review humanities and law intercultural <
CALUMET

CALUMET – intercultural law and humanities review
ISSN 2465-0145 (on-line)
ISSUE 26(2026)
For Info: www.calumet-review.com

Nicola Scerbo

# Il caso "*Paragon*". Rischi ed eterogenesi dei fini di un sistema informatico concepito per attività investigativa d'intelligence

**Abstract**
Recent developments in the Paragon case have reignited public attention on the use of particularly complex investigative tools, whose intrusive nature carries a significant risk of abuse by authorities, which could undermine the fundamental values of a democratic society. What makes this case unique is that the Graphite spyware appears to have been used by intelligence agencies not as part of the normal fight against criminal activity of particular social significance—for which the use of spyware would be considered legitimate—but rather for the covert surveillance of civil society activists and journalists. The private origin of the spyware—built and developed by an Israeli company composed by former government officials, officially for legitimate purposes only, and provided exclusively to government agencies for their national security activities—further complicates the case. This analysis, beginning with an examination and, where possible, a reconstruction of the facts in light of the limited evidence available, seeks to reconstruct the complex legal framework governing the use of surveillance tools—the careless use of which can cause significant harm to the constitutional order—with the aim of highlighting their specific uses, the reasons justifying their use, and their legitimate purposes, while also taking into account their significant technical characteristics. Given the evident complexity of the case, which is not without countless ethical and political implications, the technical analysis requires a careful assessment of the critical aspects relating to the abuse of authority. Given the evident complexity of the case, which is not without countless ethical and political implications, the technical analysis requires a careful assessment of the critical aspects related to the abuse of authority. In this regard, by reconstructing the facts surrounding the use of the Paragon software, this document aims to steer the discussion toward the potential dysfunction arising from the merging of the prerogatives typical of judicial investigative techniques with the specific characteristics of intelligence activities. This is a circumstance that exacerbates the already widespread uncertainty in defining the chain of responsibility should external parties—individuals motivated by private and economic interests, not without potential elements of fraudulent and misleading external influence—be introduced into the process within the framework of safeguards designed to protect those involved in the surveillance process. The European regulatory framework reflects the general approach to the issue of confidentiality, and national lawmakers have, quite rightly, taken steps to enact specific regulatory measures. However, the relevant policy guidelines reveal uncertainties and concerns that warrant careful further analysis looking ahead.

**Keywords**: Spyware – secret services – trojan horse – criminal law – security policies

**Abstract**
Le recenti vicende del caso *Paragon* hanno riacceso l'attenzione pubblica sull'impiego di strumenti investigativi particolarmente complessi e il cui potenziale intrusivo rappresenta un rischio significativo di abusi da parte delle autorità e di compromissione dei valori fondamentali di una società democratica. La peculiarità del caso è rinvenibile nel fatto che il *software* spia *Graphite* sembrerebbe essere stato impiegato da apparati dei servizi di

intelligence non nella regolare attività di contrasto a fenomeni criminali dal particolare allarme sociale per cui si riterrebbe legittimo l'uso dello *spyware,* bensì per l'occulta captazione di attivisti e giornalisti della società civile. L'origine privata dello *spyware*, costruito e sviluppato da una società israeliana composta da *ex* funzionari governativi, ufficialmente solo per scopi meritori ed esclusivamente fornita ad enti governativi per le loro legittime attività di garanzia della sicurezza nazionale, complica ulteriormente i profili del caso. L'analisi, partendo da una disamina e una possibile ricostruzione della vicenda, alla luce dei pochi elementi a disposizione, tenta di ricostruire il complesso quadro regolatorio dell'impiego di strumenti captativi il cui uso poco attento può determinare un significato *vulnus* per l'ordine costituzionale, cercando di risaltarne specificità d'impiego, ratio d'impiego e finalità legittime, senza estromettere la considerazione delle significative peculiarità tecniche.
Nella evidente complessità del caso, non scevra da innumerevoli ripercussioni di carattere etico e politico, l'analisi tecnica richiede attenta valutazione degli aspetti critici relativi ai fenomeni di abuso delle autorità. Il contributo, in tal senso, attraverso la ricostruzione dei fatti relativi all'impiego del *software* Paragon tenta di indirizzare il ragionamento sulla possibile disfunzione derivante dalla confusione di prerogative tipiche della tecnica investigativa giudiziaria con le peculiarità delle attività d'intelligence, esacerbando la già onnipresente incertezza nella definizione della catena di responsabilità, qualora dovessero introdursi nel processo soggetti esterni, mossi da interessi di carattere privatistico ed economico, non privo di potenziali elementi di eterodirezione fraudolenti e fuorvianti nel quadro delle garanzie verso i soggetti coinvolti dal processo captativo. Il quadro normativo europeo mostra l'orientamento sul tema della riservatezza ed il legislatore nazionale, a ragion veduta, non ha mancato di produrre interventi regolatori specifici, ma le relative linee di indirizzo politico non mancano di mostrare incertezze e perplessità che richiedono un attento approfondimento in prospettiva futura.

**Parole chiave**: Software spia – servizi segreti – cavallo di troia – diritto penale – politiche di sicurezza



## 1. Introduzione

Le vicende giudiziarie relative all' impiego dei moderni sistemi di captazione informatica, sia durante le attività investigative delle varie procure coinvolte nella normale attività di contrasto, accertamento e repressione dei reati che durante delicate attività di intelligence volte al contrasto del terrorismo internazionale ed interno, mostrano come lo strumento tecnologico si presti facilmente a fenomeni di abuso, poco inclini al rispetto del delicato equilibrio tra esigenza di tutela delle libertà fondamentali e le necessarie pratiche di contrasto ai variegati e complessi fenomeni criminali. Categorie criminologiche, dal particolare allarme sociale, hanno suscitano interventi del legislatore tesi sia a disciplinare che ampliare gli obiettivi ipotizzando l'uso di strumenti avanzati ed altamente intrusivi rendendo, allo stesso tempo, necessaria la costruzione di una architettura di pesi e contrappesi tra le differenti esigenze in gioco. Attori politici ed operatori del settore mostrano la consapevolezza circa le potenziali criticità in merito all' impiego di apparati tecnologici concepiti per affrontare fenomeni che

impattano sulla serena e regolare dinamica delle relazioni sociali. Le stesse, però, rischiano di generare una complicata eterogenesi dei fini, vulnerando il legittimo affidamento di corpi sociali impegnati nelle ordinarie attività della vita democratica. La volontà d'intervenire per confinare in specifici criteri applicativi gli strumenti interessati e, soprattutto, il margine di discrezionalità sulla scelta di priorità rispetto ad altre opzioni meno intrusive, nonché modalità operative concrete è sempre presenta tra i regolatori. Il recente caso Paragon, però, ha mostrato, nuovamente, evidenti falle alla radice del meccanismo tecnico di gestione dei diversi captatori e malware informatici, spesso e volentieri affidati alla creazione e gestione di società esterne di natura privata, prestando il fianco alle ipotesi, sollevate anche dagli addetti ai lavori, di eventuali ed inverosimili manomissioni fraudolente con ripercussioni assai inquietanti sul piano dell'architettura di un moderno Stato di diritto e le necessarie garanzie dei diritti fondamentali. Il contributo, attraverso una ricostruzione degli eventi storici e normativi sull' impiego del moderno captatore informatico, prova ad evidenziare criticità e perplessità crescenti sull'uso dello strumento, provando ad offrire al lettore un punto di vista complessivo sui rischi connessi, anche alla luce delle esperienze concrete della cronaca giudiziaria. E' evidente come casi analoghi, vista l'implementazione di tecnologie sempre più performanti e subdole, possano rappresentare la verosimile evoluzione di scenari teoricamente costruiti sulla base di valide e conformi motivazioni a carattere securitario, ma, allo stesso tempo, estremamente pericolose per la tutela di valori di riservatezza non soggetti a malcelate formule di compromesso o dissimulazioni di comportamenti degli apparati statuali non conformi ai sistemi di regolamentazione delle operazioni ad alto contenuto intrusivo. Il coinvolgimento di esponenti del contesto civile nell'ambito di operazioni che dovrebbero riguardare esclusivamente contesti di matrice militare o simili, è segnale quantomai allarmante circa la deriva concettuale e concreta dei paradigmi di appropriata gestione del potere. L'idea che l'accesso alla tecnologia di captazione possa essere condotto secondo parametri di difformità normativa o, peggio ancora, secondo criteri di opportunità personalistica e politica stimola l'attenzione degli operatori di settore e di tutti gli studiosi mossi dall'idea di evidenziare criticità e distorsioni evidenti, seppur nel contesto limitato del ragionamento accademico e teorico. D'altro canto, non è possibile esimersi dall'impegno di portare all'attenzione dell'opinione pubblica anomalie di sistema e fenomeni evidenti di abuso delle autorità, soprattutto, alla luce del sempre più efficace potenziale computazionale messo a disposizione delle autorità da parte di imprese e sviluppatori informatici. La convenienza economica, in tal senso, diviene sottospecie di un ben più pervicace ed intrusivo fattore di eterodirezione dei fenomeni sociali mediante strumenti creati per altri fini. La lotta alla criminalità o la tanto millantata ricerca della sicurezza collettiva non richiede l'uso improprio dei mezzi del potere e del sapere, ma comporta una responsabilità ulteriore e moralmente ed eticamente più elevata, in particolar modo se a determinarne gli scenari sono gli stessi che dovrebbero confinarne le derive. Il contributo, nell'ottica di una progressione continua sulla tematica oggetto di approfondimento, si pone quale utile strumento di approfondimento mediante la ricostruzione di un caso concreto ed emblematico, i cui effetti pratici e critici risultano ancora in divenire, non come elaborazione definitiva da cui attingere risposte certe, ma utile puntello per elaborazioni di appelli critici della comunità di studiosi.

## 2. L'eterogenesi dei fini nella difesa della sicurezza collettiva

Fin dall'emersione delle primissime tecnologie investigative, si è sempre posto il problema di un uso improprio degli strumenti in questione, generando apprensione sulle potenzialità intrusive di apparati molto potenti nell'ottica del contrasto ai fenomeni criminali interessati. Oggigiorno, con l'avvento dell'*AI* generativa ed i continui progressi nelle capacità tecnologiche di base, è indubbio come il principio cardine della riservatezza delle comunicazioni rischi di essere compromesso a riprova del pericolo costante è oramai evidente come lo strumento captativo, nelle sue innumerevoli declinazioni informatiche, sia divenuto il principale utensile nell'acquisizione occulta del materiale di comunicazione o conversazione tra soggetti. In pratica, le operazioni consistono nell'invasione della sfera privata del cittadino in deroga a quanto sancito dall'art. 15 della Costituzione[1]. L'ordinamento processuale penalistico italiano prevede una suddivisione a due delle categorie di intercettazioni: da un lato, le intercettazioni di conversazioni o comunicazioni telefoniche, informatiche o telematiche[2], dall'altro le c.d. intercettazioni ambientali[3]. Nel primo caso emerge la possibilità per gli inquirenti di captare, anche con software appositi, le comunicazioni e le conversazioni effettuate mediante telefono, fisso o mobile, ed i flussi di comunicazioni e dati trasmessi per via telematica e informatica. Per le seconde, invece, bisogna distinguere le comunicazioni tra presenti da quelle aventi ad oggetto conversazioni che, però, si svolgono nei luoghi di privata dimora[4]. In tal caso, alla riserva di legge e di giurisdizione, l'esistenza dei gravi indizi di reato e dell'assoluta indispensabilità alla prosecuzione delle indagini, si aggiunge l'ulteriore requisito del fondato motivo di ritenere che nel luogo di privata dimora si stia svolgendo l'attività criminosa. (c.d. captazione domiciliare). Tra le varie attività investigative, probabilmente, la fase delle indagini preliminari è quella che ha subito il condizionamento dell'evoluzione tecnologica e digitale in modo più impattante, al punto da giustificare ed introiettare l'impiego di applicativi molto complessi e con un notevole ventaglio di opzioni intrusive come l'accesso ai dati ed eventualmente una copia degli stessi, già memorizzati nel dispositivo del soggetto sottoposto alla rilevazione. Una delle caratteristiche principali del *software Graphite*, sviluppato dalla società Israeliana *Paragon solutions,* è, per l'appunto, la possibilità concreta di avviare la registrazione del traffico dati in arrivo o in partenza, la registrazione di telefonate e videochiamate, nonché, sempre a distanza, l'attivazione delle funzioni di microfono e/o telecamera indipendentemente dalla volontà dell'utente coinvolto. Di fatto, quello che avviene è una replicazione dell'apparato strumentale nelle mani degli operatori investigativi e da ciò si evince come gli interessi in gioco siano molteplici, generando un vero e proprio conflitto tra l'esigenza di tutela della riservatezza nella sfera privata e la necessità di contrasto ad attività criminose[5]. Le attività svolte nelle captazioni mediante un *keylogger* avvengono con l'impiego di uno strumento *hardware* o *software* in grado di effettuare la registrazione (*logging*) della tastiera di un *computer*, cioè, è in grado di intercettare e catturare segretamente tutto ciò che viene digitato senza che l'utente se ne accorga. Un *keylogger* di tipo *hardware* consiste in un "micro dispositivo elettronico a

[1] "La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge".
[2] *Ex* artt. 266, c.1, e 266-*bis* c.p.p.
[3] Di cui all'art. 266, c. 2, c.p.p.
[4] *Ex* art. 614 c.p.
[5] V. Cass. pen, SS. UU, 28 Aprile 2016, n. 26889.

cavetto, dall'aspetto simile a una prolunga, da collegarsi tra il cavo della tastiera e il *pc*, che riesce a catturare e memorizzare in un file di testo tutte le *password* e qualsiasi altro dato, come ad esempio gli indirizzi *web*, digitati sulla tastiera", il tipo *software* è "un programma spia o '*sniffer*' (annusatore) installato sul computer e in grado di tracciare e memorizzare in un file di *log*, nascosto all'utente, le attività svolte con il *pc*, catturando ad esempio le schermate video, i messaggi di posta elettronica, i numeri della carta di credito e così via. Spesso i *software* tipo *keylogger* vengono installati, all'insaputa dell'utente, tramite *worm* o *trojan* ricevuti attraverso l'*Internet* e che rimangono in esecuzione sul *pc* proprio per captare tutte le digitazioni (*password*, dati sensibili, numeri di carte di credito, identità ecc.) che avvengono su tastiera, registrarle e poi inviarle a un *computer* remoto spia, pronte per essere, in un secondo tempo, decodificate e usate" [6]. *Graphite*, nello specifico, è uno *spyware* di nuovissima generazione, sviluppato dalla società israeliana *Paragon solutions*, fondata nel 2019 da un gruppo di reduci dell'unità 8200 dell'esercito israeliano, corpo di *elite* altamente specializzato in cybersicurezza ed intelligence elettronica. La società, nelle cui posizioni di vertice ha visto sia *ex* comandanti dell'unità che l'*ex* primo ministro Ehud Barak, si è diffuso nel mercato dei captatori informatici attirando le mire dei capitali fino ad essere acquisita nel 2024 dall'americana *AE Industrial Partners* per centinaia di milioni di dollari. Il sofisticato *software* si infiltra subdolamente nei dispositivi interessati mediante quello che in gergo tecnico viene chiamato attacco *zero-click*, la cui peculiarità è di garantire l'accesso ai dati dell'utente senza richiedere alcun tipo di interazione con *file* o allegati ricevuti. Questo garantisce al fruitore del servizio un accesso completo al dispositivo, tra cui varie informazioni sensibili, contatti, messaggi di testo, *e-mail*, cronologia di navigazione o file multimediali. Il controllo da remoto, poi, garantisce agli operatori la possibilità di attivare a distanza ed in tempo reale microfoni o videocamere installate sul dispositivo, generando una vera e propria sorveglianza ambientale, reinviando tutti i dati captati in apposi *server* di controllo in chiave cifrata e molto difficili, se non impossibili, da intercettare a loro volta. La peculiarità del sistema consiste nella capacità di sfruttare vulnerabilità non note (*zero-day exploits*) per aggirare le protezioni dei sistemi operativi mobili, con particolare riferimento a *iOS* e *Android*, i principali diffusi sul mercato civile. Sfruttando soprattutto falle nelle diffusissime *app* di messaggistica istantanea (*Whatsapp, iMessage*, ecc.), *Graphite* inoltra nel destinatario pacchetti malevoli di codici, sfruttando anche autorizzazioni di sistema per ottenere un grado di accesso molto elevato ai dati, comportando rischi significativi per il rispetto di valori e principi fondamentali, in particolar modo del diritto alla *privacy*, alla libertà di espressione e, più in generale alla sicurezza delle informazioni personali[7]. Il fatto di cronaca ha avuto, comunque, il merito di rendere fruibile all'opinione pubblica il dibattito, un tempo riservato ad una ristretta cerchia di addetti ai lavori, sui potenziali abusi e deviazioni degli strumenti di indagine di nuova concezione tecnologica. Ha, evidentemente, condotto buona parte degli agenti interessati alla vicenda ad interrogarsi sulla pervasività di simili programmi informatici e sul rischio evidente di un uso improprio degli stessi. Professionisti ed esperti del settore hanno improvvisamente visto emergere un consistente interesse su argomenti di notevole importanza per gli aspetti più sensibili della vita di ciascun individuo. Tramite l'espediente amplificatore della comunicazione mediatica su un fatto di cronaca, l'attenzione dell'opinione pubblica si è concentrata

[6] V. il sito *online* di *Axerta investigation consulting*, https://alexasafesecurity.com/.

