NICOLA SCERBO

Equilibrio tra esigenze di tutela della sicurezza collettiva e tutela delle libertà fondamentali. Nuove tecnologie nella giustizia penale? *A.I.* (*artificial intelligence*), *Trojan horse* (captatore infomatico) e gestione dei dati da parte dell'autorità come *case studies*.

L'idea di acquisire maggiore consapevolezza delle principali criticità relative al delicato equilibrio tra esigenze di garanzia della sicurezza collettiva e rispetto delle libertà fondamentali ha richiesto la necessità di interfacciarsi con esperienze concrete nella realizzazione di investigazioni innovative (*Trojan*), nonché sull'impatto delle moderne tecnologie di intelligenza artificiale nel sistema penale. Non è mancata inoltre la possibilità di affrontare le vulnerabilità, legate ad un uso improprio, dell'enorme mole di dati a disposizione degli investigatori nella moderna società digitale. Il sistema delle garanzie elementari dell'ordinamento costituzionale e convenzionale nel contesto europeo dovrebbe garantire un argine ben consolidato alle derive autoritarie da regime poliziesco, ma il pericolo di suggestioni e fascinazioni anacronistiche è sempre dietro l'angolo e, chissà, dato i precedenti nelle politiche di lotta al terrorismo, potrebbero sempre avvolgere le più lodevoli iniziative di contrasto alla criminalità in una vorticosa spirale di violazioni delle libertà fondamentali. La raccolta sistematica del materiale, necessario per l'approfondimento, non ha deluso le aspettative inerenti al difficile compito dello studioso nel razionalizzare componenti molto eterogenee attinenti allo stesso tema, alcune di carattere estremamente tecnico e specialistico, altre, dalla forte componente umanocentrica, estremamente aleatoria e soggetta a variabili profonde, legate al contesto di riferimento. La questione decisiva è ricercare un equilibrio tra le esigenze di tutela della sicurezza collettiva e la necessaria tutela delle libertà fondamentali, costantemente messe in pericolo dalle pressioni emotive della gestione del rischio securitario, legate al potenziale danno a beni giuridici fondamentali quali la vita privata e la sicurezza pubblica. Ordine, soggetto a fenomeni creativi della criminalità organizzata, il più delle volte indefiniti nel tempo e nello spazio, ma anche oggetto di un pronto e attento interesse del legislatore, spesso affascinato da facili soluzioni di breve termine incuranti delle conseguenze di lungo termine nell'architettura degli equilibri democratici dei moderni Stati di diritto.

Belance between the needs of protecting collective security and protection of fundamental freedoms. New technologies in criminal justice? A.I. (artificial intelligence), Trojan Horse (computer sensor) and Data management by the authority as case studios.

The idea of acquiring greater awareness of the main critical issues relating to the delicate balance between the needs of guaranteeing collective security and respect for fundamental freedoms required the need to interface with concrete experiences in the implementation of innovative investigation (trojans), as well as the impact of modern artificial intelligence technologies in the criminal system. There was also no lack of the possibility of addressing the vulnerabilities, linked to improper use, of the enormous amount of data available to investigators from modern digital society. The system of basic guarantees of the constitutional and conventional system in the European context should guarantee a well-established barrier to the authoritarian drifts of the police regime, but the danger of anachronistic suggestions and fascinations is always around the corner and, who knows, given the precedents with loose ends in policies to combat terrorism, could always envelop the most laudable law enforcement initiatives in the fight against crime in a swirling spiral of violations of fundamental freedoms. The systematic collection of the material, necessary for in-depth study, has not disappointed the expectations inherent in the difficult task of the

scholar in rationalizing very heterogeneous components pertaining to the same theme, some of an extremely technical and specialized nature, others, by virtue of the strong human-centric component, extremely random and subject to profound variables linked to the reference context. The decisive issue is to seek a balance between the needs for the protection of collective security and the necessary protection of fundamental freedoms, constantly placed in danger by emotional pressures of risk management, linked to the potential damage to fundamental legal goods such as life and public order, subject to creative phenomena of organized crime, most of the time indefinite in time and space, but also the object of a ready and careful interest of the legislator, often fascinated by easy short-term solutions regardless of the consequences of long term in the architecture of the democratic balances of modern states of law.

1.*Introduzione*. L'attività di ricerca è stata finalizzata ad indagare un tema di pervadente attualità: la coesistenza equilibrata fra le esigenze di garanzia e promozione delle libertà e dei diritti inviolabili dell'uomo, elemento strutturale del sistema costituzionale democratico, e quelle, altrettanto cruciali, di tutela della sicurezza collettiva, messa costantemente in pericolo da minacce di natura criminale.

Gli attentati alle torri gemelle del 2001 hanno stravolto il paradigma dei sistemi democratici moderni, investendone massicciamente i principi cardine di libertà individuale e collettiva alla base dei meccanismi di interazione del processo di sviluppo economico, infrastrutturale e politico sociale del liberismo novecentesco.

Uno dei principali dilemmi innanzi al quale il decisore si è trovato a ragionare è stato il costante contemperamento nell'intensità delle misure di restrizione poste ai diritti fondamentali, fulcro del moderno costituzionalismo, a fronte delle pressanti esigenze di tutela della sicurezza degli individui, degli Stati e delle loro istituzioni, senza incorrere nell'aberrante effetto di negarli in nome di una protezione degli stessi.

