori di vari Paesi: il codice di procedura penale francese si occupa degli *IMSI catchers* nell'art. 706-95-20,

56. *Department of Justice Policy Guidance*, cit., 7.

Un mese più tardi, il Department of Homeland Security seguirà l'esempio ed emetterà un provvedimento quasi identico: cfr. United States Department of Homeland Security, *Department Policy Regarding the Use of Cell-Site Simulator Technology* (2015), in *https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf*.

57. «*The order shall specify: […] in the case of a cell site simulator device: a) The telephone number or other unique subscriber account number identifying the wire or electronic communications service account used by the device to which the cell site simulator device is to be attached or used; b) if known, the physical location of the device to which the cell site simulator device is to be attached or used; c) the type of device, and the communications protocols being used by the device, to which the cell site simulator device is to be attached or used; d) the geographic area that will be covered by the cell site simulator device; e) all categories of metadata, data, or information to be collected by the cell site simulator device from the targeted device including, but not limited to, call records and geolocation information; f) whether or not the cell site simulator device will incidentally collect metadata, data, or information from any parties or devices not specified in the court order, and if so, what categories of information or metadata will be collected; and g) any disruptions to access or use of a communications or internet access network that may be created by use of the device*»: Wash. Rev. Code § 9.73.260 (4)(c) (ii).

58. «*When issuing any warrant or order for electronic information, or upon the petition from the target or recipient of the warrant or order, a court may, at its discretion, do either or both of the following: (1) Appoint a special master […] charged with ensuring that only information necessary to achieve the objective of the warrant or order is produced or accessed. (2) Require that any information obtained through the execution of the warrant or order that is unrelated to the objective of the warrant be destroyed as soon as feasible after the termination of the current investigation and any related investigations or proceedings*» (California penal code, § 1546.1 e) 1-2).

59. L'interessante suggerimento è di Hemmer, *Duty of candor*, cit., 315 s.

ritoccato nel 2019; l'StPO tedesco, nell'art. 100i, introdotto nel 2002 e modificato nel 2017; in Austria, una prima regolamentazione è stata varata nel 2005: molto blanda, collocata fuori dal codice, è stata al centro di polemiche estenuanti, sfociate infine nella riscrittura del 2018, che ha portato le norme dentro al codice (§§ 132, 134 e 137 StPO) e alzato il livello delle garanzie.

In questo movimentato panorama, l'Italia è un caso a sé. Alcuni segnali avrebbero dovuto attirare attenzione: in particolare, le amministrazioni dalle quali dipendono le forze di polizia hanno a più riprese bandito gare d'appalto per l'«acquisizione di […] sistem[i] *IMSI catcher* per il monitoraggio e la localizzazione di terminali radiomobili»[60]. Ciò mostra come la nostra polizia si serva da anni dei cacciatori di IMSI. Paradossalmente, la stampa "generalista" se n'è accorta presto[61], mentre la dottrina giuridica – pur attentissima ad argomenti in qualche misura contigui, come quelli posti dai captatori informatici – qui arranca, in grave ritardo: per contare gli studiosi che hanno visto il tema e cercato di far partire un dibattito, le dita d'una mano sono fin troppe. E così, quando – un paio d'anni fa – la Corte di cassazione s'è per la prima volta misurata con il nostro mezzo d'indagine, l'ha dovuto fare senza il supporto d'una riflessione scientifica ampia.

La vicenda riguarda uno degli usi più basici del dispositivo: in un procedimento su un'associazione per delinquere finalizzata al traffico internazionale di

60. La citazione è dal primo bando di cui chi scrive ha notizia, pubblicato nel 2013 dal Ministero degli Interni (lo si può leggere in *https://www1.interno.gov.it/mininterno/site/it/sezioni/servizi/bandi_gara/dip_pubblica_sicurezza/2013_07_08_imsi.html*). Successivamente ci sono state altre gare; si vedano, ad esempio, quella bandita dal ministero dell'interno nel 2015 (in *Gazz. uff.*, 5a serie speciale, 6 maggio 2015, p. 12 s.; una rettifica in *Gazz. uff.*, 5a serie speciale, 22 maggio 2015, n. 59, 176); quella bandita dal comando generale della Guardia di Finanza nel 2018 (in *http://www.gdf.gov.it/repository/re.t.l.a/comando-generale/bandi-di-gara-e-contratti/anno-2018/acquisizione-di-n.-8-sistemi-imsi-imei-per-il-monitoraggio-della-rete-cellulare*); quella bandita dal comando generale della Guardia di Finanza nel 2019 *(Gazz. uff.*, 5a serie speciale, 27 marzo 2019, n. 37, 9).