[7] L'accesso non autorizzato ai dispositivi personali costituisce una palese violazione dell'art. 8 della Convenzione europea dei diritti dell'uomo (CEDU), che tutela il diritto alla *privacy* e alla vita privata, e dell'art. 7 del Regolamento UE 2016/679 (GDPR). L'installazione di *spyware* senza il consenso dell'utente si configura inoltre come una violazione dell'art. 5 GDPR, che richiede la liceità, la correttezza e la trasparenza nel trattamento dei dati personali.

non più sul motivo primario delle attività di indagini, ovvero la ricerca della prova di un malaffare o fenomeno criminoso di particolare allarme sociale, quanto sullo strumento impiegato nell'attività svolta dagli investigatori e i rischi che gli stessi si tramutino in rampini al servizio del potere di turno per la intromissione ed interferenza illecita nel regolare svolgimento della vita democratica, in primis, del diritto di cronaca ed informazione giornalistica.

### 3. Elementi di oscurità gestionale nel caso Paragon

Fin da subito è sembrato evidente come l'uso del *software Graphite* rappresenti l'archetipo di un potere cognitivo estremamente efficace e pervasivo, uno strumento altamente efficiente, costruito prioritariamente per eludere i naturali meccanismi di difesa dei sistemi informatici, sempre più indispensabili nell'architettura della tecnologia di massa e negli apparati specialistici di aziende ed attori strategici. Crea molta perplessità il pensiero di uno strumento in grado di introiettare e rigettare gli elementi critici e le vulnerabilità di sistemi che neanche i loro stessi creatori hanno saputo identificare per tempo, quasi in una esternazione di indissolubile antinomia tra chi vuole operare per fini lodevoli e chi, invece, è subito pronto ad approfittare delle debolezze altrui, una specie di parabola discendente di biblica rievocazione. Senza entrare troppo nel merito della vicenda o, peggio ancora, in giudizi di valore soggettivistici, non adatti a questa sede, è indispensabile indirizzare il ragionamento sugli elementi materiali ed oggettivi afferenti alle criticità sorte nelle procedure di acquisizione dei dati, nonché alla loro gestione in capo agli attori coinvolti, laddove sono emerse evidenti incongruenze e rischi di interferenza illecita sulla genuinità e qualità degli elementi acquisiti[8]. Il tema delle intercettazioni e tutto il corollario di sistema è divenuto oggigiorno, in virtù del ruolo sempre più determinante di tale strumento nella conduzione di attività investigative delicate, uno degli elementi con cui è possibile misurare il livello di maturità dell'ordinamento giuridico nelle democrazie occidentali. Desta perplessità la pretesa del regolatore di implementare *standard* sempre più elevati di tutela dei dati da parte delle aziende, quando, allo stesso tempo, è reso possibile e legittimo, per alcuni impieghi specifici in deroga, il ricorso a strumenti in grado di *by*passare ogni meccanismo di difesa con estrema facilità[9]. Addetti ai lavori, più aperti all'introduzione di innovativi meccanismi di captazione, sostengono come tali mezzi investigativi siano funzionali alla prevenzione, accertamento e contrasto di gravi forme di criminalità; pertanto, in ragione della specificità del fine, si rende indispensabile un temperamento dei diritti di inviolabilità del domicilio e segretezza della corrispondenza tutelati rispettivamente dagli art. 14 e 15 Cost., contemperandoli e coordinandoli con il più generico interesse collettivo alla pubblica sicurezza ricompreso nell' obbligatorietà dell'azione penale *ex* art. 112 Cost., subendone, inevitabilmente, la compressione, seppur temporanea[10]. La postura non è nuova e in passato si è spinta fino al punto da legittimare operazioni materiali di installazione e disinstallazione da parte degli operatori completamente scardinate da oggettivi e predeterminati parametri di valutazione

[8] V. la Segnalazione al Parlamento e al Governo sulla disciplina delle intercettazioni mediante captatore informatico, del 30 aprile 2019 sul sito online del Garante per la protezione dei dati personali, https://www.garanteprivacy.it/home/docweb/-/docweb display/docweb/9107773.
[9] Sulla natura intrusiva di uno strumento informatico concepito ad arte e non dissimile da Graphite V. Sezioni Unite Scurato, Cass. n. 32428 del 24 settembre 2020.
[10] V. Filippi, (2020).

nell'adeguatezza e proporzionalità, ritenendole, per l'appunto, del tutto funzionali al fine specifico dell'attività investigativa con la possibilità di scelta delle modalità di esecuzione anche in assenza di indicazioni specifiche dell'autorità giudiziaria[11]. Dalle varie pronunce del passato, infatti, emerge come gli atti di autorizzazione all'impiego di strumenti captativi rendano superflua l'indicazione di concrete modalità operative cui attenersi, poiché la fase esecutiva non attiene più alla scelta dell'autorità giudiziaria di impiego dello *spyware*, bensì alla discrezionalità tecnica dell'operatore, sia esso polizia giudiziaria o servizio di intelligence, nelle operazioni materiali di installazione degli strumenti (*software*, *hardware, trojan*) idonee a dar vita, in concreto, alle intercettazioni. In effetti, apparati informatici molto complicati e innovativi come il *software Graphite* si prestano perfettamente ad una simile impostazione a maglie larghe, anche in virtù della loro complessità tecnica, coperta da segreto industriale e difficilmente comprensibile senza una specifica cognizione specialistica. Ci si immagini, per l'appunto, autorità giudiziarie o autorità delegate dei servizi alle prese con complicati formulari e manuali d'uso di algoritmi ed euristiche di sistema. Anche tra le frange dei vari nuclei specialistici risulta il più delle volte difficile arrivare a conclusioni univoche su risultati ed *output* di apparati in continua evoluzione ed aggiornamento, una su tutte L'*AI*. D'altro canto, non sono esattamente le vulnerabilità ancora sconosciute ad essere sfruttate da sistemi come *Graphite?* Vulnerabilità sconosciute anche ai rispettivi creatori, figurarsi ai manipolatori. Uno degli organi maggiormente interessati da tali considerazioni in ordine all'impiego di moderne tecnologie in ambito investigativo è il CNAIPIC (Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche) [12]. Disinteressarsi alla regolamentazione dettagliata delle modalità operative comporta una sorta di delega in bianco con la possibilità di discostarsi, senza particolari ripercussioni in termini di responsabilità, dal contenuto di qualsiasi provvedimento autorizzativo, sia esso proveniente da autorità giudiziaria che delegata[13]. Così, libertà domiciliare e segretezza delle comunicazioni, valori fondamentali per un ordinamento democratico, sono rimesse al "pieno e incontrollabile" potere di impiegare qualsivoglia modalità operativa di intercettazione senza che giudice, P.M. o altra figura responsabile dell'attività investigativa sappiano, volutamente o meno, se si è proceduto in modo legittimo. La conseguenza è che, oltre alla pericolosità implicita dello strumento di indagine, dovuta alla sua struttura e complessità tecnica, si aggiunge l'elemento di notevole incertezza nelle modalità di gestione delle procedure di inserimento, captazione e disinstallazione del *software* spia, nella maggior parte dei casi, in mano all'arbitrio degli operatori e, perciò, sconosciute agli organi giudiziari di direzione e controllo delle indagini. Il caso Paragon, d'altro canto, dimostra quanto le peculiarità delle attività investigative d'intelligence siano suscettibili di significativi margini d'incertezza regolatoria e conseguente aree di confine con gli strumenti investigativi classici. Spesso, avviene una forma di osmosi istruttoria tra i vari corpi operativi, se non un vero e proprio flusso informativo mediante canali non ortodossi e poco avvezzi al controllo esterno o gerarchico. Bisogna tenere conto anche della possibilità di interferenze illecite o fraudolente di attori esterni, soprattutto, qualora ci si affidi ad apparati tecnici estremamente sofisticati ed

[11] Si veda Cass., Sez. VI, del 23 giugno 2017, *Nobile*, n. 39403, Rv. 270941; Cass., Sez. VI, del 25 settembre 2012, *Adamo*, n. 41514 Rv. 253805. Al riguardo anche Cass., Sez. II, del 18 febbraio 2013, *Badagliacca*, n. 21644, Rv. 255541; Cass., Sez. I, del 2 ottobre 2007, *Biondo*, n. 38716, Rv. 238108; Cass., Sez. IV, del 28 settembre 2005, *Cornetto*, n. 47331, Rv. 232777. V. anche Cass., Sez. VI, del 13 giugno 2017, *Romeo*, n. 36874.

[12] V. sito ufficiale del CNAIPIC, https://www.poliziadistato.it/articolo/centro-nazionale-anticrimine-informatico-per-la-protezione-delle-infrastrutture-critiche.

[13] Con "autorità delegata" ci si riferisce alla figura della direzione e coordinamento dei servizi segreti D.I.S, afferenti al sistema di informazione della repubblica, S.I.S. In tal senso, V. il sito ufficiale, www.sicurezzanazionale.gov.it.

innovativi o di frontiera, soggetti ed erogati da apparati di sicurezza esteri o aziende del settore, più o meno libere nei fini e nei mezzi. Può succedere che alcune aziende del settore *tech*, sviluppatrici dei sistemi informatici di captazione siano condizionate in modo più o meno diretto nei fini di tutela della sicurezza collettiva dei rispettivi Stati sovrani e, in tal senso, un paese come Israele potrebbe tranquillamente rientrare nell'elenco, in virtù della sua storia contemporanea. Insomma, a conti fatti l'eterogenesi dei fini di strumenti investigativi così sofisticati non risiede tanto nel potenziale intrusivo del mezzo, quanto nel fine perseguito da utilizzatori ed eventuale attenzione dei regolatori o autorità di controllo. Per usare le parole di Bobbio, "non si capisce nulla del nostro sistema di potere se non si è disposti ad ammettere che al di sotto del governo visibile c'è un governo che agisce nella penombra... e ancor più in fondo un governo che agisce nella più assoluta oscurità... un potere invisibile che agisce accanto a quello dello Stato, insieme dentro e contro, sotto certi aspetti concorrente, sotto altri, connivente, che si vale del segreto non proprio per abbatterlo ma neppure per servirlo. Se ne vale principalmente per aggirare o addirittura violare impunemente le leggi... Del resto chi promuove forme di potere occulto e chi vi aderisce vuole proprio questo: sottrarre le proprie azioni al controllo democratico, non sottostare ai vincoli che una qualsiasi costituzione democratica impone a chi detiene il potere di prendere decisioni vincolanti per tutti i cittadini, se mai, al contrario controllare lo Stato senza essere a sua volta controllato[14]."

## 4. La sicurezza ed il compromesso di un equilibrio instabile tra i valori coinvolti

Gli elementi di cronaca suggeriscono come nel caso *Paragon* sia in corso la diffusione di informazioni sempre più dettagliate sulla natura dei soggetti coinvolti e sulle ragioni alla base di un impiego del sistema *Graphite* da parte delle autorità. Già il 31 gennaio 2025 la *bigtech Meta* rendeva pubblica la circostanza per cui, attraverso i suoi sistemi di rilevamento e controlli interni, aveva dovuto gestire una campagna di mitigazione di attività di spionaggio condotte sulla sua principale *app* di messaggistica (*Whatsapp*), condotta, presumibilmente, mediante l'impiego di un software prodotto dalla società Israeliana *Paragon Solutions*, inoltrando, allo stesso tempo, *alerts* ad un centinaio di persone coinvolte da operazioni intrusive, tra cui giornalisti e attivisti di una certa notorietà, sollevando un dibattito animato su tematiche inerenti gli aspetti di *privacy*, sorveglianza digitale e diritti fondamentali. Tra gli obiettivi del presunto spionaggio ci sarebbero anche dei cittadini italiani, tra cui Luca Casarini di Mediterranea *Saving Humans* e il direttore di *Fanpage*, Francesco Cancellato, il primo noto alle cronache per il suo attivismo in favore del fenomeno migratorio, l'altro, già Direttore di una testata giornalistica molto attiva nella produzione di inchieste critiche. Le incertezze iniziali circa il movente delle varie attività di captazione non hanno, allo stato, ricevuto complete spiegazioni e la stessa *Paragon Solutions* ha affermato di aver venduto la licenza d'uso ai vari Governi democratici interessati, tra cui Italia e Stati Uniti, solo ed esclusivamente per attività lecite di controllo dei fenomeni dal particolare allarme sociale, quali la lotta al terrorismo internazionale ed alla criminalità organizzata. Si tratta di attività d'impiego comunemente inquadrate in un uso etico di *software* dall'enorme potenziale intrusivo e potenzialmente lesivi di valori estremamente delicati, quali la libera determinazione degli individui coinvolti ed il rispetto della vita democratica nella sua interezza. In virtù della delicatezza del tema e, soprattutto, della

[14] Così, Bobbio, (2011).