L'imprevedibilità e la portata destabilizzante delle azioni di natura criminale, potrebbero, infatti, condurre il decisore a adottare misure in contrasto con

l'obiettivo alla base della loro predisposizione, generando un mostro giuridico di perfetta eterogenesi dei fini, precursore del male stesso contro il quale opporsi.
La dottrina ha sempre evidenziato come il tema della tutela della sicurezza risulti fondamentale ai fini dell'ordinato svolgimento del vivere civile ed abbia rappresentato il fulcro nella costituzione delle moderne teorie dello Stato. Già Hobbes fondava il patto sociale, quale veicolo per condurre gli uomini oltre lo stato di natura, sull'esigenza di autoconservazione[1].
Nell'ambito del costituzionalismo liberale, il concetto di sicurezza ha sempre rivestito un ruolo cardine connesso alle trasformazioni dei compiti dello Stato ed all'affermazione dei diritti inviolabili dell'uomo, in particolar modo con riferimento alle libertà negative, implicanti il riconoscimento e la salvaguardia delle autonomie del singolo da qualsiasi interferenza degli altri consociati, ma soprattutto da parte degli stessi pubblici poteri, il cui intervento era ammesso soltanto in funzione repressiva e sanzionatoria di eventuali violazioni. Tutto ciò accentuava il profilo materiale ed interno della sicurezza, legato alla garanzia della pacifica convivenza dei consociati ed alla salvaguardia dei diritti fondamentali dei cittadini (libertà da).
Le tensioni sociali generate progressivamente dalla rivoluzione industriale connotarono in senso maggiormente ideale il concetto di sicurezza, quale tutela dei principi fondanti lo stato liberale borghese, facendo evolvere i compiti del potere statale che si dispiegavano non più solo in termini negativi di non interferenza, ma anche in chiave positiva di promozione dei diritti della persona (sicurezza di).
L'art. 3 della Costituzione italiana racchiude emblematicamente tale codificazione di principio dove, nella sua articolazione impegna esplicitamente la Repubblica a rimuovere gli ostacoli di ordine economico e sociale che, limitando di fatto la libertà e l'uguaglianza, impediscono il pieno sviluppo della persona. Da tale lettura, emerge come la sicurezza rappresenti un valore tutelato in via

[1] Secondo tale approccio, il conferimento delle prerogative in merito alle libertà individuali ad una autorità suprema conduceva alla nascita dello Stato, il quale attraverso il monopolio nell'uso della forza, si faceva carico di salvaguardare la sicurezza dei cittadini. Per approfondimenti sul tema si veda HOBBES, *Leviatano,* Roma 1980.

ordinaria, anche laddove non sia connesso a situazioni di emergenza politico istituzionale.
Tuttavia, nel momento in cui tali esigenze si sono presentate, è accaduto che le stesse abbiano assunto un peso maggiore nel contemperamento dei principi e diritti costituzionalmente garantiti.
Il decisore, indotto dalla paura che simili eventi generano nella popolazione, ha messo in atto misure restringenti le quali, all'apparenza in grado di rassicurare, di fatto hanno limitato diritti e libertà fondamentali. In nome delle ragioni della sicurezza, si è posto più volte il rischio di uno scivolamento dallo stato di diritto verso lo stato di prevenzione dove le ragioni di sicurezza rischiano di assumere il ben più eloquente e rischioso tenore di ragion di Stato[2].
Per riassumere il concetto nelle parole di Silvestri, "*se è vero che non può esserci libertà senza sicurezza dello Stato e delle sue istituzioni, è pur vero che la sicurezza non rappresenta un valore assoluto e, dunque, negli stati democratici ha senso solo se funzionale all'effettiva tutela dei diritti e delle libertà fondamentali*". Da ciò ne deriva come la più grande sfida per il decisore, ed il legislatore in primis, sia quella di riuscire a dare risposte che non si pongano in contrasto o addirittura violino i principi stessi dello Stato di diritto su cui essi si basano. In tali sistemi non è concesso utilizzare ogni possibile mezzo per difendersi dai propri nemici né si può negare all'eventuale criminale la dignità e quegli stessi diritti fondamentali riconosciuti ad ogni individuo[3].
Le misure normative che sono state adottate sull'onda dell'emergenza, come dimostrano anche i più recenti provvedimenti legislativi italiani, hanno fatto ricorso a soluzioni particolarmente restrittive che spaziano dalla previsione di norme incriminatrici nuove e più aspre a quelle di misure di prevenzione più stringenti, comprese deroghe al sistema processuale, più ampi poteri di polizia

[2] Si veda TORRE (a cura di) *costituzioni e sicurezza della Stato,* Bologna 2013; BONETTI, *Terrorismo, emergenza e costituzioni democratiche,* Bologna 2006*;* RUOTOLO, *Diritto alla sicurezza e sicurezza dei diritti*, in *Democrazia e sicurezza*, 2/2013; BARTOLI, *Regola ed eccezione nel contrasto al terrorismo internazionale,* in *Dir. Pubbl.,*1-2/2010, 329 ss.
[3] Si veda anche SALAZAR, *i principi in materia di libertà,* in VENTURA, MORELLI (a cura di), *principi costituzionali,* cit., 203 ss.; ACKERMAN, *La Costituzione di emergenza. Come salvaguardare libertà e diritti civili di fronte al pericolo del terrorismo, Roma 2005;* GAMBINO, SCERBO, *Diritti fondamentali ed emergenza nel costituzionalismo contemporaneo. Un'analisi comparata,* in *Dir. Pubbl. comp. Eur., 4/2009, 1497 ss.*

e di *intelligence*, nonché forti interferenze dei poteri pubblici nella *privacy* delle persone[4].

Il problema principale, posto in passato e che continua a manifestarsi, consiste nel fatto che, una volta placata l'onda dell'emergenza, tali misure tendono a permanere nell'ordinamento quando, invece, occorrerebbe rivalutarne proporzionalità e adeguatezza[5].