Possono destare qualche interesse gli importi. La gara del 2018 riguardava la fornitura di 8 *IMSI catchers* e la prestazione di alcuni servizi aggiuntivi (un corso di formazione, un help desk telefonico, eccetera); si è conclusa con un decreto di aggiudicazione (poi annullato per effetto d'un ricorso al TAR) per un prezzo complessivo di 4 milioni 700.000 euro e rotti, IVA esclusa. La gara del 2019 riguardava la fornitura di 3 *IMSI catchers* e d'un corso di formazione; si è conclusa con un decreto di aggiudicazione per un prezzo complessivo di 1 milione 800.000 euro e rotti, IVA inclusa.

Non mancano acquisti indirizzati a fini non investigativi; stando a quanto riferisce Belli (*DAP: nuovi beni e strumenti per la sicurezza degli istituti penitenziari*, in *https://www.gnewsonline.it/dap-nuovi-beni-e-strumenti-per-la-sicurezza-degli-istituti-penitenziari/*; Id., *Dal Dap 3 milioni e mezzo di euro per la sicurezza degli istituti*, in *www.gnewsonline.it/dal-dap-3-milioni-e-mezzo-di-euro-per-la-sicurezza-degli-istituti/*), nel 2019 il Dipartimento dell'amministrazione penitenziaria ha comprato due apparecchi per potenziare l'attività di controllo sull'osservanza del divieto di portare cellulari in carcere.

61. Cfr., per esempio, Colarieti, *Privacy, con Imsi Catcher caccia al cellulare in diretta: «Ora usato da polizia»*, in *il Fatto Quotidiano*, 13 giugno 2015; Id., *Tempi duri per gli evasori. La Guardia di Finanza acquista gli "Imsi catcher" per rintracciare i cellulari. Bando da due milioni per acquistare i primi 3 "cacciatori"*, in *www.lanotiziagiornale.it*.

stupefacenti, la polizia s'apposta nei dintorni dell'abitazione d'una persona sottoposta all'indagine, perlustra la zona con lo *Stingray*, recupera il codice IMEI del suo telefono e lo passa al pubblico ministero, che chiede ed ottiene l'autorizzazione ad intercettarlo. Sulla base degli esiti dell'intercettazione, è disposta un'ordinanza cautelare, poi confermata dal Tribunale della libertà. La difesa ricorre: per adoperare lo *Stingray*, dice, sarebbe servita l'autorizzazione d'un magistrato. Ma la Corte dissente.

Benché il discorso del giudice di legittimità sia molto stringato, si possono comunque isolare tre nuclei concettuali: la manovra non permette di scoprire il contenuto delle comunicazioni e non può quindi essere equiparata ad un'intercettazione (semmai, è un'attività «ad essa necessariamente prodromica»); inoltre, non raccoglie notizie sui contatti telefonici, «talché neppure potrebbe parlarsi, a ben vedere, di attività assimilabile all'acquisizione di tabulati»; in ogni caso, «non lede alcuno dei principi costituzionali o sovranazionali». La conclusione è nel senso che l'operazione dev'essere ricondotta agli atti investigativi atipici che la polizia giudiziaria può compiere di propria iniziativa[62].

Nessuno dei tre passaggi convince. Guardiamoli più da vicino, cambiandone l'ordine.

6. La Corte ha senz'altro ragione a chiedersi se questi nuovi strumenti d'indagine incidano valori protetti dalla Costituzione o dalle Carte dei diritti, ma ha il torto di chiudere fulmineamente una discussione che avrebbe meritato un andamento più disteso.