strategicità di simili apparati, nell'ottica di equilibri sempre più precari di lotta tra potenze, la stessa *Paragon* non ha fornito molti dettagli sulle modalità di selezione dei propri clienti, né su eventuali verifiche condotte sull'utilizzo delle sue tecnologie. La stessa *Meta*, che per prima ha inoltrato gli *alerts*, sollevando il polverone mediatico, non ha saputo o potuto indicare specifici mandanti, ma ha sollevato dubbi sulla possibilità che si tratti di attori istituzionali e governativi; nell'incertezza del grado di pervasività del captatore e del suo grado di accesso ai sistemi coinvolti, ha suggerito ai vari clienti di distruggere qualsiasi dispositivo o apparato elettronico che si ritenga essere stato bersaglio dell'attività di spionaggio. La rivelazione delle presunte attività di spionaggio ha avuto subito un forte impatto politico in Italia, anche in virtù delle varie accuse di un coinvolgimento diretto delle autorità di pubblica sicurezza, in quanto fruitori del sistema *Graphite*, erogato a pagamento dalla *Paragon*, ufficialmente per fini legittimi nella regolare attività di garanzia dell'ordine democratico e della sicurezza nazionale, mediante accordi commerciali e convenzioni sottoposte al controllo di regolarità burocratica ed amministrativa. Sia il Ministero dell'interno che altri organi dello Stato, inquadrati nell'attività di gestione di forze armate e polizia giudiziaria, hanno immediatamente negato qualsiasi coinvolgimento in attività illecite o condotte fuori dai canoni di legittimità normativa o, peggio ancora, per fini di dossieraggio e controllo di particolari attori invisi ai vertici del potere statuale, ma la recente Relazione sull'utilizzo dello *spyware Graphite* da parte dei servizi di informazione per la sicurezza, approvata nella seduta del 4 giugno 2025, ha confermato l'impiego del *software* da parte dei servizi, dettagliando la ricostruzione dell'intera vicenda ed escludendo, almeno per il momento, l'impiego non adeguato dello stesso[15]. In effetti, se utilizzato da governi autoritari, *Graphite* potrebbe diventare uno strumento di repressione politica, consentendo la sorveglianza massiva di oppositori, attivisti e dissidenti. Questo scenario contrasta con i principi dello Stato di diritto e della democrazia, minando la stabilità sociale e la tutela dei diritti umani e la stessa società creatrice del software, d'altro canto, si è sempre professata quale mero strumento etico al servizio di legittime finalità di contrasto ad attività lesive del sereno svolgimento della vita democratica e non quale facile *escamotage* tecnico di abuso contro oppositori o avversari politici. Il caso *Paragon* e lo *spyware Graphite*, attraverso il loro enorme impatto mediatico, rappresentano un punto di svolta cruciale nel già acceso dibattito internazionale sulle tematiche inerenti alla sorveglianza digitale e la protezione dei diritti fondamentali. Le implicazioni giuridiche, tecniche e sociali sono innumerevoli e richiedono, da parte degli attori coinvolti e dei corpi sociali tutti, un'analisi approfondita per delineare possibili scenari futuri e strategie di mitigazione efficaci. Il tema della sicurezza nazionale riecheggia sempre nelle attività condotte contro attori ritenuti potenzialmente distruttivi dell'ordine precostituito e disturbanti del legittimo affidamento alla pubblica incolumità e, tuttavia, lo stesso argomento subisce anche innumerevoli torsioni al ribasso, il più delle volte, funzionali alla creazione di un ombrello di copertura per giustificare anche il mancato rispetto di valori della persona umana e i diritti fondamentali, nell'ottica di un equilibrio precario e sul filo del rasoio. Il caso *Paragon*, anche questa volta, stimola la riflessione sulla necessità di adottare leggi chiare in merito ai temi della sorveglianza digitale, con gli Stati Ue che dovrebbero regolamentare in modo chiaro e trasparente le concrete modalità operative d'impiego di strumenti come *Graphite*, seppur nell'eccezionalità delle circostanze, onde garantire una supervisione indipendente da parte di autorità specifiche che ne possano garantire un uso conforme al rispetto dei principi dello Stato di diritto. Nel nostro ordinamento esistono diverse criticità già espresse in passato per l'impiego di strumenti simili al

[15] Per l'analisi approfondita si rinvia al testo della relazione rinvenibile negli atti parlamentari della camera sul sito https://documenti.camera.it/_dati/leg19/lavori/documentiparlamentari/IndiceETesti/034/004/INTERO.pdf.

*software Graphite*. Già nella nota Sentenza *Prisco*, si paventava la possibilità di attivare la videocamera del dispositivo in cui è inoculato un *virus* spia. Esso, infatti, è riconducibile alla videoripresa, consentita nei limiti stabiliti dalla sentenza[16], mentre, le comunicazioni avvenute mediante le applicazioni di messaggistica online sono riconducibili alle intercettazioni telematiche *ex* art. 266-bis c.p.p.[17] Inoltre, considerata l'assenza del principio di tassatività della prova, nel nostro ordinamento, è possibile ammettere prove non espressamente disciplinate dalla legge[18]. Addirittura, sull'uso dei *Trojan Horse*, nella già citata sentenza della Cassazione, Sez. V, 30 settembre 2020, (dep. 11 novembre 2020), n. 31604, la Corte si spinge ad affermare che il captatore *"non esercita alcuna pressione sulla libertà fisica e morale della persona, non mira a manipolare o forzare un apporto dichiarativo, ma, nei rigorosi limiti in cui sono consentite le intercettazioni, capta le comunicazioni tra terze persone, nella loro genuinità e spontaneità"* escludendone anche la riconducibilità dello strumento di indagine a metodi e tecniche idonee ad influire sulla libertà di determinazione del soggetto *ex* art. 188 c.p.p. Sarebbe la natura "subdola" di uno strumento di captazione di questo tipo, proprio in quanto segreto nel suo dinamismo operativo, la principale garanzia dell'integrità del processo di autodeterminazione del soggetto sottoposto ad attività investigativa, poiché, all'oscuro del controllo esercitato sul suo dispositivo, tenderà ad assumere un atteggiamento naturale non soggetto ad agenti di influenza esterni. Alcuni autori ravvisano forme di violazione del principio del *nemo tenetur se detegere* mediante l'attività di inoculazione dei captatori operata per via della inconsapevole agevolazione del destinatario realizzate con le operazioni di download esca nelle applicazioni vulnerate. In tal caso, il principio posto a tutela del destinatario di attività investigative sarebbe da intendersi non solo come diritto a non rendere dichiarazioni autoincriminanti, ma anche come diritto a non compiere azioni autoincriminanti, le stesse come conseguenza svilente della libertà morale dell'individuo[19]. Nelle sue pronunce, la Cassazione, chiamata ad esprimersi sull'appropriatezza dell'uso del *trojan*, ha ribadito come nel caso in cui con il captatore informatico (ciò potrebbe valere anche per *software* analoghi come *Graphite*) si arrivasse ad effettuare intercettazioni invalidate dall'inutilizzabilità (ad esempio quelle intercorrenti tra l'imputato ed il suo difensore) oppure si arrivasse ad attività lesive della dignità umana, ciò non inciderebbe necessariamente sulla legittimità del decreto autorizzativo, in quanto comporterebbe nell'onere motivazionale del giudice o altra autorità un requisito non previsto dalla legge. La Corte sostiene che le eventuali situazioni patologiche trovino adeguata copertura nelle disposizioni contenute all'art. 271 c.p.p. secondo cui non sarebbero utilizzabili le risultanze di specifiche intercettazioni "qualora le stesse siano state eseguite fuori dei casi consentiti dalla legge o qualora non siano state osservate le disposizioni previste dagli articoli 267 e 268 commi 1 e 3". Non sarebbero utilizzabili "i dati acquisiti nel corso delle operazioni preliminari all'inserimento del captatore informatico sul dispositivo elettronico portatile e i dati acquisiti al di fuori dei limiti di tempo e di luogo indicati nel decreto autorizzativo" e non possono essere utilizzati, inoltre, "le intercettazioni relative a conversazioni o comunicazioni delle persone indicate nell'articolo 200 comma 1, quando hanno a oggetto fatti conosciuti per ragione del loro ministero, ufficio o professione, salvo che le stesse persone abbiano deposto sugli stessi fatti o li abbiano in altro modo divulgati"[20]. Sempre secondo la Corte, *"la necessità dell'indicazione di uno specifico luogo –*

[16] Cass., S.U., del 28 marzo 2006, Prisco, *in Riv. it. dir. e proc. pen.*, 2006, 1537.
[17] V. Guarnera, (2016: 1: 212 ).
[18] *Ex* art. art. 189 c.p.p.
[19] V. Signorato, (2018: 238).
[20] Così sempre Cass., Sez. V, del 30 settembre 2020, (dep. 11 novembre 2020), n. 31604.

*quale condizione di legittimità dell'intercettazione – non risulta imposta né dall'art. 266 c.p.p., comma 2 (in cui, con riferimento all'intercettazione di comunicazioni tra presenti, vi è solo la previsione di una specifica condizione per la legittimità dell'intercettazione se effettuata in un luogo di privata dimora), né dalla giurisprudenza della Corte EDU*". Di conseguenza, "devono ritenersi legittime le intercettazioni 'tra presentì eseguite a mezzo di captatore informatico installato su un dispositivo portatile, nell'ambito dell'attività investigativa svolta in relazione a procedimenti di criminalità organizzata e ciò prescindendo dalla preventiva individuazione ed indicazione dei luoghi in cui la captazione deve essere espletata". Chiamando in soccorso le parole di Murone, "nell'ambito dei procedimenti aventi ad oggetto i c.d. 'reati comuni' sono proprio le considerazioni sulla struttura del mezzo probatorio a fare emergere un profilo di incompatibilità fra l'utilizzo dello strumento tecnico del captatore informatico e l'applicazione della disciplina sulle intercettazioni, atteso che nell'ambito di tali procedimenti non si riuscirebbe a dare attuazione alla clausola prevista dall'art. 266, comma 2, c.p.p. a tutela del domicilio e posto che, se anche fosse tecnicamente possibile seguire gli spostamenti dell'utilizzatore del dispositivo elettronico e sospendere la captazione ove quest'ultimo facesse ingresso in luogo di privata dimora, ne risulterebbe comunque impedito il controllo dell'organo giudicante al momento dell'autorizzazione. Lo scenario, tuttavia, cambia decisamente in relazione ai delitti di criminalità organizzata. Per tali più gravi delitti, infatti, è certamente ragionevole pensare che il legislatore – in considerazione dell'eccezionale gravità e pericolosità delle minacce derivanti alla società e ai singoli dalle articolate organizzazioni criminali che dispongono di sofisticate tecnologie e di ingenti risorse finanziare – abbia voluto operare uno specifico bilanciamento di interessi, optando per una più pregnante limitazione della segretezza delle comunicazioni e della tutela del domicilio"[21].

## 5. Il captatore come chiave di volta nel contrasto alla criminalità internazionale

Già il d.lgs 29 dicembre 2017, n. 216 c.d. Orlando, aveva disciplinato per la prima volta l'utilizzo del captatore informatico (*trojan horse*), come strumento di ricerca della prova solo per il perseguimento dei gravi reati di criminalità organizzata e terrorismo. Per quanto attiene ai reati comuni, invece, è stato escluso l'impiego del *virus* spia in quanto, nell'impossibilità di elaborare preventivamente una lista dettagliata di tutti i potenziali luoghi di privata dimora in cui il *software* potrebbe essere impiegato, diverrebbe impossibile rispettare le condizioni di legittimità previste dall'impianto del codice di rito. Le Sezioni Unite, con la sentenza 28 aprile 2016, n. 26889 (*Scurato*), avevano già legittimato l'utilizzo del nuovo strumento di indagine per il compimento di attività investigative mediante intercettazioni "tra presenti", ma solo nei casi di procedimenti contro la criminalità organizzata. Molti dubbi erano stati sollevati in merito alla possibilità di una deriva elastica nei criteri di utilizzabilità del *software* e la Corte aveva evidenziato la "forza intrusiva" dello strumento con la conseguenza logica che "la qualificazione del fatto di reato, ricompreso nella nozione di criminalità organizzata, dovesse risultare ancorata a sufficienti, sicuri e obiettivi elementi indiziari, evidenziati nella motivazione del provvedimento di autorizzazione in modo rigoroso". Pertanto, nel rispetto dell' ineludibile contemperamento tra esigenze di tutela della sicurezza collettiva (da preservare) ed il rispetto delle libertà fondamentali (potenzialmente violate) un ruolo determinante è rappresentato dal provvedimento di autorizzazione

[21] V. Murone (2021).

dell'organo competente il quale riveste "una fondamentale funzione di garanzia, spiegando le ragioni dell'assoluta indispensabilità dell'atto investigativo e indicando con precisione quale sia il criterio di collegamento tra l'indagine in corso e la persona da intercettare"[22]. Già qualche anno fa, un caso simile a quello rappresentato dall'impiego di *Graphite* aveva sollevato non poche perplessità in merito alla possibilità che gli strumenti in questione, così sofisticati, non avessero un inquadramento ben definito e una catena di controllo specifica in capo alle autorità competenti, fino al punto da comprometterne il legittimo affidamento. È noto, ad esempio, il caso dei dati raccolti con il *malware Exodus*, i quali finivano su *server* negli Stati Uniti, accessibili da qualsiasi dispositivo e *browser*, in una sorta di *caveau* da cui ottenere informazioni sensibili per attività di dossieraggio. Gli Stati ed i loro apparati di sicurezza, infatti, si affidano spesso a società private per l'installazione e la cura dei captatori informatici, rendendo, in tal modo, molto più permeabile la filiera su cui si snoda l'attività di indagine, in virtù del coinvolgimento di una pluralità di soggetti, spesso privi dei requisiti professionali, organizzativi e persino dell'affidabilità, necessari per svolgere attività così delicate e sensibili. Le non trascurabili opportunità messe a disposizione dall'emergere delle nuove tecnologie, si pensi su tutte l'*AI*, deve essere sempre oggetto di costante attenzione e monitoraggio da parte del decisore chiamato a valutarne la possibilità di impiego nel contrasto ai fenomeni criminali, soprattutto, in virtù della contestuale potenzialità intrusiva e lesiva dei diritti fondamentali delle persone coinvolte, difficilmente rimediabili una volta compromessi. *Software* come *Graphite,* in linea teorica molto utili per l'attività di contrasto alla mafia, al terrorismo e alla corruzione, corrono il rischio di divenire, in assenza di un adeguato controllo esterno, strumenti di sorveglianza di massa o, peggio ancora, meccanismi subdoli per il controllo del giornalismo critico minando così valori come la libertà di espressione, garantita dall'art. 21 della Costituzione italiana e dall'art. 11 della Carta dei diritti fondamentali dell'Unione europea. Molti giornalisti, infatti, nel timore di poter essere intercettati, potrebbe adottare meccanismi difensivi di autocensura, vulnerando un elemento cardine della libertà di informazione e dell'interesse pubblico ad essere costantemente aggiornati sui fatti più rilevanti della vita civile. Un *software* come *Graphite*, molto più intrusivo dei normali apparati di intercettazione telefoniche o ambientali, spia le attività del *target*, ma anche di soggetti terzi estranei, rendendo possibile l'accesso ad un insieme di dati sensibili contenuti nel dispositivo infettato quali foto, video, *mail*, messaggi e *password* di ogni genere. L'utilizzo dell'espediente legato al contrasto ad attività criminali dal particolare allarme sociale, quali terrorismo e criminalità organizzata, non può rappresentare un *passe-partout* per ogni tipo di attività investigativa, a maggior ragione, se attuata da specifici apparati dello Stato. Come già detto, nelle mani di operatori sconsiderati o poco attenti agli equilibri dello Stato di diritto, strumenti sofisticati come *Graphite* potrebbero diventare facilmente meccanismi di indiretta repressione politica, consentendo la sorveglianza e il controllo massivo di oppositori, attivisti e dissidenti. I recenti fatti di cronaca hanno avvalorato i timori di chi si rende portatore di perplessità e riserve in merito agli usi impropri degli attrezzi del mestiere senza adeguate contromisure degli organi di controllo. L'Unione europea, dal canto suo, potrebbe implementare strumenti normativi adeguati adottando, così come già fatto con l'*AI Act* sull'intelligenza artificiale o nel Regolamento sui sistemi a doppio uso, un approccio molto più rigido nei confronti di *spyware* commerciali limitando vendita, esportazione ed impiego di tecnologie con potenziale di sorveglianza avanzato. Anche la possibile introduzione di liste nere dedicate a specifici strumenti nel contesto dell'UE, a maggior ragione se prodotti da società private riconducibili a contesti

[22] V. Bosco (2012).

geografici in cui vigono regimi non perfettamente democratici e scarsa tutela dei diritti umani. Allo stesso tempo, potrebbe essere valutata una modifica sostanziale del GDPR, Regolamento (UE) 2016/679, includendo specifiche disposizioni normative per gli *spyware* associate ad un sistema sanzionatorio in grado di deflettere e generare una deterrenza significativa contro le potenziali violazioni del sistema regolatorio. Un ruolo significativo di responsabilizzazione, dovrebbe, però, essere giocato dalle *bigtech* come *Meta, Google, Apple, ecc.*, le quali potrebbero rendersi protagonisti di una *compliance* aziendale efficace per integrare, nelle loro valutazioni di impatto sull'uso dei dati, specifiche misure volte a mitigare i rischi interni nell'uso di *spyware.* Il costante e proattivo dialogo con le autorità competenti dovrebbe spingere le aziende tecnologiche coinvolte a segnalare per tempo eventuali segnali di violazioni in atto, rendendo più facile e spedite le attività di contrasto degli abusi. Un ruolo determinante è giocato dal fattore educativo e relativo substrato culturale di riferimento, laddove si rende indispensabile un coinvolgimento proattivo delle masse di utenti delle varie piattaforme di comunicazione mediante campagne di informazione e sensibilizzazione al riconoscimento tempestivo dei vari segnali di accesso e compromissione dei propri sistemi.