Dunque, nelle scelte di politica criminale, vi è in gioco il rapporto tra la sfera dei diritti individuali e quella dei poteri statuali sanzionatori. Il diritto penale, da un lato protegge quegli interessi meritevoli di tutela su cui il legislatore pone l'attenzione e dall'altro incide in modo restrittivo sugli stessi beni che intende tutelare. Il pericolo è che il diritto penale del fatto si trasformi in diritto d'autore e che l'arretramento della soglia di punibilità porti allo sconfinamento verso la repressione di forme di manifestazione del pensiero o, peggio ancora, che il

[4] I più recenti studi hanno dimostrato come i più recenti atti terroristici europei siano stati perpetrati nella quasi totalità non da immigrati stranieri, ma da cittadini europei di seconda o terza generazione. Ulteriore aspetto socioculturale da tenere in considerazione sono le politiche di integrazione messe in atto nel corso degli anni in Europa ed Italia. Il loro fallimento deriva dal fatto che proprio nella marginalizzazione socio culturale ed economica che le caratterizza matura il seme del fondamentalismo di matrice religiosa ed il sovvertivismo anarco insurrezionalista; all'interno dei contesti di degrado ed isolamento tipici della ghettizzazione si radicano le idee che portano alle conseguenze contro le quali si lotta, in società indifferenti evidentemente incapaci di trasmettere e soprattutto rendere effettivo il concreto valore dei principi di libertà, uguaglianza, solidarietà e giustizia, sui quali, almeno in teoria si fonda lo stato di diritto. Per approfondimenti sul tema si veda J*ihadista della porta accanto. Radicalizzazione e attacchi jihadisti in Occidente* di VIDINO, MARONE, ENTENMANN, Traduzione dall'inglese (*Fear Thy Neighbor. Radicalization and Jihadist Attacks in the West, ISPI*, 2017) a cura di CARENZI.

[5] Si è venuto così a configurare un diritto penale del nemico in contrapposizione a quella che dovrebbe essere il diritto penale del fatto, attraverso misure che rispondono in via immediata all'esigenza rassicurante di sicurezza. Sono stati adottati più volte provvedimenti connessi all'appartenenza a determinati gruppi etnici o razziali, quali indicatori di particolare pericolosità sociale, oppure è stata avviata l'applicazione di particolari misure di prevenzione nonché il potenziamento dell'impiego di provvedimenti amministrativi incidenti sulla libertà di circolazione o di soggiorno, ma adottati al di fuori del circuito di garanzie del processo penale. A tal riguardo si veda BASSU, *Terrorismo e costituzionalismo. Percorsi comparati,* Torino 2010; R. BARTOLI, *Il terrorista internazionale: criminale, nemico o nemico assoluto?* entrambi in AA.VV., *I diritti dei nemici,* in *Quaderni fiorentini*, Milano 2009, 1706 ss. 1727 ss.; VIGANO', *Pubblicato sulla gazzetta ufficiale il nuovo decreto legge in materia di contrasto al terrorismo,* in www.penalecontemporaneo.it, *23 Febbraio 2015.*

soggetto interessato venga punito non più per quello che fa, ma per quello che è.[6]

2. *Le nuove tecnologie nel sistema penale.* L'acquisizione delle comunicazioni telefoniche e telematiche mediante l'impiego di moderni strumenti di captazione informatica (*trojan*), estremamente invasivi ed enormemente vulnerabili a distorsioni abusive durante il loro impiego nelle attività investigative, hanno caratterizzato le discussioni critiche degli addetti ai lavori fin dai suoi primi impieghi quale fondamentale strumento di ricerca della prova.
L'acquisizione dei cosiddetti dati esterni relativi al traffico informatico e telematico e di ogni altra informazione utile in possesso degli operatori di telecomunicazioni ha suscitato di recente l'interesse del legislatore, tanto da portarlo ad emanare d'urgenza notevoli correttivi normativi, soprattutto, in virtù delle efficaci e nette prese di posizione della giurisprudenza europea a riguardo, particolarmente attenta e sensibile al tema del rispetto della vita privata nel contrasto ad attività criminali di una certa rilevanza.
Ultimo, ma non per importanza, l'impiego di moderni strumenti di elaborazione computazionale di autoapprendimento, altrimenti detta *A.I* (*Artificial Intelligence)*, basati sulla costruzione di specifici algoritmi (*software*) in grado di alimentare un sistema progressivo ed automatizzato di ricerca delle innumerevoli possibili correlazioni con modelli di riferimento agglomerati in appositi contenitori di dati, stoccati in strutture fisiche di memoria (*hardware*).
L'attività di ricerca svolta, durante il percorso di dottorato, ha permesso un approfondimento delle tematiche oggetto del progetto introduttivo, concluso alla stregua degli indirizzi programmatici inizialmente approntati.
L'idea di acquisire una maggiore consapevolezza, circa le principali criticità afferenti al tema del delicato equilibrio tra le esigenze di garanzia della sicurezza collettiva ed il rispetto delle libertà fondamentali, ha consentito la possibilità di

[6] Al riguardo si veda BOSCO, *Cyberterrorismo e cyberwarfare: profili giuridici e analisi della casistica a livello internazionale*, in CASSANO, SCORZA, VACIAGO (a cura di), *Diritto dell'Internet. Manuale operativo. Casi, legislazione, giurisprudenza*, Cedam, Padova, 2012; CARLI, *Cyber warfare vs leggi umanitarie*, in Informazioni della Difesa, 5/2013; FLOR, *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, WENIN (a cura di), Trento, 2017.

interfacciarsi con esperienze concrete nell'implementazione di innovativi strumenti di indagine (*trojan*), nonché l'impatto delle moderne tecnologie di intelligenza artificiale nel sistema penale.
Non è mancata, anche, la possibilità di affrontare le vulnerabilità, legate ad un uso, improprio, dell'enorme mole di dati a disposizione degli inquirenti dalla moderna società digitale.
Il tema, a dire il vero, è già stato oggetto di numerose considerazioni degli addetti ai lavori, frutto anche dell'enorme impatto espansionistico dovuto alle logiche emergenziali connaturate alle politiche criminali *post* attentato alle torri gemelle. La pandemia da *coronavirus* ed il conflitto ucraino, nostro malgrado, hanno esacerbato ulteriormente la percezione generalizzata e manichea dell'eterna lotta tra bene e male, in una rafforzata logica di relazione amico-nemico, generalmente intesa come arte del possibile, ad ogni costo, anche del sacrificio di valori connaturati alle moderne democrazie occidentali.
La raccolta sistematica del materiale, necessario all'approfondimento, non ha deluso le aspettative inerenti al difficile compito dello studioso nel razionalizzare componenti molto eterogenee afferenti al medesimo tema, alcune di carattere estremamente tecnico e specialistico, altre, in virtù della forte componente umanocentrica, estremamente aleatorie e soggette a profonde variabili legate al contesto di riferimento.
La possibilità, ad esempio, di considerare l'uso dell'intelligenza artificiale nell'ambito del processo penale quale opportunità indefettibile di supporto all'attività cognitiva del giudice, piuttosto che un enorme pericolo per il sistema di garanzie della persona sottoposta a cognizione, potrebbe variare sensibilmente da sistema a sistema, anche con simili valori di riferimento.
Potrebbe sorgere spontanea la domanda su come sia possibile una così accentuata divergenza nell'approccio ad un sistema tecnologico concepito e sviluppato con le medesime regole matematiche ed ingegneristiche, valide in ogni parte del globo. La risposta non è semplice e, così come per le altre questioni affrontate nel percorso di ricerca, non ha risposta univoca, ma dipende e dipenderà molto, anche nel futuro prossimo, dalle sensibilità specifiche del target di riferimento, anche alla luce delle necessità specifiche di politica criminale poste all'attenzione del legislatore di turno.