Ci si potrebbe anzitutto domandare se i codici IMSI e IMEI rientrassero fra i dati esteriori delle comunicazioni telefoniche e costituissero quindi informazioni protette dall'art. 15 Cost.[63]. Di per se stessi quei codici non accedono necessaria-

62. Cass., Sez. IV, 12 giugno 2018, n. 41385, in *Mass. Uff.*, n. 273929-01.

Nel senso che l'apparecchio possa essere usato senza autorizzazione dell'autorità giudiziaria anche Di Stefano, Fiammella, *Intercettazioni: remotizzazione e diritto di difesa nell'attività investigativa (Profili d'intelligence)*, 2a edizione, Milano, 2018, 215 s.

63. Secondo Corte cost., n. 81 del 1993, l'art. 15 Cost. abbraccia anche l'acquisizione dei dati che, senza rivelarne il contenuto, possono però portare all'identificazione dei soggetti delle comunicazioni nonché del tempo e del luogo delle stesse. Gran parte della dottrina concorda (Camon, *Sulla inutilizzabilità nel processo penale dei tabulati relativi al traffico telefonico degli apparecchi "cellulari", acquisiti dalla polizia senza autorizzazione dell'autorità giudiziaria*, in *Cass. pen.*, 1996, 3725 s.; De Leo, *Controllo delle comunicazioni e riservatezza*, in *Cass. pen.*, 2002, 2209 s.; Filippi, *L'intercettazione di comunicazioni*, Milano, 1997, 28 s.; Id., *Il rilevamento del "tracciato axe": una nuova denominazione per una vecchia tecnica d'indagine*, in *Giur. it.*, 1999, 1689; Id., *Il* revirement *delle sezioni unite sul tabulato telefonico: un'occasione mancata per riconoscere una prova incostituzionale*, in *Cass. pen.*, 2000, 3250 s.; Parodi, *Le intercettazioni*, Torino, 2002, 56; Potetti, *Corte costituzionale n. 81/93: la forza espansiva della tutela accordata dall'art. 15 comma 1 della Costituzione*, in *Cass. pen.*, 1993, 2744; Ruggieri, *Divieti probatori e inutilizzabilità nella disciplina delle intercettazioni telefoniche*, Milano, 2001, p. 87), anche

mente ad una chiamata e possono essere registrati anche quando il telefono è in *stand by*; come s'è detto, però, in molti casi – il procedimento che ha provocato l'intervento della Corte di cassazione ne è un esempio – essi vengono raccolti proprio allo scopo di rendere possibile un controllo sulle comunicazioni che saranno scambiate attraverso l'apparecchio monitorato. Si aggiunga che, quando sono in ballo diritti inviolabili, l'interprete ha, se così possiamo esprimerci, un "onere della prova attenuato": non è tenuto a dimostrare che una certa misura comprime una libertà fondamentale; per far scattare le tutele accordate dalla Carta, basta il dubbio. L'ha spiegato magnificamente la Corte costituzionale, in un passo di grande importanza e nobiltà: «la stretta attinenza della libertà e della segretezza della comunicazione al nucleo essenziale dei valori della personalità – attinenza che induce a qualificare il corrispondente diritto come parte necessaria di quello spazio vitale che circonda la persona e senza il quale questa non può esistere e svilupparsi in armonia con i postulati della dignità umana – comporta un particolare vincolo interpretativo, diretto a conferire a quella libertà, per quanto possibile, un significato espansivo»[64]. Tutto ciò potrebbe portare a concludere per l'applicabilità dell'art. 15 Cost.

Occorre tuttavia ammettere che gli *IMSI catchers* possono venire utili a molti altri fini. Abbiamo già accennato al pedinamento elettronico; un esempio ulteriore, anch'esso non raro[65], viene dalle indagini sul furto di telefoni: qui gli inquirenti vogliono scoprire chi ha l'apparecchio rubato; quali conversazioni vi faccia, con chi, dicendo cosa, non interessa. Dare la caccia agli IMSI può insomma servire a molte cose, non solo a controllare comunicazioni riservate. Perciò sembra ragionevole escludere che i codici identificativi dei telefoni e delle sim card facciamo parte dei dati esteriori delle comunicazioni salvaguardati dall'art. 15 Cost.