## 6. Il segreto di Stato e la sua rilevanza per il caso Paragon

In seguito all'avviso di attacco informatico inoltrato dalla società *Meta* al collaboratore della ONG *Mediterranea Saving Humans,* si è palesata una certa confusione in merito alla gestione di presunti atti secretati riguardanti il caso, per i quali, in un primo momento era stata negata la possibilità di aggiungere altri elementi, oltre a quelli forniti in via ufficiale dal Ministro per i rapporti con il Parlamento, in quanto appartenenti alla categoria di protezione come "classificati", ovvero, secretati. L'ultima relazione del Copasir chiarisce molti degli aspetti legati alla vicenda, ma, nelle prime fasi, l'incertezza e le legittime riserve delle parti interessate hanno spinto molti ad approfondire il tema del Segreto di Stato. In effetti, la nota del ministero interessato indicava come la vicenda sia "stata ed è oggetto di audizioni presso il Copasir", aggiungendo che "ogni altro aspetto delle vicende di cui trattasi deve intendersi classificato e, ai sensi dell'articolo 131, comma 1 del regolamento della Camera, anche se richiamato in futuri atti non potrà formare oggetto di informativa da parte del governo se non nella sede del Copasir". Una parziale ricostruzione della vicenda potrebbe dare qualche indicazione maggiore sul paino interpretativo, nonostante la disciplina sul segreto di stato risenta di molte riserve tecniche derivanti dalla specialità della materia. L'approfondimento del caso Paragon, in tal senso, può divenire un utile caso di studio da cui attingere vulnerabilità sistemiche afferenti al comparto della sicurezza collettiva e delle attività di prevenzione tipiche degli apparati d'intelligence. L'uso di strumenti innovativi ed altamente pervicaci è caratteristica intrinseca delle modalità operative del settore e, tuttavia, la tecnica informatica ha notevolmente incrementato il potenziale intrusivo dei meccanismi di ricerca informativa da parte degli operatori d'intelligence. Il caso *Paragon* rientra nelle prerogative dell'autorità delegata alla Sicurezza della Repubblica e, pertanto, con funzioni di controllo dell'attività dei servizi segreti per conto della Presidenza del Cons la legge 124 del 2007. Una nota dell'autorità delegata, in effetti, ha ribadito la natura della vicenda, chiarendo come "ogni altro aspetto" inerente alla vicenda *Paragon* dovesse "intendersi classificato" e non avrebbe potuto "formare oggetto di informativa da parte del governo se non nella sede del Comitato parlamentare per la sicurezza della Repubblica (Copasir)". La comunicazione, in linea teorica, precludeva la possibilità di ulteriori

interrogazioni sul caso da parte delle opposizioni durante il successivo *question time* previsto il 19 febbraio, adducendo l'ulteriore elemento preclusivo dettato dall'art. 131 del regolamento della Camera, in base al quale "il Governo può dichiarare di non poter rispondere" a un'interrogazione parlamentare specificandone, però, il motivo. Il 18 febbraio, durante una riunione dei capigruppo alla Camera, il Governo ha poi cambiato versione, dichiarandosi disponibile a rispondere alle interrogazioni parlamentari, a condizione che si eliminassero richieste specifiche in merito al caso *Paragon* e al conseguente uso del *software Graphite*. Il caso *Paragon* è stato, inoltre, impiegato come espediente delle minoranze parlamentari al fine di acquisire maggiori informazioni, soprattutto, sul generale uso delle intercettazioni nonché dei relativi costi da parte del Ministero della Giustizia, mediante finanziamenti al reparto dell'amministrazione penitenziaria (DAP), e, più nello specifico, ai nuclei speciali Gruppo operativo mobile (GOM) e del Nucleo investigativo centrale (NIC). Il ruolo determinate nella vicenda ruota intorno alla definizione di "classificato" e ciò che ne comporta sul gradiente di segretezza riguardo al documento. Come si può leggere sul sito governativo del sistema d'informazione per la sicurezza della Repubblica, il segreto di Stato "è un vincolo posto dal presidente del Consiglio dei ministri" su "atti, documenti, notizie, attività e ogni altra cosa la cui diffusione sia idonea a recare danno all'integrità della Repubblica, anche in relazione ad accordi internazionali, alla difesa delle istituzioni poste dalla Costituzione a suo fondamento, all'indipendenza dello Stato rispetto agli altri Stati e alle relazioni con essi, alla preparazione e alla difesa militare dello Stato"[23]. Secondo la legge n. 124 del 2007, la quale disciplina il funzionamento e le prerogative dei servizi di sicurezza, il potere di apposizione od opposizione del segreto da parte della presidenza del Consiglio dei ministri non può riguardare qualsiasi argomento, ma, piuttosto, non possono essere secretate "notizie, documenti o cose relativi a fatti di terrorismo o eversivi dell'ordine costituzionale"[24]. L'apposizione del segreto, come si evince dalla declinazione normativa, è, infatti, un atto politico che può essere disposto esclusivamente dal presidente del Consiglio dei ministri[25]. Oltre al generico segreto di Stato apponibile dalla figura del presidente del Consiglio, esistono, tuttavia, ulteriori gradi di classificazione le cui prerogative di esercizio riguardano le diverse autorità, di volta in volta, coinvolte dall'esercizio del potere afferente alle tematiche della sicurezza nazionale. E coì si possono avere i differenti gradi e livelli crescenti di riservatezza come: riservato (R), riservatissimo (RR), segreto (S) e segretissimo (SS)[26]. Le relative classifiche sono attribuibili dai "soggetti originatori dell'informazione", come "le pubbliche autorità e gli operatori economici, in possesso di abilitazione di sicurezza industriale, che fanno parte dell'organizzazione nazionale di sicurezza"[27]. La normativa chiarisce come "la classifica di segretezza è apposta, e può essere elevata, dall'autorità che forma il documento, l'atto o acquisisce per prima la notizia, ovvero è responsabile della cosa, o acquisisce dall'estero documenti, atti, notizie o cose"[28]. Nel caso specifico, la relativa classifica di segretezza avrebbe potuto trovare origine in qualche struttura ministeriale coinvolta nelle varie fasi. Chi, dando vita al documento interessato, ne assegna anche la relativa classifica di segretezza in virtù della rilevanza, della tutela di particolari interessi nazionali, di conseguenza, limita allo stesso tempo

[23] V. definizione completa sul sito www.sicurezzanazionale.gov.it.
[24] Così all'art. 39, comma 11 della legge 3 agosto, n.124 del 2007
[25] Così all'art. 39 della legge 124 del 2007.
[26] V. comma 3 dell'art. 42 della legge 124 2007.
[27] V. lo schema esemplificativo presente sul sito ufficiale dei servizi di sicurezza al seguente indirizzo: www.sicurezzanazionale.gov.it.
[28] Così al comma 2 dell'art. 42 della legge 124 2007.

l'accesso alle informazioni contenute nel documento a una ristretta cerchia di soggetti che abbiano effettiva necessità di conoscere le informazioni ivi contenute e in ragione e nell'esercizio delle proprie funzioni; gli stessi devono essere adeguatamente informati in merito alla regolare gestione, conservazione e tenuta dei documenti, nonché muniti di specifica abilitazione. Inoltre, elemento prioritario e funzionale alla corretta gestione dei vari livelli di segretezza è che l'attribuzione di una relativa classifica preveda contestualmente l'implementazione di un sistema di misure idonee ad assicurare che la limitazione dell'accesso sia effettivamente realizzata. Da ciò si evince come a ciascun livello di classifica, dovrebbe corrispondere anche una serie di prescrizioni parallele, tese a garantirne l'efficace e concreta protezione (sistemi di conservazione e di riproduzione), proporzionata alla rilevanza dell'interesse tutelato. Alla luce del sistema delle prescrizioni normative afferenti al segreto di Stato, una qualche forma di formalizzazione dei vari passaggi deve pur essere messa a disposizione e non appare sufficiente, qualora dovesse essere sostenuta dalle parti, almeno alla corte dei più attenti al garantismo, una superficiale affermazione di circostanze segrete, fondamentali per il rispetto della sicurezza nazionale, senza ottemperare alla regolare esecuzione di procedure e protocolli formali necessari a garantire la sicurezza nazionale tanto di cui la normativa si fa portatrice. Un ruolo di raccordo e garanzia a rigor di norma, spetterebbe prioritariamente alla figura politica della presidenza del Consiglio[29]. D'altro canto, situazioni come il caso Paragon mostrano quanto il rischio di una eterogenesi dei fini sia sempre dietro l'angolo. Nonostante le lodevoli e legittime prerogative delle autorità preposte alla garanzia della sicurezza collettiva, la possibilità che un uso improprio e fuori luogo dei poteri investigativi afferenti alle specifiche esigenze del comparto d'intelligence è foriera di notevoli ripercussioni sulla tenuta ed il rispetto dei valori di affidabilità reciproca tra società civile ed organi di tutela della sicurezza collettiva. In soccorso, è utile ricordare le parole di Bobbio, il quale non esclude gli "*arcana imperii*" dalla forma di governo democratico, ma, contestualmente, ne precisa i limiti applicativi, laddove afferma che "la democrazia avanza e l'autocrazia retrocede via via che il potere diventa sempre più visibile e gli arcana imperii, i segreti di Stato, da regola diventano eccezione, un'eccezione accolta in ambiti sempre più ristretti e tassativamente stabiliti"[30].

## 7. Gestione pratica dei sistemi di captazione informatica

Dal momento che il fattore umano assurge a ruolo determinante nella gestione delle tecnologie di ogni tipo, è opportuno chiedersi se esso debba semplicemente limitarsi alla sola scelta di obiettivi e monitoraggio del sistema, oppure debba spingersi sino al punto da compromettere le reali prestazioni e potenzialità dello strumento impiegato. Il dilemma non è di facile risoluzione, per cui è ipotizzabile che venga affinata, di volta in volta, una significativa rimodulazione dinamica. Si considera del tutto diverso l'impiego dei sistemi di captazione nelle attività di contrasto a fenomeni criminali di particolare allarme sociale, quali la lotta al terrorismo internazionale e criminalità organizzata, rispetto a usi finalizzati al contrasto di criminalità comune. In tali attività si annida il coefficiente di tolleranza all'implementazione di sistemi più invasivi e soggetti al concreto pericolo di abuso nel loro impiego. In virtù degli innumerevoli aspetti legati alla tutela delle principali libertà fondamentali, sistemi come *Graphite* dovrebbero essere soggetti ad un attento e pervicace monitoraggio, non solo dal punto di vista

[29] V. comma 7 della legge 124 2007.
[30] Bobbio, (2021: 15).

squisitamente tecnico, ma, per quel che attiene alla pertinenza del ragionamento, prioritariamente giuridico, nel pieno rispetto dei diritti fondamentali comunemente riconosciuti e tutelati. Il tema delle intercettazioni e le relative tipologie di applicativi sviluppati a tal fine, ha rappresentato, fin dall'insorgenza della moderna tecnologia investigativa, un punto di acceso dibattito per dottrina, giurisprudenza e addetti ai lavori. L'elemento di raccordo muove dalla considerazione dei potenziali rischi di usi impropri degli innumerevoli strumenti messi a disposizione degli inquirenti, i quali sono forieri di particolare apprensione per l'estrema complessità tecnica alla base del loro funzionamento e alla peculiare predisposizione concettuale di estrema malleabilità e vulnerabilità ad agenti esterni. Lo stesso Copasir già in passato ha manifestato profonde riserve sul metodo di analisi della sezione centrale per il controllo sui contratti secretati della Corte dei conti, evidenziando come esista una "zona grigia di atti che le amministrazioni degli enti non inviano alla sezione in nessuna fase del controllo e che i contratti senza visto e registrazione della sezione non sono efficaci, ma la sezione stessa non dispone di poteri che possano far emergere ciò che non viene a sua conoscenza"[31]. Le stesse indicazioni del Copasir rilevano come il dato sia in netto contrasto con "la poderosa attività delle procure in merito all'impiego di sistemi di intercettazione che vede l'ordinamento italiano tra i maggiori utilizzatori di tali strumenti". I primi passi verso una rendicontazione seria delle spese di intercettazione sono avvenuti con il decreto legislativo del 2018, c.d. riforma Orlando, configurando le spese di intercettazioni tra le generali della giustizia, adeguandosi al testo unico del 2002. In tema di indagini condotte dalla polizia giudiziaria, il conferimento di un incarico diretto da parte del P.M. ad un soggetto privato dovrebbe rientrare tra le spese di giustizia[32]. Lo stesso Copasir si è posto l'obiettivo fondamentale di individuare gli strumenti normativi più idonei alla tutela informativa del paese. Secondo il Copasir, infatti, serve "una valorizzazione di apposite linee guida tra le aziende coinvolte e gli uffici giudiziari competenti, sull'esempio di alcune Procure italiane, per il corretto impiego delle strumentazioni volte ad attività di intercettazione e captazione"[33]. Resta però, da valutare l'aspetto legato ad aree grigie, strutturalmente collegate ad attività preventive o dei servizi di intelligence. Sull'impiego di sistemi gestiti da società private rimane emblematico, come già accennato, il caso *Exodus*, un *software* di captazione usato in passato da varie procure e che, dopo le indagini che ne hanno evidenziato la scarsa sicurezza d'insieme, ha spinto le parti interessate a rilevare i rischi di integrità ed affidabilità dei sistemi così concepiti. *Exodus* era altro un *malware* di captazione introdotto nei sistemi di comunicazione dei soggetti sottoposti alle indagini, mediante vari espedienti tecnici non molto dissimili da *Graphite*[34]. Come emergerebbe dai documenti sui pagamenti della polizia di stato, rilasciato sulla base della normativa sulla "trasparenza nell'uso delle risorse pubbliche, art. 4 D.lgs. n.33 del 2013-art. 5 D.lgs. n.97 2016, eSurv, ha ricevuto in data 6 novembre 2017 un versamento pari a 307.439,90 euro. La spesa è inserita alla voce "Acquisto di beni e servizi" di "Sistema di intercettazione attiva e passiva"[35]. In pratica, l'impiego dei captatori si esercita mediante l'inoculazione di un virus informatico all'interno del dispositivo e nel verbale delle operazioni di indagini, oltre ai relativi requisiti tecnici, dovrebbero essere indicati anche

[31] Così la Relazione sulla disciplina per l'utilizzo di contratti secretati del Copasir del 21 ottobre 2021, https://www.publicpolicy.it/wp-content/uploads/2022/02/Relazione-Annuale-Copasir-2021-2022.pdf.
[32] V. Jacobazzi (2021).
[33] Sempre alla relazione del Copasir 2021.
[34] V. Ghidotti (2019).
[35] V. pag. 11 del documento rinvenibile sul sito della polizia di Stato.