Il sistema delle garanzie di fondo del sistema costituzionale e convenzionale in ambito europeo dovrebbe garantire un argine ben consolidato alle derive autoritarie da regime di polizia, ma, il pericolo di suggestioni e fascinazioni anacronistiche è sempre dietro l'angolo e, chissà, visti i precedenti a maglie larghe nelle politiche di contrasto al terrorismo, potrebbe sempre avvolgere in una spirale vorticosa di violazioni alle libertà fondamentali le più lodevoli iniziative di *law enforcement* nell'attività di contrasto al crimine.

3. *L'A.I. e le sue implicazioni per il sistema penale.* La velocità disarmante con la quale una simile tecnologia sta progressivamente interessando ogni aspetto del vivere quotidiano, ha parallelamente iniziato a coinvolgere settori più sensibili, quali la giustizia e, più in generale, tutto il settore delle indagini, spingendo studiosi e, non solo, a chiedersi quali possano essere le possibili implicazioni nell'impiego di simili strumenti in dinamiche afferenti alla tutela delle più svariate libertà individuali, personale, di pensiero, di riservatezza ecc[7].
Non mancano esempi pratici nell'impiego di sistemi sperimentali di intelligenza artificiale in ambito penale, anche se le esperienze più significative al riguardo provengono per il momento da realtà non perfettamente in linea con il sistema di garanzie della realtà europea[8].
Il più interessante e, allo stesso tempo, inquietante impiego dell'intelligenza artificiale, soprattutto alla luce dei suoi possibili esiti sugli aspetti più delicati della libertà individuale, riguarda il cosiddetto impianto di giustizia predittiva,

[7] Al riguardo si veda BACCARI e MARRAFFINO, Le prospettive di utilizzo delle *chatbot* nel procedimento penale, in Dir. pen. proc., 2021, n. 8, p. 1008 ss.; NAGNI, Artificial intelligence, l'innovativo rapporto di (in)compatibilità fra machina sapiens e processo penale, in questa Rivista, 2 luglio 2021; DELVECCHIO, L'informatizzazione della giustizia penale, in Dir. pen. cont. – Riv. trim., 2021, n. 2, p. 60 ss; Predizione decisoria, diversion processuale e archiviazione, in Dir. pen. cont. – Riv. trim., 2021, n. 2, p. 42 ss. LAVORGNA e SUFFIA, La nuova proposta europea per regolamentare i Sistemi di Intelligenza Artificiale e la sua rilevanza nell'ambito della giustizia penale, in Dir. pen. cont. – Riv. trim., 2021, n. 2, p. 88 ss. SALVADORI I., Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale, in Rivista italiana di diritto e procedura penale, 2021, n. 1, p. 83 ss.; ID., Il diritto penale dei software a "duplice uso", in WENIN, FORNASARI (a cura di), Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali, Napoli, 2017, p. 361 ss. (B.P.).

[8] La commissione europea per l'efficienza della giustizia ha elaborato nel 2018 la *Carta etica per l'impiego dell'intelligenza artificiale nei sistemi giudiziari ed ambiti connessi*. Per ulteriori approfondimenti si veda al seguente link: https://rm.coe.int/carta-etica-europea-sull-utilizzo-dell-intelligenza-artificiale-nei-si/1680993348.

altrimenti inteso come sistema che consenta di prevedere il possibile esito di una controversia in virtù dei precedenti esiti di casi analoghi[9].
Come sostenuto dal Presidente della Corte di appello di Brescia, Claudio Castelli «In realtà la prevedibilità è un enorme valore e la predittività non è che lo sviluppo della prevedibilità delle decisioni. Prevedibilità significa certezza del diritto, perché quanto conta oltre alle norme sono le interpretazioni che le trasformano in diritto vivente, ovvero la concreta possibilità di godere di un diritto. Le diverse interpretazioni non dipendono solo e fondamentalmente da opzioni valoriali diverse, ma dalla complessità ed incertezza dell'attività di interprete in un momento ed in un assetto come l'attuale in cui abbiamo una realtà multifonte in rapida evoluzione che impongono la ricostruzione dell'ordinamento e della gerarchia delle fonti[10]».
Le opzioni tecnologiche disponibili alimentano il timore circa la possibile visone meccanicistica del ruolo del giudice, edulcorato o, se si vuole, mascherato dall'impiego delle nuove tecniche nella prospettiva di decisione automatizzate ed indifferenti alla realtà umana[11].
Si tratta di una prospettiva molto inquietante, alla quale si potrebbe dare risposta concreta alimentando il grado di consapevolezza sull'esistenza di possibili fattori esterni ed interni, dal potenziale condizionante in merito a decisioni sensibili, nel tentativo di sterilizzarne gli effetti principali attraverso l'uso di una discrezionalità ragionata, motivata e trasparente.
In pratica, non una vera e propria sostituzione del giudice con la macchina, ma un contributo che può essere erogato dall'intelligenza artificiale alla sua già