Se però s'allarga lo sguardo alle fonti sovranazionali, il panorama cambia. In effetti si stenta a credere che la Corte di cassazione abbia potuto affermare che un'operazione investigativa attraverso la quale si scannerizza di nascosto un territorio e si raccolgono tutti i codici IMSI o IMEI di tutti i telefoni di tutti coloro che si trovano lì, non interferisce con il diritto al rispetto della vita privata garantito dagli artt. 8 C.E.D.U. e 7 CDFUE. Può venire utile al riguardo una recente

se non mancano voci dissenzienti (Caprioli, *Colloqui riservati e prova penale*, Torino, 2000, 66 s. e 174; Diddi, *Tutela della* privacy *e acquisizione di tabulati telefonici*, in *Giust. pen.*, 1999, III, c. 622 s.; Di Martino, in *Le intercettazioni telefoniche*, Padova, 2001, 5; Idda, *I "dati esteriori" delle conversazioni telefoniche e la loro pretesa riconducibilità al concetto di comunicazione*, in *Giur. it.*, 2001, 1702 s.; Pace, *Problematica delle libertà costituzionali*, Parte speciale, 2a edizione, Padova, 1992, 251; Pannacciulli, *Le comunicazioni riservate tra nuove tecnologie e giustizia penale*, Bari, 2012, 102; Zaccarini, *Libertà e segretezza della corrispondenza (art. 15 della costituzione e art. 226 c.p.p.)*, in *Riv. pen.*, 1955, I, 451).

64. Corte cost., n. 81 del 1993.

65. Oltre alla pronuncia della Corte di giustizia citata nella nota successiva, si veda Thomas v. Florida, 127 So. 3d 658, 660 n.2 (Fla. Dist. Ct. App. 2013).

pronuncia della Corte di giustizia su un tema (non perfettamente identico ma) contiguo. La Corte è innescata nel corso d'una indagine spagnola su una rapina, nella quale era stato sottratto, fra l'altro, un cellulare; per individuare il responsabile, la polizia aveva chiesto al giudice istruttore d'ordinare ai fornitori dei servizi di comunicazione elettronica la trasmissione dei numeri di telefono attivati, nei giorni successivi alla rapina, sul codice IMEI del cellulare rubato, con i nomi dei relativi intestatari. Adesso non interessa l'oggetto della domanda di pronuncia pregiudiziale né il responso della Corte; importa un tassello del suo ragionamento: quella misura costituiva un'ingerenza nella sfera protetta dall'art. 7 CDFUE[66].

Se dunque andare alla caccia di IMSI significa comprimere il diritto al rispetto della vita privata, allora si dovrà farlo all'interno dei limiti fissati dalle Carte sovranazionali, fra i quali assume speciale importanza l'esigenza che la misura sia disposta «*in accordance with the law*» (art. 8 § 2 C.E.D.U.). Certo, sappiamo che, secondo la giurisprudenza elaborata a Strasburgo, il termine «*law*» abbraccia anche gli orientamenti giurisprudenziali; ma a condizione che siano stabili e tali da permettere all'interessato di pronosticare attendibilmente in quali casi potrà essere oggetto dell'ingerenza[67]. Qualora accogliessimo la tesi della Corte di cassazione: qualora, cioè, l'uso d'un *IMSI catcher* venisse ricondotto agli atti atipici di polizia giudiziaria, esso risulterebbe in definitiva consentito in qualsiasi indagine, su qualsiasi reato, in qualsiasi territorio, senza che dovesse ricorrere alcun presupposto: il requisito della prevedibilità della misura non sarebbe soddisfatto.

Un'ultima considerazione. Non c'è dubbio che il valore incrinato dalle indagini condotte con lo *Stingray* sia soprattutto il diritto al rispetto della vita privata, ed è dunque questo il tema sul quale conviene concentrare l'attenzione; non bisogna però dimenticare che, in alcune circostanze, potrebbero venire in gioco beni ed interessi ulteriori, anch'essi protetti da fonti collocate al vertice della scala gerarchica. Ripensiamo alle vicende nelle quali la polizia statunitense ha usato il marchingegno per controllare chi partecipava a manifestazioni politiche; in simili evenienze non dovremmo forse interrogarci sui rischi corsi dalla libertà di riunione (art. 17 Cost.) e da quella di manifestazione del pensiero (art. 21 Cost.)?