la tipologia di software (programma specifico) impiegato[36]. Un aspetto fondamentale, è che le comunicazioni intercettate finiscano nel c.d. "Archivio digitale", in cui deve essere assicurata l'integrità del materiale intercettato, registrato e trasmesso ai ricevitori. Nel caso in cui, però, non sia possibile un trasferimento contestuale dei contenuti intercettati con i captatori all'interno dell'archivio, le ragioni dell'impedimento devono essere riportate nel verbale delle operazioni materiali compiute dalla polizia giudiziaria, al termine delle quali, inoltre, il captatore deve essere disattivato con modalità che lo rendano inidoneo per ulteriori impieghi. A ulteriore garanzia delle parti sottoposte alle indagini "Il pubblico ministero dà indicazioni e vigila affinché nei verbali non siano riportate espressioni lesive della reputazione delle persone o quelle che riguardano dati personali definiti sensibili dalla legge, salvo che risultino rilevanti ai fini delle indagini"[37]. I difensori, entro il termine fissato dal P.M., hanno facoltà di esaminare gli atti di indagine e ascoltare le registrazioni o di prendere visione delle comunicazioni informatiche e telematiche presenti nell'archivio digitale. Dunque, "Scaduto il termine, il giudice dispone l'acquisizione delle conversazioni o dei flussi di comunicazioni informatiche o telematiche indicati dalle parti, che non appaiano irrilevanti, procedendo anche d' ufficio allo stralcio delle registrazioni e dei verbali di cui è vietata l'utilizzazione e di quelli che riguardano categorie particolari di dati personali, sempre che non ne sia dimostrata la rilevanza. Il pubblico ministero e i difensori hanno diritto di partecipare allo stralcio e sono avvisati almeno ventiquattro ore prima"[38]. A garanzia della genuinità e regolarità delle procedure, Il G.I.P. dispone la "trascrizione integrale delle registrazioni ovvero la stampa in forma intellegibile delle informazioni contenute nei flussi di comunicazioni informatiche o telematiche da acquisire, osservando le forme, i modi e le garanzie previsti per l'espletamento delle perizie. Le trascrizioni o le stampe sono inserite nel fascicolo per il dibattimento. Il giudice, con il consenso delle parti, può disporre l'utilizzazione delle trascrizioni delle registrazioni ovvero delle informazioni contenute nei flussi di comunicazioni informatiche o telematiche effettuate dalla polizia giudiziaria nel corso delle indagini"[39]. In nuovo archivio digitale è sottoposto a controllo e direzione dell'ufficio del procuratore della repubblica. La gestione dello stesso, pertanto, deve avvenire garantendo il requisito specifico della segretezza della documentazione con riferimento al materiale diretto delle attività di intercettazione e ai contenuti irrilevanti, di cui, peraltro, è vietata l'utilizzazione[40]. L'uso dei captatori informatici è foriero di incisività considerevole nella vita privata di cittadini sottoposti ad attività di indagine, il che comporta una potenziale compromissione di valori fondamentali sulla riservatezza delle comunicazioni. La ricerca di un equilibrato punto d'incontro tra i valori costituzionali che vengono in rilievo solleva costantemente il dilemma sull'uso appropriato dello strumento, evidenziando la necessità che si tratti di circostanze assolutamente eccezionali. La possibilità di intercettare conversazioni o comunicazioni telefoniche, informatiche o telematiche[41], impiegando *software* specifici, attraverso i quali captare comunicazioni e conversazioni effettuate con l'uso di telefoni, fissi o mobili, nonché i flussi di comunicazioni e dati trasmessi per via telematica e informatica è foriera di ripercussioni notevoli sulla gestione pratica delle dinamiche operative. Mediante l'uso dei

[36] *Ex* art. 267 c.p.p., comma 3.
[37] Così al comma 2-*bis* art. 268 c.p.p.
[38] Così al comma 6 art. 268 c.p.p.
[39] Così al comma 7 art. 268 c.p.p.
[40] V. il nuovo testo della legge di conversione Legge 31 marzo 2025, n. 47 ("Modifiche alla disciplina in materia di durata delle operazioni di intercettazione"), https://www.gazzettaufficiale.it/eli/id/2025/04/09/25G00055/sg.
[41] *Ex* artt. 266, c.1, e 266-*bis* c.p.p.

sofisticati captatori, gli inquirenti possono avvalersi di un corposo elenco di opzioni intrusive quali l'accesso ai dati ed eventualmente una copia degli stessi, anche di quelli già memorizzati nel dispositivo del soggetto sottoposto al controllo. È, inoltre, possibile avviare la registrazione del traffico dati sia in arrivo che in partenza, la registrazione di telefonate e videochiamate, nonché, sempre a distanza, l'attivazione delle funzioni di microfono e/o telecamera indipendentemente dalla volontà dell'utente coinvolto. Mediante *software* come *Graphite*, sarebbe possibile una replicazione dell'apparato strumentale sottoposto alla captazione, attraverso il meccanismo della registrazione di tutto ciò che avviene entro un certo raggio di azione sfruttando, in ragione delle tendenziali abitudini digitali del soggetto, una disponibilità costante per l'apparato. Le principali criticità d'impiego, rappresentate dalla intrinseca predisposizioni di sistemi concepiti con simili architetture informatiche, strettamente correlate alla potenziale acquisizione massiva ed indeterminata di dati personali e sensibili determina la necessità di una complessa ed attenta valutazione degli interessi in gioco configurando il più delle volte un delicato equilibrio tra l'esigenza di tutela della riservatezza nella sfera privata del cittadino e la necessità di contrasto ad attività criminali. Se una simile circostanza possa determinare anche possibili sconfinamenti verso stati di controllo generalizzato di particolari categorie di soggetti, in ragione del ruolo degli stessi all'interno dei meccanismi relazionali della società civile e politica non è dato saperlo con certezza. Ragionare sulla possibilità di un uso improprio degli strumenti informatici captativi è il presupposto per un controllo vigile ed attento nell'operato anche nelle peculiarità delle autorità delegate in attività legittime ma, in ragione di evidenze casistiche non trascurabili, potenzialmente portatrici di zone grigie e seri elementi di perplessità ulteriori.

## 8. La gestione delle intercettazioni classiche: novità normative e differenze d'impiego con le attività d'intelligence

Nel corso degli anni vi è stato un uso sempre più frequente di strumenti tecnologici innovativi ed intrusivi nel contesto delle attività investigative, garantito dalle performance sempre più efficienti di *hardware* e *software.* Allo stesso tempo, si è cercato di materializzare un uso prudente del captatore informatico in quanto considerato potenzialmente invasivo e rischioso dalle stesse Procure, in virtù degli elevati costi presentati dalle licenze d'uso e dalla gestione di apparati molto sofisticati, soggetti alla supervisione di personale specialistico ad elevata qualificazione e valore aggiunto. Si parla di costi quasi triplicati rispetto agli strumenti tradizionali, senza considerare gli innumerevoli problemi pratici legati all'eccessivo uso delle batterie dei dispositivi portatili inoculati e alla necessità di considerare interventi deflattivi di *antivirus* e *firewall* di sistema. Tutte circostanze che richiedono attenta pianificazione degli investigatori, anche con l'assistenza ed il supporto di consulenti e società private. Non è raro, infatti, che gli uffici competenti affidino appalti di servizi ed acquistino licenze d'uso ad imprese il cui *core business* è rappresentato da interessi prettamente finanziari in una logica efficentista da ottimizzazione di costi e risultati incompatibile con il misurato approccio richiesto ad organi ed apparati dello Stato proiettati alla gestione e valutazione di delicati equilibri afferenti alla tutela di diritti della persona umana. Nonostante, come si è visto, non manchi un articolato apparato normativo teso a disciplinare l'impiego dei captatori, dopo molteplici discussioni delle forze politiche, coinvolte dalla sensibilità del tema, anche nell'ottica del forte interesse da parte dell'opinione pubblica su aspetti peculiari della riservatezza, è stato di recente convertito in legge il disegno di Legge Zanettin, recante "modifiche alla

disciplina in materia di durata delle operazioni di intercettazione". Essa si compone di un unico articolo, che modifica l'art. 267 c.p.p. e l'art. 13 d.l. 13 maggio 1991, n. 152. Si interviene poi sull'art. 13 d.l. n. 152/1991 per coordinare la relativa disciplina, esplicitando che la stessa, quanto alla durata delle intercettazioni, deroga alla nuova previsione introdotta nell'art. 267, co. 3 c.p.p.[42] Alla luce di risvolti giuridici, mediatici e politici di alcuni recenti casi, tuttavia, è la mancanza di una disciplina organica e completa sugli aspetti accessori che determina non poche criticità. Mancano, infatti, molti decreti ministeriali che determinino in modo univoco quali debbano essere i requisiti tecnici dei captatori informatici e vi sono innumerevoli problemi legati alla inoculazione e disattivazione dei *software* spia. Altro tema fondamentale, inoltre, è l'aspetto legato alla legittimità della perquisizione condotta con i captatori in quanto, come si è visto, è possibile acquisire qualsiasi dato presente nelle memorie del dispositivo e, soprattutto, mancano norme chiare in merito alla genuinità della prova e alla possibilità concreta di una manipolazione del dato grezzo in un contesto internazionale e digitale in cui il valore dei dati è di estrema importanza. L'evoluzione dei fenomeni criminali ha comportato la necessità di implementare strumenti adeguati al progresso tecnologico permettendo l'uso, con le dovute limitazioni e garanzie, di anticipazione nel perseguimento e repressione di alcune tipologie di reati dal carattere fluido ed *extra*territoriale, dalla forte connotazione criminogena, poco suscettibili ad attività di indagine basate esclusivamente sul metodo classico. I più recenti provvedimenti legislativi, espressi ancora una volta nella facile e veloce formula politica della decretazione d'urgenza, sembrerebbero essere ancora in linea con l'impianto generale di politica criminale securitaria,[43]. Come già anticipato nelle precedenti pagine, la Cassazione a Sezioni Unite, è già intervenuta sulla vicenda interpretativa affermando nella sentenza n. 26889 del 2016 (*Scurato*), come "in tema di intercettazioni di conversazioni o comunicazioni, ai fini dell'applicazione della disciplina derogatoria delle norme codicistiche prevista dall'art. 13 del d.l. n. 152 del 1991, convertito dalla legge n. 203 del 1991, per procedimenti relativi a delitti di criminalità organizzata. Più di recente, però, nella sentenza n. 34895 del 2022 ha sottolineato che nel richiamare l'art. 51, comma 3-bis e 3-quater c.p.p., avrebbe inteso riferirsi solo ai delitti associativi annoverati nel relativo elenco (e non anche ai reati monosoggettivi aggravati dal metodo mafioso). Da quest'ultima interpretazione si evince come "in tema di intercettazioni di conversazioni o comunicazioni, per delitti di "criminalità organizzata", di cui all'art. 13 d.l. 13 maggio 1991 n. 152, conv., con modif., dalla l. 12 luglio 1991, n. 203, devono intendersi tutti i reati di tipo associativo, anche comuni, correlati ad attività criminose più diverse, ai quali è riferito il richiamo ai delitti elencati nell'art. 51, commi 3-bis e 3-quater, c.p.p., con esclusione delle ipotesi di mero concorso nei delitti commessi avvalendosi delle condizioni di cui all'art. 416-bis c.p. ovvero al fine di agevolarne l'attività". Tale impostazione preclude, dunque, la possibilità di disporre intercettazioni sulla base della disciplina derogatoria in esame per delitti aggravati ai sensi dell'art. 416 bis.1 c.p., perché commessi con metodo mafioso o con la finalità di agevolare un sodalizio mafioso. L' obiettivo della riforma è di contemperare le necessità investigative, di pubblica informazione per le vicende di pubblico interesse, nonché il diritto dei cittadini alla loro riservatezza quando estranei al procedimento. È assodato come lo strumento della captazione costituisca uno dei pilastri nell'attività investigativa e, poiché la maggior parte delle intercettazioni (telefoniche, ambientali e di altro genere) viene disposta nell'ambito di indagini di competenza delle direzioni distrettuali antimafia, lo strumento captativo è divenuto indispensabile a fini di accertamento e repressione dei reati di maggior gravità, quali quelli concernenti le organizzazioni

[42] Per un ampio approfondimento sul nuovo disegno di legge V. Gatta (2025).
[43] V. Bertolucci (2025).

mafiose o il terrorismo. Se è vero che il ricorso a tale mezzo di ricerca della prova è meno diffuso in altri Paesi a democrazia avanzata, è vero anche che gli stessi non sono soggetti ai medesimi fenomeni di diffusa pervasività e gravissima pericolosità rappresentati dalla presenza sul territorio delle organizzazioni di stampo mafioso. L''intento del legislatore, con il recente intervento normativo, è determinare l'obbligo di motivazione del decreto di proroga delle intercettazioni, nonché disciplinare più nello specifico durata e modalità operative. Di particolare interesse, risulta l'istituzione della figura del "funzionario responsabile delle intercettazioni", a sua volta, nell'ottica di una gestione interna dei ruoli e ne rispetto delle gerarchie funzionali, nominato dal procuratore della Repubblica. Sempre nel medesimo intervento normativo, al fine di incrementare le generali garanzie di sistema, il legislatore si è premurato di introdurre una regolamentazione specifica per il procedimento di acquisizione delle conversazioni intercettate non utili alle indagini, affinché le stesse rimangano coperte da segreto e non abbiano mai ingresso fra gli atti conoscibili. La relativa tutela, in particolare, dovrebbe essere assicurata mediante una "scrematura" (ad opera prima del P.M., poi del GIP) delle conversazioni ritenute irrilevanti, custodite in apposito registro riservato e secretate. Al fine di garantire anche la libertà dei cittadini di essere adeguatamente informati su attività di pubblico interesse ed alla libera stampa, a sua volta ad informare gli stessi ed esercitare il giudizio critico tipico della professione svolta, sono state implementate autonome fattispecie per l'illecita divulgazione di notizie relative ad atti del procedimento penale coperti da segreto e l'accesso illecito ai medesimi atti, al fine di evitare che ciò si traduca in un pregiudizio per le indagini ovvero in una indebita propalazione di notizie riservate; è stata, inoltre, prevista una specifica sanzione amministrativa per la pubblicazione di dati personali in violazione delle disposizioni previste dal decreto legislativo 30 giugno 2003, n. 196 (c.d. Codice della *privacy)* e dal codice di deontologia, la cui applicazione e rispetto è rimessa al GDPR[44].
L'architettura le attività d'intercettazione, nonostante alcune specificità dedicate al contrasto della criminalità mafiosa, è caratterizzata da una finalità di risultato che non può non risentire di limitazioni e prerogative processuali, inquadrabili nelle prerogative classiche della forza pubblica e dei meccanismi di tutela e garanzie per le parti processuali. Diversamente, il Caso Paragon dimostra quanto, nel quadro delle attività d'intelligence, la normativa standard di riferimento, nonostante novelle ed interventi del legislatore, risenta di ineludibili aree grigie e punti di riferimento assai più aleatori. Il tutto dipende essenzialmente dalle peculiarità dei fenomeni interessati e dalle modalità tecniche operative necessarie al loro contrato, non sempre rinvenibili nei quadri di ortodossia normativa, seppur necessariamente soggetti ad elementi di tutela immancabili nei sistemi democratici occidentali. La trasparenza e la possibilità di un controllo contestuale e postumo, in tal senso, non sempre trovano riferimenti normativi specifici come nelle tipiche attività intercettative, tuttavia, non è possibile escludere in toto il principio di affidamento ed affidabilità delle autorità coinvolte.