[9] In materia il contributo ed il dibattito dottrinale sono enormi. Solo per citarne alcuni, CADOPPI, Giudice Penale e giudice civile di fronte al precedente, in Indice penale, 2014, p. 14 ss; COSTANTINO, La prevedibilità della decisione tra uguaglianza e appartenenza, Relazione all'XI assemblea degli osservatori civili, 2016; SALVANESCHI, Diritto giurisprudenziale e prevedibilità delle decisioni: ossimoro o binomio, Relazione all'XI assemblea degli osservatori civili, 2016; VIGANÒ, Il principio di prevedibilità della decisione giudiziale in materia penale, in Diritto penale contemporaneo, 19 dicembre 2016; XII Assemblea Nazionale degli Osservatori – Roma 2017 Gruppo di lavoro – Prevedibilità delle decisioni e dialogo fra i diversi gradi della giurisdizione.
[10] Per approfondimenti sul tema si veda *giustizia predittiva* a cura di CASTELLI, in Q*uestione Giustizia,* rivista online*, 08/02/2022.*
[11] Timori rappresentati anche dal Report del Gruppo 1 Prevedibilità, predittività e umanità del giudicare della XIII Assemblea Nazionale degli Osservatori sulla giustizia civile.

innata capacità di elaborazione dei dati, ma velocizzandone notevolmente i tempi.
Da tali considerazioni emerge come i sostenitori di un uso sostitutivo dell'*A.I.,* mediante decisioni automatizzate, sull'assunto di possibili risvolti positivi in termini di oggettività, non suscettibilità a pressioni esterne, ma, soprattutto, tempistiche più brevi, non si rendano conto delle possibili conseguenze di una simile determinazione. Le decisioni delle varie *A.I.* derivano dalla qualità ed integrità dei dati impiegati nel processo elaborativo, sia negli aspetti processuali che nei precedenti giurisprudenziali, pertanto, elemento essenziale, nell'implementazione di tali sistemi, dovrebbe essere la costante ed agevole controllabilità dei parametri di riferimento.
Ciò che realmente emerge dalle considerazioni anzidette è che non esiste una linea univoca sull'impiego di nuove tecnologie di giustizia predittiva, ma è indispensabile un approccio evolutivo e progressivo a quella che può essere considerata una vera e propria rivoluzione copernicana nella gestione del comparto giustizia, soprattutto in ambito penale.
La chiave di volta, probabilmente, risiede in un atteggiamento pacato ed esplorativo di un fenomeno che, per quanto avversato dalla dottrina e da parti consistenti degli addetti ai lavori, offre alcune opportunità meritevoli di considerazione, anche alla luce dei potenziali rischi che una simile tecnologia potrebbe comportare nel caso in cui sia lasciata a sé stessa o, peggio ancora, a mani poco esperte.
E' fondamentale comprenderne i meccanismi e, come per ogni altra precedente evoluzione della tecnica, non è facile eliminare completamente gli effetti di un processo in divenire, semmai, si può tentare di mitigarne le criticità. L' arrivo sul mercato delle tecnologie di *A.I.* pone una serie di domande alle quali è difficile rispondere.
In pochissimi anni, come per altre tecnologie, sono stati compiuti passi da gigante con sviluppi inimmaginabili anche solo pochi anni fa.
Le opportunità create dai sistemi in questione pongono quesiti di natura legale ed etica altrettanto nuovi a cui gli addetti ai lavori sono soggetti nelle rispettive attività di implementazione.

Il legislatore, dal canto suo, è inesorabilmente vincolato alla gestione di un processo esponenziale ed in costante fermento, difficilmente imbrigliabile nei sofismi da equilibrista della tecnica normativa.
I grandi dibattiti giurisprudenziali partono da questioni etiche di notevole impatto ed i quesiti, scaturiti dalla possibile implementazione delle tecnologie di *A.I.* nel sistema penale, godono di un'attenzione privilegiata in funzione dell'impatto diretto sulla vita di ciascun individuo delle scelte compiute nel complesso meccanismo di accertamento dei reati e conseguente giudizio di colpevolezza.
D'altro canto, in altre occasioni, dalla valutazione di opportunità nel preferire l'uso di strumenti in grado di ledere la libertà morale dell'individuo, è stata preferita l'esclusione a priori ed in modo oggettivo, anche contro la volontà del soggetto interessato, delle macchine della verità o di mezzi di accertamento dell'attendibilità delle testimonianze12.
L' art. 188 c.p.p., infatti, afferma che "Non possono essere utilizzati, neppure con il consenso della persona interessata, metodi o tecniche idonei a influire sulla libertà di autodeterminazione o ad alterare la capacità di ricordare e di valutare i fatti". La volontà del legislatore nazionale di escludere la possibilità di impiego di simili strumenti deriva dalla scelta consapevole, nel rispetto delle libertà fondamentali, di subordinare la ricerca della verità storica, derivante dalla esatta ricostruzione dei fatti, alla ricerca della verità giudiziale, unico obiettivo legittimo del processo penale.
Uno Stato democratico, se vuol considerarsi tale, non dovrebbe porre in subordine il rispetto dei diritti dell'individuo alla ricerca della verità ad ogni costo13.
Si potrebbe obiettare che un conto è l'assoggettamento del soggetto parte del procedimento penale a strumenti tecnici di pressione, altro, invece, è il supporto della moderna tecnologia all'attività cognitiva del giudice nella valutazione

[12] C. App. Brescia, sentenza 15 luglio 2020 (dep. 11 novembre 2020), n. 1683, Pres. Deantoni, rel. Milesi. Si veda anche GENNARI, Nuove e vecchie scienze forensi alla prova delle corti, Maggioli, Santarcangelo di Romagna, 2016, 117-123.
[13] l'unico caso in cui la-*IAT* è stato utilizzato in corte è quello in cui il test è stato presentato per la prima volta e cioè G.i.p. Cremona, 19 luglio 2011, n. 109, inedita.