7. Anche se non ha mostrato alcuna consapevolezza dell'esigenza che il nostro mezzo d'indagine sia regolato dalla legge, la Corte di cassazione s'è comunque domandata se esso possa essere avvicinato ad istituti tipici. Un accostamento alle captazioni foniche è stato però escluso, perché cacciare gli IMSI è cosa diversa e meno grave dell'intercettare telefonate. Qui viene il dubbio che la Corte non ab-

66. Corte di giustizia UE, grande sezione, 2 ottobre 2018, causa C-207/16.

67. L'indirizzo è molto conosciuto e le citazioni potrebbero essere numerose; a titolo esemplificativo si può consultare Corte EDU, 2 settembre 2010, Uzun c. Germania, ric. n. 35623/05, § 62 (della versione inglese; in alcuni testi italiani, verosimilmente per una svista del traduttore, è il § 59).

bia compreso fino in fondo le potenzialità dello strumento: è eccessivo affermare che l'*IMSI catcher* attui «una sorta di controllo online per cui ogni attività del soggetto monitorato viene captata»[68]; è vero però che *alcuni* cacciatori di IMSI possono spingersi molto in là e certamente possono registrare il contenuto delle comunicazioni.

Non sappiamo quali apparecchi siano stati acquistati dai vari corpi di polizia[69], non sappiamo quale modello sia stato adoperato nel procedimento in cui s'è pronunciata la Corte e non vi sono ragioni per ipotizzare che la polizia giudiziaria l'abbia usato per fini ulteriori rispetto a quelli dichiarati; una cosa però la sappiamo: la Corte di cassazione ha sottovalutato la «*capacity for abuse*»[70] dello *Stingray*.

Eppure è un aspetto cruciale: in un celebre passo d'una celebre sentenza, la Corte costituzionale ha spiegato come il rispetto dell'art. 15 cost. postuli «garanzie che attengono alla predisposizione *anche materiale* dei servizi tecnici necessari per le intercettazioni [...], in modo che l'autorità giudiziaria possa esercitare *anche di fatto* il controllo necessario ad assicurare che si proceda alle intercettazioni autorizzate, solo a queste e solo nei limiti dell'autorizzazione»[71].

Il legislatore, dal canto suo, in qualche circostanza ha dimostrato di saper affrontare questi problemi: la disciplina sugli impianti che possono essere usati per fare le intercettazioni (odierno art. 268, co. 3 e 3-*bis*, c.p.p.) nacque nel 1974 (legge dell'8 aprile, n. 98), proprio per venire incontro alle richieste della Consulta. Più di recente, l'art. 2, co. 3, d.l. 30 dicembre 2019, n. 161 (al momento non ancora convertito), riprendendo un'indicazione già contenuta nella riforma Orlando (art. 1 comma 84 lettera e) n. 5 l. 23 giugno 2017, n. 103), ha affidato ad un

68. Così Nocerino, *Le intercettazioni e i controlli preventivi. Riflessi sul procedimento probatorio*, Milano, 2018, 154.

69. In qualche caso, i provvedimenti sulle gare d'appalto bandite dalle amministrazioni per l'acquisizione degli *IMSI catchers* tentano – a dire il vero, non senza tratti d'ambiguità – di lanciare messaggi tranquillizzanti. Si consideri il bando del 2019 (citato *supra*, nota 60); secondo il relativo capitolato tecnico (§ 3.1.16), «il sistema deve poter essere impiegato in modalità *man in the middle* tra la rete del gestore ed il terminale target (al riguardo si precisa che il sistema non verrà utilizzato per effettuare intercettazioni *on the air*)». A seguito di una richiesta di chiarimenti, l'amministrazione dirama f.a.q. nelle quali spiega che «il sistema [dev'essere in grado d'ottenere] i dati richiesti (IMSI/IMEI) senza l'intervento del gestore telefonico. Per "intercettazioni *on the air*" si intende l'ascolto in diretta e/o registrato delle comunicazioni tra cellulari. Si ribadisce che il Corpo non effettua intercettazioni telefoniche con gli apparati in acquisizione» (la documentazione citata è in *http://www.gdf.gov.it/repository/re.t.l.a/comando-generale/bandi-di-gara-e-contratti/anno-2019/acquisizione-di-n.-3-sistemi-di-monitoraggio-della-rete-cellulare/#null*). Mancano comunque – o almeno, chi scrive non è riuscito a rintracciarle – notizie che valgano per tutti gli strumenti attualmente in dotazione alle forze dell'ordine.