## 9. Attività di intelligence ed attività investigative: due momenti differenti dell'agire securitario

L'aspetto cruciale nella vicenda del caso *Paragon* riguarda la distinzione concettuale e giuridica tra le due differente tipologie di attività investigative, inquadrate e regolamentate in un differente complesso

[44] V. testo del DDL *Zanattin*, recante "Modifiche alla disciplina in materia di durata delle operazioni di intercettazione" convertito in Legge n. 47/25 del 31 marzo 2025, GU n. 83 del 9 aprile 2025.

normativo. Le une, attività investigative *standard*, afferenti all'ordinaria attività dell'autorità giudiziaria, nell'ambito delle indagini condotte per il fine di prevenzione, contrasto e accertamento delle fattispecie criminose comune, seppur, in alcune circostanze, rappresentate da fenomeni di particolare allarme sociale; le altre, attività di intelligence degli apparati di sicurezza, volte alla prevenzione, contrasto a fenomeni in grado di arrecare seri danni alla tenuta democratica dello Stato e, dunque, prerogativa esclusiva di nuclei privilegiati e soggetti a particolari deroghe del sistema di garanzie poste a tutela della riservatezza, proprio in virtù del particolare pericolo rappresentato all'ordine costituzionale. La sicurezza, intesa come tutela dell'ordine democratico, rappresenta un valore garantito in via ordinaria, anche laddove non sia connesso a situazioni di emergenza politico istituzionale. Tuttavia, è accaduto che il valore della sicurezza, inteso in senso straordinario, abbia assunto un peso maggiore nel contemperamento dei principi e diritti costituzionalmente garantiti. Lo Stato ha più volte messo in atto misure restringenti le quali, all'apparenza attuate col fine meritorio di rassicurare, di fatto, hanno sempre di più limitato diritti e libertà fondamentali, sollevando anche il relativo rischio di uno scivolamento dallo Stato di diritto verso lo Stato di prevenzione, dove le ragioni di sicurezza rischiano di assumere il tenore di "ragion di Stato"[45]. La sfida più grande per il decisore politico è riuscire nell'arduo compito di erogare risposte ai bisogni di sicurezza che non si pongano in evidente contrasto o arrivino al punto da violare i principi stessi dello Stato di diritto. Di conseguenza, non può e non deve essere permesso l'impiego di ogni possibile mezzo per difendersi dai propri ipotetici o presunti nemici, né, d'altronde, si può privarli della dignità elementare del vivere civile e, dunque, il nucleo essenziale di quegli stessi diritti fondamentali riconosciuti ad ogni individuo[46]. I provvedimenti normativi adottati sull'onda dell'emergenza hanno fatto ampio ricorso a soluzioni restrittive con norme incriminatrici nuove e misure di prevenzione più stringenti, comprese deroghe al sistema processuale penalistico, nonché più ampi poteri di polizia e di intelligence, il tutto nell'architettura complessiva di implementare forti interferenze dei poteri pubblici nella vita personale delle persone coinvolte. Il progresso tecnologico, l'esplosione dei canali social e da ultimo l'*AI* stanno stravolgendo la gestione dei profili legati alla sicurezza e, di conseguenza, sia i servizi di intelligence, nel garantire la loro attività di prevenzione che le polizie giudiziarie, nell'ambito delle indagini rivolte alla repressione dei reati, sono costantemente messe sotto pressione dalla mole massiva di informazioni e fantasiosi strumenti impiegati nel mondo del *web*, del *cyber*spazio e delle telecomunicazioni in generale, tutti sistemi sofisticati di interazione in cui le dinamiche criminali e minacciose per l'ordine democratico si esplicano nelle più creative forme. La complessità stessa dell'architettura tecnologica odierna rende necessario l'impiego di un altrettanto fantasioso ed ingegnoso armamentario di strumenti volti al contrasto delle innumerevoli iniziative di matrice criminale[47]. Nelle differenti scelte di politica criminale, vi è, infatti, in gioco il nucleo essenziale nel rapporto equilibrato tra la sfera del rispetto dei diritti individuali e quella dei poteri statuali di intervento e ridimensionamento degli stessi in funzione delle varie necessità repressive di volta in volta poste a carico degli esecutori. Un ruolo significativo è rappresentato dai servizi di intelligence ed apparati di sicurezza mediante la loro peculiare attività di prevenzione, per i quali è stato riadattato costantemente l'inquadramento normativo, al fine di garantirne i margini già elastici di legittimità giuridica, sempre nel rassicurante fine del contrasto ai più gravi fenomeni di criminalità organizzata, di terrorismo o di eversione dell'ordine costituzionale.

[45] V. Bonetti (2006); Bartoli, *Regola ed eccezione nel contrasto al terrorismo internazionale*, (2013); Ruotolo, (febbraio 2013).
[46] V. Salazar (2015: 203); Ackerman (2005).
[47] V. il già citato Bosco (2012); Carli (2013); Flor (2017).

Analogamente a quanto già fatto in tema di misure di prevenzione e di perquisizioni preventive con strumenti costruiti appositamente per il contrasto del fenomeno della criminalità organizzata, è stata strutturato un sistema specifico per l'uso di intercettazioni, creando l'apposito istituto delle intercettazioni preventive di polizia, in cui l'atto, per l'appunto preventivo, costituirà solo la base della pre-inchiesta, volta a ricercare il dato che poi possa essere utilizzato come notizia di reato[48]. Il sistema è costruito in modo analogo a quanto previsto in tema di notizie anonime, provenienti da riservati colloqui investigativi "confidenziali", o dalle informazioni dei servizi d'informazione o sicurezza, prevedendo l'esclusione di qualsiasi riferimento alla fonte che ha dato l'avvio all'attività preventiva. La genesi dell'atto preventivo, infatti, non deve risultare da nessun atto processuale e, forse, in tali circostanze si annida subdolamente la possibilità di abusi e violazioni derivanti dalla eventuale sottoposizione del *target* a dinamiche captative senza esserne consapevole e senza portene contestare l'illegittimità[49]. Lo strumento, per via delle sue innumerevoli potenzialità, si presta facilmente a derive non esattamente in linea con i canoni di regolarità normativa cui deve essere sottoposto il maneggiamento di pesi e contrappesi nel sistema di tutela delle libertà fondamentali, tra tutte, il rispetto della vita privata e la necessità che la stessa non veda affacciarsi alla sua porta interferenze indebite dell'autorità pubblica. Già nel lontano 2004 La Corte Costituzionale, con sentenza del 29 dicembre 2004 n. 443, ha stabilito come non sia possibile alcun confronto tra la disciplina delle intercettazioni ordinarie e quella relativa alle intercettazioni preventive: Le stesse, infatti, sempre secondo la corte non tenderebbero all'accertamento e repressione del reato ma esclusivamente a prevenirne la commissione e sarebbero, per tale specifica caratteristica foriere di una minore garanzia rispetto agli standard regolatori garantiti dall'art. 266 del codice di rito.. I recenti interventi hanno tentato un riordino della disciplina, con l'intento di migliore definizione e distinzione tra le differenti tipologie di attività investigative e, infatti, la manovra finanziaria approvata per l'anno 2023 contiene una riforma specifica dell'ulteriore categoria delle intercettazioni preventive effettuate dai Servizi di informazione per la sicurezza, introdotte nell'ordinamento italiano nel 2005 (art. 4, d.l. 144/2005) come strumento di contrasto al terrorismo internazionale. Anche tale strumento è stato appositamente implementato per lo svolgimento di attività tecniche eseguite *ante delictum* e del tutto inutilizzabili nel procedimento penale, dirette, infatti, "a raccogliere informazioni utili per la prevenzione di gravi reati e non per l'acquisizione di elementi finalizzati all'accertamento della responsabilità per singoli fatti delittuosi"[50]. Non si tratta né intercettazioni giudiziarie, regolamentate dal codice di procedura penale negli artt. 266 c.p.p. ss., né d'intercettazioni preventive di polizie regolate dall'art. 226 disp. att. c.p.p. Sono fondamentalmente un autonomo terzo *genus*, ossia intercettazioni effettuate dai Servizi d'*intelligence* all'interno della loro attività di sicurezza ed informazione. Da più parti e per molto tempo era stata sollevata la necessità di un intervento concreto per definirne gli aspetti, sia perché sempre impiegato nella quotidiana attività investigativa dei servizi, sia perché spesso e volentieri i relativi risultati informativi vengono acquisiti ai fini dell'avvio di procedimenti penali specifici, fino al punto da imporne il materiale probatorio necessario alla decisione del caso concreto. L'impostazione, nel passato, ha generato non poca confusione anche per gli addetti ai lavori, i quali ne hanno sfruttato le aree grigie per le ordinarie regole probatorie confondendo ruoli e garanzie funzionali. L'intervento del legislatore con la l. n. 197/2022 ha, in primo luogo, attribuito le spese relative a tali operazioni captative

[48] Così all'art. 226, comma 5, disp. att. c.p.p.
[49] V. Sprangher (2009: 49-51); Vele, (2011: 46-47); Delle Fave (2013: 259).
[50] V. Cantone – L.A. D'Angelo (2006: 54).

all'apposito programma di spesa concernente il Sistema di informazione per la sicurezza della Repubblica, iscritto nello stato di previsione del Ministero dell'economia e delle finanze, ma, nonostante tutto, l'impianto normativo generale mantiene ancora molte delle criticità del passato, come la complessa individuazione dei soggetti legittimati alla richiesta o ai limiti sul contenuto dei decreti autorizzativi e alle c.d. deleghe in bianco[51]. La ratio di fondo dell'intervento nasce dall'esigenza di razionalizzare le risorse investigative e, infatti, alla relazione di accompagnamento del Ministro[52] si può leggere come le spese e soggetti sottoposti a captazione siano importanti e non trascurabili[53]. Aver reso il comparto dell'intelligence autonomo nella gestione finanziaria delle intercettazioni preventive comporta non solo la segretezza delle informazioni acquisite, rendendo, almeno in linea teorica, possibile evitare o limitare indebite contaminazioni con il procedimento probatorio e, soprattutto, tra i due differenti comparti, secondo i rispettivi differenti fini, della sicurezza nazionale e giustizia penalistica. La sottrazione della relativa competenza al Ministero della Giustizia dovrebbe evitare che i dati acquisiti possano essere conservati da organi esterni evitando, di conseguenza, "la circolazione al di fuori del comparto di *intelligence* di documentazione [...] contenente elementi di natura sensibile [...] che rende riconoscibile l'attività dei Servizi di informazione, determinando un evidente *vulnus* alle esigenze di riservatezza delle suddette operazioni"[54]. Con la nuova disciplina, in sostanza, il legislatore non si distanzia molto dalla linea originaria stabilita nel lontano 2005, allorquando, anziché integrare la disciplina già prevista per le intercettazioni preventive di polizia, di cui all'art. 226 disp. att. c.p.p., scelse di introdurre una nuova e più specifica forma di intercettazione preventiva ad uso esclusivo dei Servizi di informazione per la sicurezza della Repubblica, stabilendo alcuni ruoli peculiari per quanto attiene agli attori in gioco e ai presupposti applicativi, mentre, per quanto concerne le concrete modalità operative, faceva semplicemente rinvio alle previsioni contenute nei commi 2, 3, 4 e 5 dell'art. 226 disp. att. c.p.p. Il recente intervento, invece, nel farsi portatore del superamento di una tecnica consolidata come quella del semplice rinvio, cerca di compiere un passo ulteriore stabilendo la definitiva autonomia dell'istituto delle intercettazioni preventive d'*intelligence*, definendo una integrale regolamentazione negli artt. 4 e 4 *bis*, d.l. 144/2005, attribuendogli identità politica e spessore operativo. La riforma, in alcuni casi, si limita a riprodurre il contenuto pressoché integrale dell'art. 226 disp. att. c.p.p., in altri procede a minimi ritocchi linguistici e/o sistematici che, sì, migliorano l'istituto ma, allo stesso tempo, non ne alterano la struttura complessiva. La nuova costruzione normativa in tema di intercettazioni preventive d'*intelligence* rimane quasi invariata rispetto al passato, salvo alcune innovazioni formali che contribuiscono solamente a conferirle maggiore coerenza sistemica e d'intenti. Una peculiarità della riforma riguarda il fatto che oltre al verbale sintetico delle operazioni svolte e ai supporti utilizzati durante l'esecuzione materiale della captazione, ora sussiste in capo agli stessi un obbligo di consegna sui contenuti delle captazioni. Una delle principali caratteristiche delle attività preventive risiede nel fatto che, secondo il dettato del comma 5 dell'art. 4 *bis*, gli elementi acquisiti mediante tale specifica attività non possano essere utilizzati nel corso del procedimento penale, non possano essere menzionati in atti di indagine né costituire oggetto di deposizione né essere altrimenti divulgati, con la possibilità di utilizzare quel materiale solo per mere finalità investigative (c.d.

[51] La disciplina riformata, dopo l'approvazione parlamentare, confluisce nell'art. 1, comma 684 del d.d.l. AS 442.
[52] Relazione tecnica di accompagnamento alla proposta emendativa, rinvenibile sul sito del Senato, https://www.senato.it/export/ddl/full/59329.
[53] Dati consultabili su www.giustizia.it.
[54] Così sempre alla Relazione tecnica di accompagnamento alla proposta emendativa, 2.

*exclusionary rules)*; nell'eventualità in cui, attraverso l'esecuzione delle intercettazioni e dei controlli *ante delictum*, si scopra l'avvenuta consumazione del reato, l'informazione potrebbe rappresentare la base della c.d. pre-inchiesta, con fine di ricercare quell'ulteriore dato da cui far dipendere l'inizio del procedimento penale[55]. Interventi normativi su temi di nicchia, come le intercettazioni di intelligence, permettono un maggior grado di attenzione del dibattito politico e parlamentare e, come si è potuto anche osservare nei recenti eventi riguardanti il caso *Paragon*, il tema è foriero di ripercussioni pratiche per gli addetti ai lavori e potente strumento di critica per l'opinione pubblica[56]. L'obiettivo principale del legislatore è quello di arginare il ragionevole pericolo di una malcelata osmosi probatoria del materiale acquisito in fase preventiva per scopi processuali e, di conseguenza, vengano così veicolate notizie acquisite in base a criteri che obbediscono, però, a scelte discrezionali del potere esecutivo, scevri dalle logiche di garanzia procedimentale del processo e potenzialmente motivate da finalità non sempre compatibili con il regolare equilibrio tra le parti in gioco. Così, il legislatore, eliminando ogni possibile riferimento alle previsioni di cui all'art. 226 disp. att. c.p.p., introduce una disciplina autonoma per la particolare categoria delle intercettazioni preventive d'*intelligence*, tipizzandone presupposti, limiti, regole e modalità operative. Molte criticità rimangono in essere e non sono state del tutto superate, ma il concreto effetto innovativo sull' architettura normativa dovrà essere rivalutato con la generale messa in opera della novella[57]. Casi come *Graphite* possono, in tal senso, aiutare operatori ed interpreti a circostanziare in modo dettagliato i principali elementi critici legati all'uso improprio degli istituti costruiti per finalità specifiche, come le attività investigative preventive o d'intelligence. È sempre, però, presente quel sottile alone di eterogenesi dei fini tanto timorata dai tutori del garantismo costituzionale, ma, allo stesso tempo, mai veramente confinata. Nell'eterna illusione digitale, sarebbe bene non credere nell'assoluta gestione equilibrata dei confini di intromissione nelle sfere private dei cittadini. Come si suol dire, "*quis custodiet ipsos custodes*" ma, ogni tanto, sarebbe bene saperlo. Nel caso Paragon rimangono, allo stato attuale, forti elementi di criticità relativi all'impiego del sistema e alle possibili esecuzioni del programma fuori dalle legittime finalità d'intelligence e, nonostante le autorità coinvolte si sforzino nel giustificare la regolarità nella modalità di messa in opera, permangono quelle tipiche riserve e dubbi difficilmente accettabili in uno stato di diritto.