di responsabilità dell'imputato o nel giudizio prognostico nella determinazione del grado di recidiva *post factum* del condannato14.
Ebbene, le esperienze maturate in altri ordinamenti hanno mostrato gli elementi critici derivanti dall'impiego di sofisticati sistemi di elaborazione dei dati, vuoi per difetto originario della tecnologia di calcolo, vuoi per le distorsioni eterointegrative del necessario intervento umano, prima o dopo il settaggio del sistema di valutazione.
Errori cognitivi, *bias*, algoritmi difettosi, dati parziali, pregiudizio statistico ecc. sono solo alcuni dei possibili difetti di ingegnerizzazione di tecnologie che, per quanto straordinariamente stupefacenti nelle manifestazioni apparenti, presentato, allo stato attuale, diversi *vulnus*, derivanti da un grado di maturazione in itinere15.
Inutile far riferimento ad ambiti poco agevoli e carichi di opacità tipici dei regimi totalitari. In tali contesti, come quello cinese, seppur non mancano esempi di sperimentazione concreta di *A.I.* in ambito penale, almeno per il momento, è assai difficile, se non impossibile, recuperare informazioni meritevoli di considerazione alla luce della scarsa genuinità o completezza intrinseca dei dati[16].
Più agevole, anche per le ripercussioni già avute nei circoli di studio della

[14] Il noto caso Loomies ne è un esempio. Si veda a riguardo la sentenza della *Supreme Court of Wisconsin, State of Wisconsin v. Loomis, Case no. 2015AP157-CR, 5 April – 13 July 2016.*

[15] TVERSKY e KAHNEMAN, Judgment under Uncertainty: Heuristics and Biases 1974, cit. in WILKE e MATA, Encyclopedia of Human Behavior Kahneman, Pensieri lenti e veloci, p. 238 in http://www.pensierocritico.eu/bias-blind-spot.html.

[16] L'esempio tipico è quello del procuratore *robot* nell'ambito del processo penale per la valutazione delle prove, dei presupposti per custodia cautelare e arresto e della pericolosità dell'indagato/imputato. Il sistema, sviluppato da una *equipe* di ricercatori sotto la guida del Prof. Shi Young utilizza per la valutazione un database di 17000 casi avvenuti tra il 2015 ed il 2020, ma al momento è in grado di analizzare solo otto fattispecie di reato previste dal Codice penale cinese (nella fattispecie frodi con carte di credito, gioco d'azzardo, guida pericolosa, lesioni internazionali, intralcio ai doveri d'ufficio, furto, frode e "*scelta di litigi e provocazione di guai*"). Secondo quanto dichiarato dal Prof. Young, dai primi test emergerebbe un margine di errore del 3% nella valutazione del grado colpevolezza od innocenza dell'imputato, ma senza che il robot possa prendere parte alla parte attiva della decisione. Lo stesso interverrebbe come mero ausilio al, libero convincimento del giudice. Infatti, sempre secondo il Prof. Young, affinché la macchina possa prendere autonomamente decisioni "avrebbe bisogno di "convertire un linguaggio umano complesso e in continua evoluzione in un formato matematico o geometrico standard che un computer potrebbe capire". Per ulteriori approfondimenti si veda l'articolo pubblicato sul S*outh China Morning Post* il 26 dicembre 2021 al seguente link: https://www.*scmp.com/news/china/science/article*/3160997/*chinese-scientists-develop-ai-prosecutor-can-press-its-own*

materia o, a maggior ragione, nella costruzione di proposte normative in ambito europeo, è il caso di impiego del cosiddetto sistema *COMPAS*.
Si tratta di uno dei tanti sistemi di valutazione del rischio a disposizione dell'apparato giudiziario statunitense, impiegato per ricevere informazioni utili a valutare la possibilità di reati futuri e le tipologie di misure da applicare nella prevenzione17.

4.*Prospettive per il sistema di garanzie europeo*. Come ogni altro fenomeno influenzato dall'evoluzione tecnologica e dal suo processo evolutivo, è fondamentale porre un notevole grado di attenzione sia sui potenziali rischi che sulle innegabili opportunità. Quando si discute di giustizia predittiva, se da una parte è innegabile il raggiungimento di obiettivi pratici rappresentati da risparmio in termini di costo e tempo necessari a processare operazioni di ricostruzione dei fatti estremamente complesse, dall'altro è innegabile il potenziale rischio di una significativa vulnerabilità nel sistema di garanzie e tutele dell'individuo, nonché sull'esercizio della funzione giurisdizionale.
Con riferimento al tema oggetto di studio, il *GDPR* riserva già nell'art. 22 uno specifico dettato normativo relativo al divieto di essere sottoposti a decisioni interamente automatizzate: così al comma 1 si specifica che «l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici

[17] «Per "*polizia predittiva*" possiamo intendere l'insieme delle attività rivolte allo studio e all'applicazione di metodi statistici con l'obiettivo di "predire" chi potrà commettere un reato, o dove e quando potrà essere commesso un reato, al fine di prevenire la commissione dei reati stessi. La predizione si basa fondamentalmente su una rielaborazione attuariale di diversi tipi di dati, tra cui quelli relativi a notizie di reati precedentemente commessi, agli spostamenti e alle attività di soggetti sospettati, ai luoghi, teatro di ricorrenti azioni criminali, e alle caratteristiche di questi luoghi, al periodo dell'anno o alle condizioni atmosferiche maggiormente connesse alla commissione di determinati reati; tra i dati utilizzati a questi fini talora compaiono anche informazioni relative all'origine etnica, al livello di scolarizzazione, alle condizioni economiche, alle caratteristiche somatiche (...una rivincita di Lombroso?), riconducibili a soggetti appartenenti a determinate categorie criminologiche (ad es., potenziali terroristi), etc». Così BASILE, Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine, in *diritto penale e uomo*, rivista, 29 settembre 2019. Per un completo inquadramento della materia della predictive policing, v. PERRY, MCINNIS, PRICE, SMITH, Hollywood, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, *Rand Corporation*, 2013.

che lo riguardano o che incida in modo analogo significativamente sulla sua persona»[18].
Ciò significa che, qualora dovesse intervenire un algoritmo nella decisione, ma la stessa sia sottoposta al controllo umano, lo scudo previsto dall'articolo in questione non sarebbe applicabile, perdendo di valore tutelante. Come già detto, l'imputato avrebbe sempre diritto a ricevere informazione sull'esistenza