70. Così Norman (*Taking the sting out of the Stingray*, cit., 150). Si veda anche Benway (*You can run, but you can't hide*, cit., 281), il quale osserva che «*Stingrays produce a unique problem because of their ability to operate both as a pen register and as a wiretap device*».

71. Corte cost., n. 34 del 1973 (il corsivo è aggiunto).

decreto ministeriale il compito di stabilire i requisiti dei softwares che possono essere impiegati per le intercettazioni fatte con i captatori, precisando che questi requisiti devono «garantire che i programmi informatici utilizzabili *si limit[i]no all'esecuzione delle operazioni autorizzate*»[72].

Qualcosa del genere dovrebbe essere immaginato anche per gli *IMSI catchers*. Per esempio, si potrebbe prevedere che venissero dotati d'un software che, senza possibilità di essere disattivato, registrasse tutte le operazioni compiute, così da rendere possibili verifiche postume.

Naturalmente non può essere un giudice a stabilire tutto questo; ma, se non vuole cozzare frontalmente con le indicazioni della Corte costituzionale, un giudice non dovrebbe nemmeno lasciare carta bianca alla polizia, nell'attesa che tutto questo, prima o poi, venga stabilito.

8. La Corte di cassazione esamina infine un inquadramento nella disciplina sull'acquisizione dei dati relativi al traffico telefonico o telematico (art. 132 d.lgs. 30 giugno 2003, n. 196), ma scarta anche quest'idea; vale la pena riflettere brevemente sul ragionamento seguito e sugli esiti raggiunti; prima però servirà una precisazione.

Secondo le categorie adoperate dalla convenzione di Budapest sul *cybercrime* (art. 18 § 3 lett. a), i codici IMSI e IMEI rientrano fra le «informazioni relative agli abbonati». Le norma dettate al riguardo dai firmatari della convenzione cambiano di Stato in Stato: in alcuni Paesi l'acquisizione dei codici è sostanzialmente equiparata a quella dei dati di traffico; in altri valgono precetti meno severi[73]. Il nostro ordinamento appartiene al primo gruppo: infatti, in base all'art. 3 lett. e) punti 2.2.-2.5 d.lgs. 30 maggio 2008, n. 109, i codici IMSI e IMEI fanno parte dei dati che gli operatori di telefonia e di comunicazione elettronica devono conservare per le finalità di cui all'art. 132 del codice della *privacy*. Di conseguenza, gli organi delle indagini hanno due strade per procurarsi quelle informazioni: possono inoltrare una richiesta ai *providers* in base all'art. 132 cod. *privacy*; oppure possono adoperare un *IMSI catcher*[74]. Per battere la prima

72. Non è detto peraltro che il risultato sarà all'altezza delle aspettative: in passato è già stato emesso un decreto ministeriale a questi fini (d.m. giustizia 20 aprile 2018), con esiti tutto sommato deludenti. Su tale provvedimento, Conti, *La prova informatica e il mancato rispetto della* best practice*: lineamenti sistematici sulle conseguenze processuali*, in *Cybercrime*, diretto da Cadoppi, Canestrari, Manna, Papa, Torino, 2019, 1337 s.; Torre, *D.m. 20 aprile 2018: le disposizioni di attuazione per le intercettazioni mediante inserimento di captatore informatico*, in *Dir. pen. proc.*, 2018, 1255 s.

73. Cfr. Cybercrime Convention Committee, *Criminal justice access to data in the cloud: challenges. Discussion paper*, 26th may 2015 (in *https://rm.coe.int/1680304b59*), 8 e 19.

74. Inutile dire che stiamo parlando d'una alternativa teorica, che non si presenterà in tutti i procedimenti: per esempio, se le forze di polizia che conducono un'indagine non avessero *IMSI catchers* in dotazione, l'unica via sarebbe l'acquisizione del tabulato; se invece vi fossero motivi

servirebbe un provvedimento motivato del pubblico ministero; sulla seconda, invece, la polizia si potrebbe inoltrare da sola, senza bisogno del magistrato. Cosa giustifica la differenza?