## 10. La tutela del dato come tema ricorrente nella disciplina europea e la rilevanza nella gestione del caso Paragon

Il tema dell'acquisizione dei dati ai fini investigativi rappresenta da molto tempo una delle maggiori criticità per le garanzie di riservatezza delle comunicazioni come vincolo alle attività di intercettazione, sia che esse avvengano nelle modalità più convenzionali che con l'uso dei moderni e più intrusivi captatori informatici. La maggiore disponibilità di una così consistente miniera informativa, gestita in alcuni casi senza particolari riserve, è maturata anche nel contesto di un'opinione pubblica in preda ad un pericoloso sonnambulismo con ricadute non irrilevanti nel sistema dei valori di riferimento. Il *vulnus*

[55] V. Curtotti, (2018: 438).
[56] Cfr. *European Union Agency for Fundamental Rights, Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU: mapping of Member States' legal frameworks, October* 2018, disponibili su www.fra.europa.eu.
[57] V. Cascini, (2025).

di tutela, in tal caso, risiede non tanto nella possibilità per gli inquirenti di accedere ai dati, il più delle volte davvero indispensabili per la conduzione delle operazioni investigative, quanto nel potenziale delle tecnologie impiegate a tal fine e come un cattivo uso delle stesse, vuoi per scarsa conoscenza dello strumento o, peggio ancora, per volontà distorsiva, possa, impunemente, distruggere la vita privata delle persone coinvolte. La maggiore consapevolezza europea sul tema ha accelerando il processo d' integrazione dei sistemi giuridici nazionali verso un adeguamento ai canoni di riferimento di carte e trattati. I principi stabiliti fungono da supporto nell'equilibrio delle garanzie poste a tutela dei cittadini europei contro gli abusi delle autorità pubblica nel corso delle indagini e Il legislatore nazionale, anche in virtù di una giurisprudenza attiva, si è premurato di innovare l'impianto normativo in maniera conforme. Si tratta di un lento percorso iniziato con la dichiarazione di invalidità della direttiva 2006/24/CE c.d. *Frattini*, nel caso *Digital Rights Ireland*[58]. Il fine era di assicurare una adeguata protezione contro le ingerenze della forza pubblica nella sfera privata dei cittadini, rappresentata da una crescente richiesta di acquisizione e conservazione dei dati gestiti e generati dagli erogatori dei servizi di telecomunicazione. La Corte, infatti, sempre nel rispetto del suo ruolo di interprete unico del diritto eurounitario, ha circoscritto l'operato del legislatore nazionale in tema di limitazione dei diritti fondamentali, fornendo strumenti utili a dirimere le varie controversie sollevate da casi concreti e aiutando a contemperare in modo adeguato le differenti esigenze in gioco. In alcuni casi emblematici[59], i giudici europei sono stati chiamati a stabilire il limite entro cui le autorità nazionali possono intervenire su maneggio, conservazione e accesso ai dati personali nelle attività di accertamento e contrasto alla criminalità. Sono stati stabiliti *gold standards* sulla totale prevalenza delle istanze di protezione e rispetto della vita familiare e privata rispetto alle esigenze investigative nell'attività di prevenzione, accertamento e contrasto dei reati dallo scarso allarme sociale, ribadendo il principio del primato del diritto dell'Unione sul diritto degli stati membri[60]. Ciò ha comportato la disapplicazione automatica della disciplina nazionale non conforme da parte del giudice nazionale senza attendere la rimozione del diritto interno da parte del legislatore nazionale nelle more di un ipotetico rinvio pregiudiziale, con la possibile sospensione temporanea negli effetti, nel rispetto dei principi di equivalenza ed effettività. La Corte ha specificato come si debbano escludere l'acquisizione di informazioni "che siano state ottenute mediante una conservazione generalizzata e indiscriminata dei dati relativi al traffico e dei dati relativi all' ubicazione incompatibile con il diritto dell'Unione..."[61]. Nell'architettura dell'ordinamento europeo, assume il ruolo di criterio dominante il principio di proporzionalità, il quale comporta una invalicabile impossibilità di sconfinamento oltre certi limiti nella vita privata. Eventuali restrizioni dovranno essere necessarie e proporzionate e, soprattutto, funzionali al raggiungimento di un fine legittimo per una società democratica[62]. Le attività d'intelligence e le relative peculiarità dimostrano quanto una simile architettura di tutele a livello sovranazionale debba necessariamente incardinarsi nel sistema di garanzie delle parti coinvolte. La tutela della sicurezza pubblica, infatti, intesa quale interesse collettivo della generalità dei consociati,

[58] Corte di Giustizia UE (Grande Sezione), 5.4.2022.
[59] Corte di Giustizia dell'unione Europea (Grande Sezione), cause riunite VD (C-339/20) e SR (C-397/20), 20 Settembre 2022.
[60] V. Tartara, (2022).
[61] V. Sentenza del 2 marzo 2021, *Prokuratuur* (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche), C-746/18, EU:C:2021:152, punto 44 e giurisprudenza ivi citata.
[62] Regolamento (UE) 2016/679, (considerando n. 4).

dovrà essere perseguita tra le varie forme possibili, nel modo più idoneo a garantire un accesso ed una gestione dei dati con il minor sacrificio per la riservatezza e che "non appaiano prerogative assolute, ma vadano considerati alla luce della loro funzione sociale...Infatti, come risulta dall'articolo 52, paragrafo 1, della Carta, quest'ultima ammette limitazioni all'esercizio di tali diritti, purché tali limitazioni siano previste dalla legge, rispettino il contenuto essenziale dei summenzionati diritti e, nel rispetto del principio di proporzionalità, siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui. Pertanto, l'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58 alla luce della Carta richiede che si tenga conto allo stesso modo dell'importanza dei diritti sanciti agli articoli 3, 4, 6 e 7 della Carta e di quella che rivestono gli obiettivi di salvaguardia della sicurezza nazionale e di lotta alle forme gravi di criminalità nel contribuire alla protezione dei diritti e delle libertà altrui"[63]. Già nel caso irlandese, la grande sezione della Corte aveva ribadito come i dati fossero suscettibili di fornire informazioni sensibili sulla vita privata delle persone e come la possibilità di disporne fosse foriera di ripercussioni sui diritti fondamentali stabiliti dalla Carta europea, ingerenza suscettibile di abuso in caso di una gestione non ben garantita.[64] Per garantire il criterio della proporzionalità, il legislatore nazionale dovrebbe non solo prevedere norme chiare e precise, supportate dalla previsione di criteri oggettivi di accesso ai dati, ma la portata invasiva della misura prescelta dovrebbe essere basata su un equilibrio tra le opposte esigenze di tutela con misure assolutamente necessaria ed adeguate. Mentre la salvaguardia della sicurezza nazionale potrebbe, in linea di principio, essere considerata obiettivo idoneo a giustificare una conservazione generalizzata ed indifferenziata dei dati, la proporzionalità impone che ciò non avvenga in maniera sconsiderata e, soprattutto, non nel caso della prevenzione ed accertamento della generalità dei reati comuni. In quest'ultimo caso, l'ingerenza nella vita privata delle persone non sarebbe evidentemente tollerabile[65]. Il dato, generalmente inteso quale strumento di accesso cognitivo ad informazioni utili per la tutela della sicurezza collettiva, quando diviene *target* specifico, sotto forma di flusso comunicativo, durante attività d'intelligence mediante strumenti informativi pervasivi, non può non risentire di una architettura europea rivolta al massimo grado di tutele possibili, impiegando come grimaldello e perno centrale la proporzionalità delle modalità d'impiego. Come era giusto aspettarsi, il legislatore nazionale non è rimasto sordo all'evoluzione della giurisprudenza europea e le prime modifiche al codice di procedura introdotte con la legge 23 novembre 2021, n. 178 di conversione del D.L. 30 settembre 2021, n. 132 ne sono un esempio. La novella, come chiarito nel suo preambolo, si pone l'obiettivo "di garantire la possibilità di acquisire dati relativi al traffico telefonico e telematico per fini di indagine penale" , di rispettare i "principi enunciati dalla Grande sezione della Corte di giustizia dell'Unione europea nella sentenza del 2 marzo 2021, causa C- 746/18", limitando l'acquisizione dei dati "ai procedimenti penali aventi ad oggetto forme gravi di criminalità", sempre sotto il "controllo di un'autorità giurisdizionale". La novella non prende in considerazione l'ipotesi di una diversificazione del trattamento in funzione della diversa tipologia di dato, distaccandosi dall'interpretazione della Corte quando non distingue tra la conservazione generalizzata, ammessa solo per i dati anagrafici e di indirizzo IP ed una conservazione più mirata, ammessa solo qualora siano rispettati i requisiti di proporzionalità relativi all'ipotesi delle forme gravi

[63] V. Sentenza del 6 ottobre 2020, La *Quadrature du Net* e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punti da 120 a 122 nonché giurisprudenza citata (punto 48).
[64] Cfr. Corte di Giustizia UE (Grande Sezione), 5.4.2022.
[65] V. sul tema Nicolicchia, (2018).

di criminalità che presentino un forte rischio per la sicurezza pubblica o nazionale, sempre per lo stretto tempo necessario. Che ciò possa direttamente interessare anche l'impostazione delle modalità investigative d'intelligence, viste le peculiarità del comparto di riferimento, non è scontato, ma il legislatore nazionale potrebbe in futuro introdurre alcuni correttivi nell'ottica delle indicazioni euro unitarie, magari apportando qualche significativa modifica garantista sulle modalità di conservazione e gestione dei dati e le operazioni di acquisizione degli stessi nel rispetto di criteri sempre più precisi, oggettivi e, soprattutto, non discriminatori. Le notevoli criticità rappresentate dalle operazioni sul campo impegneranno anche la giurisprudenza sui casi concreti, come il caso Paragon, in cui si dovrà garantire non solo la corretta applicazione ed osservanza del diritto dell'unione nell'ordinamento interno ma, allo stesso tempo, anche la disapplicazione della normativa interna non conforme anche nelle attività investigative d'intelligence. La validità *erga omnes* delle decisioni in seno alla Corte di Giustizia[66] è elemento consolidato e oramai pacifico per i massimi organi giurisdizionali interni quali Cassazione e Corte costituzionale[67], nonostante alcune recenti riserve di quest'ultima[68]. Avendo le decisioni della Corte di Giustizia "il valore di ulteriore fonte del diritto comunitario, non nel senso che esse creino *ex novo* norme comunitarie, bensì in quanto ne indicano il significato ed i limiti di applicazione, con efficacia *erga omnes* nell'ambito della Comunità"[69], queste determinano significativi effetti anche su situazioni non ancora del tutto definite, fatto salvo il potere sospensivo degli effetti del diritto interno nelle decisioni pregiudiziali. Le riserve dei giudici interni[70] non appaiono sufficienti a scalfire il consolidato orientamento in ordine alla prevalenza del diritto unitario e alla sua interpretazione conforme derivante dalle statuizioni della Corte. L'autonomia decisionale degli Stati membri sulle disposizioni processuali rende verosimile una competenza esclusiva nella determinazione delle regole di ammissibilità nel processo delle informazioni raccolte mediante accesso ai dati con sistemi di captazione a condizione, però, che tali regole di diritto interno siano conformi al principio di equivalenza, nel senso che siano almeno uguali o maggiormente favorevoli ai limiti fissati dal diritto unitario ed allo stesso tempo non rendano eccessivamente oneroso l'esercizio dei diritti fissati dall'unione (principio di effettività)[71]. La stessa Corte di Giustizia, nel noto caso *Prokuratuur*, ha precisato come l'obiettivo del principio sia "di evitare che informazioni ed elementi di prova ottenuti in modo illegittimo arrechino indebitamente pregiudizio a una persona sospettata di avere commesso dei reati" aggiungendo che "la necessità di escludere informazioni ed elementi di prova ottenuti in violazione delle prescrizioni del diritto dell'Unione deve essere valutata alla luce, in particolare, del rischio che l'ammissibilità di informazioni ed elementi di prova siffatti comporta per il rispetto del principio del contraddittorio e, pertanto, del diritto ad un processo equo"[72]. Il giudizio di ammissibilità del materiale ottenuto mediante strumenti di captazione dovrà essere svolto sulla base della disciplina processuale interna, ma a condizione che i soggetti coinvolti abbiano potuto esercitare un certo margine di controllo, nonché le rispettive facoltà difensive sulla genuinità ed autenticità dello stesso. È vero che gli strumenti captativi delle attività d'intelligence richiedono peculiarità d'impiego e margini di

[66] Corte di Giustizia dell'Unione Europea (Grande Sezione), 5 aprile 2022, cit. punti da 78 a 81.
[67] Si veda Cass. Pen. 17.5.2019 n. 13425 e Sentenze gemelle n. 113/85 e 389/89.
[68] "obiter dictum" della sentenza della Corte Cost. 269/17.
[69] Così Cass. Sez. 5, 11 dicembre .2012, n. 22577; cfr. Cass. 2 marzo 2005 n. 4466 e Cass. 30 agosto 2004 n. 1735.
[70] V. Ordinanza del 5 aprile 2021 del GIP del Tribunale di Roma. V. anche Cass. 17 maggio 2019, n. 13425.
[71] Così la Corte Giustizia UE, 2 marzo 2021, *Prokuratuur*, C-746/18, EU:C:2021:152, punto 42 e Corte Giustizia UE, 6 ottobre 2020, *La Quadrature du Net* e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punti 222- 223.
[72] Corte Giustizia UE, 2 marzo 2021, *Prokuratuur*, C-746/18, EU:C:2021:152, punto 43 e 44.

segretezza difficili da trasporre in toto nella logica delle garanzie processuali, tuttavia è anche vero che la normativa europea non pone necessariamente una distinzione tra le due distinte attività. Che ciò sia consapevole volontà di eterointegrazione o necessaria indeterminatezza per contesto applicativo non è possibile saperlo, ma esperienze pratiche possono aiutare legislatori ed operatori nell'arduo compito di inquadrare una disciplina di riferimento. Un ordinamento democratico dovrebbe sempre prevedere la concreta possibilità del contraddittorio e di formulare eccezioni ed opposizioni sulla genuinità di quanto ottenuto. In un quadro d'incertezza di lungo periodo, si corre il rischio di sminuire i valori unitari in ordine alla tutela delle libertà fondamentali, ma gli orientamenti giurisprudenziali e normativi mostrano la determinazione verso orizzonti più garantisti in tema di gestione dei dati, anche dinanzi alle irrinunciabili esigenze della sicurezza collettiva. D'altro canto, recenti decisioni hanno mostrato precise indicazioni in merito e non è possibile disattendere tali moniti sulla base di malcelati tentativi di legittimazione supportati dalla ragion di Stato[73]. La recente pronuncia della Corte di giustizia europea HK del 2 marzo 2021 ha, infatti, spinto il nostro legislatore ad un necessario intervento in funzione correttiva onde evitare potenziali contrasti con la disciplina unitaria e, di conseguenza, porre in sufficiente condizione di armonia interpretativa le future decisioni dei giudici nazionali. La decisione dalla Corte si è mossa in maniera proattiva sul tema della gestione dei dati stabilendo che "l'accesso, per fini penali, ad un insieme di dati di comunicazioni elettroniche relativi al traffico o all'ubicazione, che permettano di trarre precise conclusioni sulla vita privata, è autorizzato soltanto allo scopo di lottare contro gravi forme di criminalità o di prevenire gravi minacce alla sicurezza pubblico". Più nello specifico, Il giudizio della Corte ha riguardato l'accesso della pubblica autorità ai dati personali relativi al traffico o all'ubicazione "idonei a fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o sull'ubicazione delle apparecchiature terminali da costui utilizzate e a permettere di trarre precise conclusioni sulla sua vita privata, per finalità di prevenzione, ricerca, accertamento e perseguimento di reati, senza che tale accesso sia circoscritto a procedure aventi per scopo la lotta contro le forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza pubblica". La Corte, nel richiamare le sue precedenti decisioni[74], ribadisce come gli Stati nazionali siano autorizzati a adottare misure legislative che consentano l'accesso ai dati per finalità di prevenzione, ricerca, accertamento e perseguimento dei reati a condizione, però, che vengano rispettati i principi generali del diritto dell'unione tra cui, in particolar modo, il principio di proporzionalità e, più in generale, i principi fondamentali della Carta[75]. Secondo la Corte, in tale contesto "la direttiva osta a misure legislative che impongano ai fornitori di servizi di comunicazione elettronica, in via preventiva, una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione". Più nel dettaglio, affinché venga rispettato il principio di proporzionalità la Corte riconosce come legittimi soltanto di obiettivi della lotta a gravi forme di criminalità e di prevenzione delle minacce alla sicurezza pubblica. Per soddisfare il requisito di proporzionalità, la normativa nazionale deve prevedere regole chiare e precise che disciplinino portata e applicazione della misura, fissando dei requisiti minimi che consentano alle persone interessate dall'accesso ai dati di fruire delle garanzie sufficienti ad una protezione efficace contro i

[73] V. Ubertis, (2017: 3).
[74] Tra tutte, V. Sentenza del 6 ottobre 2020, La *Quadrature du Net* e a., C-511/18, C-512/18 e C-520/18, punti da 166 a 169.
[75] V. Art. 52 comma 1 ed art 53 della Carta.

rischi di abusi[76]. Tale normativa "deve essere legalmente vincolante nell'ordinamento interno e precisare in quali circostanze e a quali condizioni sostanziali e procedurali possa essere adottata una misura che prevede il trattamento di dati del genere, in modo da garantire che l'ingerenza sia limitata allo stretto necessario". Come si può ben evidenziare, la disciplina europea in tema di gestione del dato è foriera di ripercussioni notevoli nelle dinamiche statuali interne e, tuttavia, trattando ancora in modo più o meno esplicito di attività di contrasto al crimine classico ed alla contestuale prevenzione e repressione dei reati, il tutto si amalgama difficilmente con le peculiarità e l'indefinitezza dei fenomeni criminali soggetti alle attività investigative d'intelligence. Ciò non deve scoraggiare operatori e parti coinvolte nel processo di integrazione normativa eurounitaria, in quanto, anche se in linea generale scevri da automatismi di garanzia, casi come l'impiego del software israeliano possono spingere l'opinione pubblica e decisori verso nuovi orizzonti garantisti sull'intero territorio europeo.