[18] Così, ai considerando collegati 71 e 72 «l'interessato dovrebbe avere il diritto di non essere sottoposto a una decisione, che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani. Tale trattamento comprende la «profilazione», che consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato, ove ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona. Tuttavia, è opportuno che sia consentito adottare decisioni sulla base di tale trattamento, compresa la profilazione, se ciò è espressamente previsto dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento, anche a fini di monitoraggio e prevenzione delle frodi e dell'evasione fiscale secondo i regolamenti, le norme e le raccomandazioni delle istituzioni dell'Unione o degli organismi nazionali di vigilanza e a garanzia della sicurezza e dell'affidabilità di un servizio fornito dal titolare del trattamento, o se è necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, o se l'interessato ha espresso il proprio consenso esplicito. In ogni caso, tale trattamento dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione. Tale misura non dovrebbe riguardare un minore. Al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello *status* genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti. Il processo decisionale automatizzato e la profilazione basati su categorie particolari di dati personali dovrebbero essere consentiti solo a determinate condizioni. La profilazione è soggetta alle norme del presente regolamento che disciplinano il trattamento dei dati personali, quali le basi giuridiche del trattamento o i principi di protezione dei dati. Il comitato europeo per la protezione dei dati istituito dal presente regolamento («comitato») dovrebbe poter emanare orientamenti in tale contesto».

di un processo decisionale automatizzato e sui meccanismi alla base di tale funzionamento, incluse le potenziali conseguenze giuridiche del suo impiego.
Sulla base del costrutto normativo già previsto dagli articoli del *GDPR*, l'interessato avrebbe diritto a ricevere tutta una serie di informazioni relative all'esistenza di un processo decisionale automatizzato[19], sulla logica alla base del suo funzionamento e, soprattutto, sulle conseguenze derivanti dal suo impiego.
I principi relativi alle coperture del segreto industriale, indicano, però, che lo stesso non può avere accesso totale alle formule matematiche impiegate dall'algoritmo, ma deve comunque avere accesso a tutta una serie di informazione che consentano una comprensione semplice ed intelligibile del suo funzionamento[20].
Allo stesso tempo, però, il *GDPR*, prevede una serie di deroghe specifiche, coperte da riserva di legge, in cui può essere limitata la portata degli obblighi derivanti dal regolamento, a condizione di rispettare i parametri essenziali delle *libertà fondamentali* e sia una misura *necessaria e proporzionata* in una *società democratica.*
Il fenomeno, in continua evoluzione, non ha lasciato indifferente l'unione europea, la quale, in un quadro normativo non agevole, attraverso la commissione, ha iniziato un percorso di regolamentazione con una proposta di armonizzazione delle regole in ambito europeo.
L'iniziativa europea è essenzialmente orientata ad un contenimento degli gli aspetti critici legati all'uso della tecnologia di *A.I.*, soprattutto con riguardo alla tutela delle libertà fondamentali, senza, però, trascurarne i potenziali elementi

[19] I primi accenna della giurisprudenza italiana in tal senso provengono dal settore del diritto amministrativo. Una recente sentenza del Consiglio di Stato, la n. 2270 dell'8 aprile 2019, sez. VI, ha legittimato l'impiego di algoritmi nelle procedure valutative dalla pubblica amministrazione, a condizione, però, che vi sia trasparenza e possibilità di controllo giurisdizionale. I giudici hanno precisato che l'impiego di algoritmi e procedure automatizzate è considerato un a*tto amministrativo informatico* e, come tale, deve necessariamente sottostare ai principi generali di ragionevolezza, pubblicità, proporzionalità e trasparenza.
[20] Il Parlamento europeo, nel *report* del 2019 *AI and Robotics,* ha specificato la necessità di avere la cosiddetta *intellligibility of decisions,* nonché il diritto della persona interessata dal trattamento dei dati di essere informato sulla logica del meccanismo di elaborazione e sulla presenza di un controllo umano esterno.

di carattere positivo[21]. In generale gli Stati membri prevedono un incremento delle risorse da investire in tale settore.
Il raggiungimento di una elevata qualità del sistema è ritenuto un fattore determinante nella costruzione del sistema di gestione.
Affinché si possa avere fiducia nei sistemi di intelligenza artificiale, la commissione europea ha proposto tre iniziative legislative convergenti in tal senso. Si parla di a) *European legal framework for A.I. to address fundamental rights and safety risks specific to the A.I. systems; b) EU rules to address liability issues related to new technologies, including A.I. systems; c) a revision of sectoral safety legislation (e.g. Machinery Regulation, General Product Safety Directive).*
Secondo la commissione, una mitigazione dei rischi connessi all'uso dell'*A.I.* può avvenire mediante una legislazione complementare con norme proporzionate e flessibili. In tale modo, l'unione europea dovrebbe divenire un riferimento *gold standard* globale nel settore dell'intelligenza artificiale.
Sempre secondo la commissione, con un simile quadro di rifermento, sviluppatori ed utenti della tecnologia avrebbero un quadro giuridico preciso basato su quattro diversi livelli di rischio: rischio inaccettabile, rischio elevato, rischio limitato e rischio minimo. Nella relazione alla proposta di regolamento si può leggere una prima definizione di intelligenza artificiale, intendendo con la stessa

[21] *Nell' annual report lays out the challenges of protecting fundamental rights in the digital age del 10 Dicembre 2021 è specificato che «the increasing use of artificial intelligence systems can yield great benefits, but certain applications are complex and opaque, which can be a challenge for compliance with or enforcement of fundamental rights. Many Member States have developed national strategies on artificial intelligence to ensure transparency, traceability and robustness and find effective ways to comply with fundamental rights. In April 2021, the Commission proposed a legislative act to ensure that artificial intelligence systems that pose a high-risk to fundamental rights are appropriately tested and documented».* Per approfondimenti, si veda il *report* sul sito ufficiale della commissione europea. Come specificato al paragrafo della relazione 1.1 alla proposta, «l''uso dell'intelligenza artificiale, garantendo un miglioramento delle previsioni, l'ottimizzazione delle operazioni e dell'assegnazione delle risorse e la personalizzazione dell'erogazione di servizi, può contribuire al conseguimento di risultati vantaggiosi dal punto di vista sociale e ambientale nonché fornire vantaggi competitivi fondamentali alle imprese e all'economia europea. Tale azione è particolarmente necessaria in settori ad alto impatto, tra i quali figurano quelli dei cambiamenti climatici, dell'ambiente e della sanità, il settore pubblico, la finanza, la mobilità, gli affari interni e l'agricoltura. Tuttavia, gli stessi elementi e le stesse tecniche che alimentano i benefici socio-economici dell'*A.I.* possono altresì comportare nuovi rischi o conseguenze negative per le persone fisiche o la società».