Secondo la Corte di cassazione, l'acquisizione dei tabulati è più lesiva, perché rivela notizie ulteriori, ossia gli estremi (data, ora, luogo, durata, numero chiamante, numero chiamato…) delle comunicazioni fatte o ricevute dall'apparecchio sotto controllo; logico, quindi, che per essa valgano garanzie più robuste. Qui bisogna capirsi: è vero che, quando si domanda un tabulato, di solito si formula una richiesta generica, volta a conoscere *tutti* i dati di traffico relativi ad un abbonato; ma naturalmente non è vietato formulare una domanda più stretta, che punti ad estrarre soltanto alcune informazioni; per esempio, i soli codici identificativi d'un apparecchio. Se chi scrive non prende abbagli, anche in tal caso servirebbe il provvedimento motivato del pubblico ministero; eppure, l'iniziativa non sarebbe affatto più pesante di quella svolta con lo *Stingray*. Al contrario, è proprio l'*IMSI catcher* a mostrarsi più efficace da un lato, più temibile dall'altro. Più efficace perché, quando viene adoperato uno *Stingray*, nessuno, nemmeno i dipendenti delle compagnie telefoniche, è al corrente dell'operazione[75]; non ne restano quindi tracce, né si corre il rischio d'una fuga di notizie. Più temibile perché, come s'è notato, lo strumento è per sua natura incapace d'un controllo selettivo: setaccia e registra i dati di tutti gli apparecchi attivi in un certo territorio[76]. Abbiamo visto quanti fermenti, quante idee attraversino gli Stati Uniti, a livello federale e a livello statale, per arginare in qualche modo la forza cieca ed indiscriminata degli *IMSI catchers*.

Diversamente da quanto ritiene la Corte di cassazione, una disciplina che nell'un caso (l'acquisizione del tabulato) pretendesse il decreto motivato del magistrato, nell'altro (l'uso dello *Stingray*) lasciasse libera la polizia, non sarebbe dunque giustificata e presterebbe il fianco ad una censura alla luce dell'art. 3 Cost.

9. Dopo aver imperversato per decenni negli Stati Uniti, gli *IMSI catchers* sono sbarcati in Europa e da qualche anno vengono usati anche da noi. Non si sa tutto del loro funzionamento, perché le case costruttrici hanno steso un velo di riservatezza, ma alcune caratteristiche sono note e meritano di essere nuovamente segnalate: questi strumenti non possono stringere la sorveglianza su un obiettivo

per ritenere che la persona sottoposta alle indagini stesse adoperando una sim card o un telefono intestati ad uno sconosciuto prestanome, l'unica via sarebbe l'*IMSI catcher*.

75. Cfr. Hampton, *From smartphones to Stingrays*, cit., 171; Jonassen, *StingRays, Triggerfish, and Hailstorms*, cit., 1160.

76. Sul punto, alla letteratura statunitense già citata si possono aggiungere Di Stefano, Fiammella, *Intercettazioni: remotizzazione e diritto di difesa*, cit., 215 s. e Nocerino, *Le intercettazioni e i controlli preventivi*, cit., 152 s.

specifico: battono indiscriminatamente un territorio, raccogliendo i codici identificativi di tutti i telefoni che vi si trovano; inoltre, sono – almeno nel caso dei modelli più famosi – dotati d'una lunga serie di funzioni aggiuntive, che sotto alcuni aspetti li avvicinano ai captatori informatici.

Questi tratti aprono interrogativi formidabili; oltreoceano s'è sviluppato un dibattito teso, ricco d'intuizioni e di suggerimenti, che a poco a poco hanno cambiato, arricchendoli di garanzie, sia gli orientamenti giurisprudenziali sia la legislazione statale; di quel dibattito, però, in Italia non è arrivata nemmeno l'eco.

Così, nell'incuranza o nell'inconsapevolezza degli studiosi, il primo tentativo d'affrontare le questioni giuridiche poste dagli *Stingray* è venuto dalla Corte di cassazione, con esiti sotto tanti aspetti insoddisfacenti. S'avverte perciò il bisogno che la dottrina intervenga, s'impadronisca dell'argomento, cerchi di far nascere, prima, e di guidare, poi, la discussione. Le righe che precedono hanno tentato di muovere un passo in questa direzione.