## 11. Considerazioni conclusive

Il caso *Paragon* mostra evidenti criticità afferenti alla gestione di sistemi informatici dalla estrema complessità tecnica, frutto di una evoluzione dello stato dell'arte a livelli inimmaginabili. Contemperare esigenze specifiche di tutela della sicurezza collettiva con le contestuali esigenze di tutela delle libertà fondamentali costituisce la più grande sfida per gli addetti ai lavori, anche dei più garantisti ed avveduti. Le recenti vicende mediatiche hanno ancora una volta sollevato questioni ineludibili di carattere pratico, potenzialmente impattanti nella vita privata di ciascun individuo. Non è pensabile, in tal senso, una indifferenza del sistema politico nel suo ruolo attivo di determinazione della pacifica convivenza civile! È indispensabile, al fine di evitare derive critiche e chine scivolose verso estremi applicati delle tecnologie captative, portare all'attenzione dell'opinione pubblica casi come quello ricostruito nello studio e le relative problematiche in termini di approccio regolatorio e gestionale. Le ripercussioni, nel caso di uso inappropriato degli applicativi simili al *software Grafite* sono notevoli non solo per i singoli soggetti interessati alle attività investigative, ma anche alla generale tenuta degli equilibri di contemperamento tra le esigenze di tutela della sicurezza pubblica e la garanzia del rispetto di valori fondamentali della riservatezza e del diritto di cronaca. L'eterogenesi dei fini, elemento cardine del ragionamento proposto nel contributo, è rinvenibile nel generale senso di sfiducia determinato nella generalità dei consociati, i quali affidano la garanzia dell'incolumità pubblica, dinanzi alle minacce esterne, alle autorità preposte al ruolo di garanti della sicurezza, senza, però, compromettere il rispetto dei valori fondamentali della riservatezza e della privacy. L'impiego di sistemi altamente sofisticati, potenziati da un notevole progresso tecnologico ed informatico, non dovrebbe rappresentare la scusa per approfittare del potenziale offerto dalla scienza investigativa e dalle evoluzioni captative conseguenti all'introduzione di moderni algoritmi e apparati per l'acquisizione di metadati e comunicazioni riservate. Tuttavia, casi emblematici dimostrano quanto il confine tra uso legittimo ed abuso inopportuno dei sistemi sia sottile e come le autorità, per svariati motivi, possono impunemente abusare delle prerogative riversate alle autorità statuali per la difesa dell'ordine collettivo, eludendo controlli e supervisione attenta delle disfunzioni. Non meno importanti risultano essere le tutele dell'autonomia di corpi sociali coinvolti in operazioni a carattere umanitario le quali, sempre nel

[76] V. Caianello (2014: 143); Conti (2019: 2: 1575); Kostoris (2018: 120); Marchese (2016: 381).

rispetto di parametri oggettivi di adeguatezza delle operazioni di supporto e soccorso svolte, non dovrebbero, allo stesso tempo, subire le pressioni e le interferenze di iniziative fuori dai margini della regolarità istituzionale. L'elemento di raccordo, in un simile scenario di ripercussioni pratiche durante le regolari attività dei servizi o operatori di sicurezza statuali, potrebbe essere determinato da un approccio sempre orientato al rispetto delle riserve di strutture ordinamentali funzionali a garantire il cittadino da interferenze esterne e non ad abusare degli strumenti che la tecnologia moderna offre. Una ricerca dell'università di Toronto (*Citizen lab*) ha evidenziato come l'intrusione del *software Graphite*, venduto ai Governi nazionali per la meritevole lotta al crimine, sia in realtà stato impiegato per finalità da accertare e preoccupanti, qualora confermate, di controllo negli smartphone di attivisti, preti e giornalisti. Il documento redatto dal gruppo di ricerca, nella sua interezza, analizza i vari passaggi del caso paragonandolo ad "un'arma ipersonica nel mondo della sicurezza". Il caso *Paragon* dimostra in ogni caso che uno strumento molto costoso è in grado di operare indisturbato sulle principali piattaforme commerciali di comunicazione e può essere costruito ad arte, non da una semplice impresa privata, ma da un'azienda che tra i soci fondatori vede *ex* primi ministri ed *ex* comandanti dei servizi d'intelligence israeliani. Nonostante *Graphite* sia un *software* costruito al servizio di agenzie governative di paesi democratici per il fine legittimo della lotta contro gravi crimini, ciò non è stato sufficiente ad evitarne un impiego che sembrerebbe essere in netto contrasto con la sua missione principale. Il caso è stato aperto nel gennaio 2024 in seguito agli *Alert* della società di gestione delle app di messaggistica coinvolte (*Meta*), con un semplice messaggio in cui avvisava come "a dicembre *whatsapp* avesse interrotto le attività di una società *spyware* che si ritiene abbia attaccato il dispositivo"[77]. Non è ancora molto chiaro come proseguirà la vicenda, anche se molte procure si stanno già interessando e vi è anche un forte interesse del Parlamento europeo e dei nostri apparati di garanzia, primo su tutti il Copasir. D'altro canto, la linea politica del Governo sembrerebbe essere orientata al continuo inasprimento delle misure riguardanti il tema della sicurezza nazionale e delle attività di intelligence. Nel dibattito parlamentare afferente all' *iter* di approvazione del recente DDL Sicurezza, che interviene sul contrasto al terrorismo e alla criminalità organizzata e sui controlli di polizia, si aumentano anche i poteri dei servizi segreti. La modifica rende permanenti alcuni principi stabiliti dalla disciplina transitoria del 2015, emanata a suo tempo nell'ottica dell'emergenza, rappresentata dal contrasto del terrorismo religioso, intervenendo su alcune scriminanti e su alcune condotte, previste dalla legge come reato, che, in presenza di valide giustificazioni, il personale dei servizi è autorizzato a realizzare senza ripercussioni in ordine alla loro responsabilità. Scriminanti, quali ad esempio la partecipazione ad associazioni sovversive, l'arruolamento con finalità di terrorismo anche internazionale e la banda armata, sarebbero ulteriormente arricchite con la possibilità di una direzione e organizzazione di associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico, detenzione di materiale con finalità di terrorismo, fabbricazione o detenzione di materie esplodenti, istigazione a commettere delitti di terrorismo o crimini contro l'umanità, senza alcuna ripercussione per gli operatori dei servizi, anzi attribuendo loro la possibilità non solo di infiltrare tali organizzazioni, ma, anche, di dirigerle con una vera e propria "licenza criminale"[78]. Desta qualche perplessità l'assenza di una contestuale implementazione e rafforzamento dei poteri del Copasir, l'unico organismo parlamentare, espressione della rappresentatività popolare, in grado di controllare le attività dei servizi e di verificare che le stesse

[77] Per un'analisi approfondita del report V. B. Marczak, J. S. Railton, K. Robertson, A. Perry, R. Brown, B. A. Razzak, S. Anstis, and R. Deibert, (2025).
[78] Così Scarpinato, ex magistrato e senatore della repubblica.

siano condotte con modalità in grado di garantire il rispetto delle leggi e delle libertà costituzionali nell'esclusivo interesse della nazione[79]. Il decreto, approvato attraverso un particolare *iter* parlamentare, ha destato critiche e remore da parte della comunità politica, accademica e giurisprudenziale non solo per l'atipica procedura di rideterminazione dei vari passaggi parlamentari del testo, ma, anche, per innumerevoli riserve di costituzionalità generali sollevate dal capo dello Stato e dalla Corte di Cassazione[80]. Il caso Paragon dimostra quanto sia necessaria l'attenzione dell'opinione pubblica e di corpi sociali dinanzi a potenziali fenomeni di abuso dell'autorità o a impieghi non ortodossi di strumenti innovativi, costruiti inizialmente per finalità legittime di contrasto al crimine internazionale, ma potenzialmente trasmutabili in perniciosi artifici della tecnica informatica per improprie acquisizioni comunicative. Per concludere, è indubbio che sistemi come *Paragon* non siano gli unici con il potenziale critico di un'alterazione della regolare vita democratica, e che, alla luce dell'evoluzione della tecnica, possano persino emergere dipiù pericolosi ed invasivi per la vita privata. È vero, però, che una sottovalutazione d'insieme dei rischi connessi agli usi impropri di strumenti concepiti per finalità legittime non si addice all'architettura normativadi uno Stato di diritto maturo ed evoluto. Nel quadro d'insieme non solo il decisore politico, ma soprattutto, la società civile, dovrebbero assumere rispettivamente il ruolo di garante e disupervisore  attento contro fenomeni distorsivi dell'ordine costituzionale.

**Bibiliografia**

Ackerman, B. 2005, *La Costituzione di emergenza. Come salvaguardare libertà e diritti civili di fronte al pericolo del terrorismo*, Roma.Bartoli, B. 2010, *Regola ed eccezione nel contrasto al terrorismo internazionale*, in Dir. Pubbl., febbraio, 329.

Bertolucci, F. 2025, *Dati digitali e sequestro: un'apparente inversione di rotta*, su *Discrimen*, rivista *online*, 18 luglio.

Bobbio, N. *Democrazia e segreto*, Einaudi, 2011.

Bonetti, P. 2006, *Terrorismo, emergenza e costituzioni democratiche*, Bologna.

Bosco, F. 2012, *Cyberterrorismo e cyberwarfare: profili giuridici e analisi della casistica a livello internazionale*, in Cassano, G., Scorza, G.,Vaciago, G., (a cura di), Diritto dell'Internet. Manuale operativo. Casi, legislazione, giurisprudenza, Cedam, Padova.

Caianello, M. 2014, *Il principio di proporzionalità nel procedimento penale*, in *Dir. pen. cont.*, Riv. trimestrale, 3-4, 143.

Cantone, R. – D'Angelo, L. A. 2006, *Una nuova ipotesi di intercettazione preventiva,* in Aa. Vv., *Le nuove norme di contrasto al terrorismo,* a cura di A.A. Dalia, Giuffrè, 2006, 54.

Carli, C. 2013, *Cyber warfare* vs leggi umanitarie, in Informazioni della Difesa, marzo.

Cascini, G. 2025, *Durata massima delle intercettazioni (45 giorni: l. n. 47/2025 e nuovo art. 267, co. 3 c.p.p.): tra problemi interpretativi, irrazionalità e incongruenze,* su *Sistema penale,* rivista *online*, 3 giugno.

Conti, C.2019, *Sicurezza e riservatezza*, in *Dir. pen. proc.*, 2, 1575.

Curtotti, D. 2018, *Procedimento penale e intelligence in Italia: un'osmosi inevitabile, ancora orfana di regole*, in *Proc. pen. giust.*, f. 3, 438.

Delle Fave, C. 2013, *Manuale di polizia giudiziaria*, Milano.

[79] Per un approfondimento completo sul tema si veda il testo integrale del DDL Sicurezza atto Senato n. 1236.

[80] Si rinvia in tal senso all'analisi approfondita del testo convertito con legge 9 giugno 2025, nonché alla relazione dell'ufficio del massimario della corte di Cassazione n.33/2025.

Filippi, L. 2020, *Il virus trojan: uno strumento nelle mani incontrollabili della polizia giudiziaria*, del 30 novembre, su *Penale, diritto procedura*, rivista *online*.

Flor, R. 2017, *Cyber*-terrorismo e Diritto Penale in Italia, in Diritto Penale e Modernità. *Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali*, Atti del convegno Trento 2 e 3 ottobre 2015, Università degli Studi di Trento, Quaderni della facoltà di Giurisprudenza,Fornasari,G, Wenin, R. (a cura di), Trento.

Gatta, G. L. 2025, *Durata massima delle intercettazioni (45 giorni). Note a caldo sulla legge Zanettin*, su *Sistema penale*, rivista *online*, 3, 24 marzo.

Ghidotti, C. 2019, Exodus, eSurv: *storia di uno spyware italiano*, su punto-informatico, sito *online* del 20 marzo.

Guarnera, P. 2015, Cass.pen., 10 novembre, in *Arch. pen.*, 2016 (1), 212, con nota di Testaguzza, A, *Chat BlackBerry: sistema "pin-to-pin"*.

Jacobazzi, G. M. 2021, *Intercettazioni, contratti secretati. Il Copasir ora chiede chiarezza*, su "il Dubbio", quotidiano *online* del 23 ottobre.

Kostoris, R. E. 2018, *Processo penale e paradigmi europei*, Torino, 120

Kostoris, R. E. (a cura di) 2016, *Principio di proporzionalità, diritti fondamentali e processo penale, in Percorsi giuridici della postmodernità*, a cura di, Bologna, 381.

Marczak, B 2025, Railton,J.S. Robertson, K., Perry,A., Razzak,B.A, Anstis,S., And Deibert,R.*Virtue or vice? An initial analysis of Paragon's expanding spyware operations* del 19 marzo, sul sito ufficiale del gruppo di ricerca.

Murone, M. S. 2021, *Brevi note sul rapporto tra trojan horse e libertà di autodeterminazione*, del 12 febbraio, su *Penale, diritto e procedura*, rivista *online*.

Nicolicchia, F. 2018, *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, su *Dir. Pen. Contemp.*, rivista *online*.

Ruotolo, M. 2013, *Diritto alla sicurezza e sicurezza dei diritti*, in Democrazia e sicurezza, III, 2.

Salazar, C. 2015, *I principi in materia di libertà*, in Ventura,L., Morelli, A., (a cura di), *Principi costituzionali*, cit., 203 ss.

Signorato, S. 2018, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino.

Spangher, G. 2009, *Trattato di Procedura penale*, 3. Torino, 49-51.

Tartara, V. 2022, *La corte di giustizia conferma il "divieto di conservazione generalizzata e indiscriminata" dei dati relativi al traffico delle comunicazioni elettroniche per finalità preventive di contrasto alla criminalità. possibili ricadute nell'ordinamento italiano*, su sistema penale, rivista *online*.

Torre, A. 2013 (a cura di) *Costituzioni e sicurezza della Stato*, Bologna.

Ubertis, G. 2017, *Equità e proporzionalità versus legalità processuale: eterogenesi dei fini?* in *Arch. Pen.*, 3 (rivista web).

Vele, A. 2011, *Le intercettazioni nel sistema processuale penale: tra garanzie e prospettive di riforma*, Padova.

nicolascerbo@hotmail.it

Pubblicato online il 21 settembre 2026