«una famiglia di tecnologie in rapida evoluzione in grado di apportare una vasta gamma di benefici economici e sociali in tutto lo spettro delle attività industriali e sociali».
Tenendo in considerazione la velocità del progresso tecnologico, con la proposta di regolamento l'*UE* si è impegnata a perseguire un approccio equilibrato cercando di preservare «la leadership tecnologica dell'*UE* e assicurare che i cittadini europei possano beneficiare di nuove tecnologie sviluppate e operanti in conformità ai valori, ai diritti fondamentali e ai principi dell'Unione»[22].
La costruzione di un modello di gestione *umanocentrica* della tecnologia di intelligenza artificiale, inoltre, la si evince dalla specificazione secondo cui «Le regole per l'*A.I.* disponibili sul mercato dell'Unione o che comunque interessano le persone nell'Unione dovrebbero pertanto essere incentrate sulle persone, affinché queste ultime possano confidare nel fatto che la tecnologia sia usata in modo sicuro e conforme alla legge, anche in termini di rispetto dei diritti fondamentali».
In alcune recenti conclusioni del consiglio europeo riguardo all'uso dell'intelligenza artificiale si è indicato, come requisito per il rispetto dei diritti fondamentali e l'agevolazione nell'applicazione delle norme di riferimento, di tenere sempre in considerazione l'opacità, la complessità, la faziosità ed un certo grado di imprevedibilità nel comportamento di taluni sistemi di *A.I.*[23].
Il principio di proporzionalità, inteso come pilastro dell'architettura normativa, dovrebbe essere garantito da un approccio duro al rischio alto, con imposizione di oneri solo in caso di potenziale *vulnus* per la sicurezza e la tutela delle libertà fondamentali.
Come indicato nella relazione alla proposta «i requisiti di qualità elevata dei dati, documentazione e tracciabilità, trasparenza, sorveglianza umana,

[22] Come si legge la paragrafo 1.1 della relazione alla proposta con la stessa «si tiene fede all'impegno politico della presidente Von Der Leyen che, nei suoi orientamenti politici per la Commissione 2019-2024 "Un'Unione più ambiziosa, ha annunciato che la Commissione avrebbe presentato una normativa per un approccio europeo coordinato alle implicazioni umane ed etiche dell'intelligenza artificiale. A seguito di tale annuncio la Commissione ha pubblicato il 19 febbraio 2020 il Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia. Il Libro bianco definisce le opzioni strategiche su come conseguire il duplice obiettivo di promuovere l'adozione dell'*A.I.* e affrontare i rischi associati a determinati utilizzi di tale tecnologia».
[23] Consiglio dell'Unione Europea, *Conclusioni della presidenza – La Carta dei diritti fondamentali nel contesto dell'intelligenza artificiale e della trasformazione digitale*, 11481/20, 2020.

precisione e robustezza sono strettamente necessari per attenuare i rischi per i diritti fondamentali e la sicurezza posti dall'*A.I.* e che non sono oggetto di altri quadri giuridici in vigore».
Uno degli aspetti più interessanti del nuovo impianto normativo sarà l'obbligo per i futuri fornitori dei sistemi di *A.I.* di informazione in caso di «*incidenti gravi o malfunzionamenti che costituiscono una violazione degli obblighi in materia di diritti fondamentali* non appena ne vengono a conoscenza, nonché in merito a qualsiasi richiamo o ritiro di sistemi di *A.I.* dal mercato. Le autorità nazionali competenti indagheranno quindi sugli incidenti o sui malfunzionamenti, raccoglieranno tutte le informazioni necessarie e le trasmetteranno periodicamente alla Commissione con metadati adeguati».

5. *Quale futuro per l'A.I. nel sistema penale?.* Pur non essendo ancora esistente una definizione chiara ed univoca di cosa sia l'intelligenza artificiale, è pur vero che, fin dalla nascita del termine negli anni Sessanta, ad opera del matematico McCarthy, i processi computazionali riconducibili al fenomeno di apprendimento automatizzato hanno subito l'attenzione della comunità di studiosi intenzionati a carpirne potenzialità e pericoli. Roger Schank, uno dei fondatori del metodo computazionale, tentò già negli anni Ottanta di identificarne i caratteri essenziali nella copresenza di cinque elementi distinti: capacità comunicativa; conoscenza di sé; conoscenza del mondo esterno; comportamento teso ad un fine; alto grado di creatività.
La conseguenza logica di tale approccio risiede nell'impossibilità di immaginare tali sistemi solo come surrogati umanoidi nelle manifestazioni estetiche, soprattutto nelle fasi iniziali. Inoltre, aspetto più rilevante, poco o nulla dell'intelligenza artificiale è direttamente riconducibile alle ancora inesplorate complessità dei meccanismi della mente umana, soprattutto per ciò che attiene agli ambiti emotivi e della *psiche* relazionale[24].
L' impiego di tali sistemi nei processi di *Law enforcement è* già realtà. Come si evince dal documento di presentazione al convegno annuale degli esperti di

[24] Gli esperti di *A.I.* preferiscono parlare di razionalità, laddove per "*razionalità*" si intende la «capacità di scegliere la migliore azione da intraprendere per conseguire un determinato obiettivo alla luce di alcuni criteri di ottimizzazione delle risorse a disposizione». Così, RUSSELL, NORVIG, in *Artificial intelligence: A Modern Approach, Prentice Hall,* 3ª edizione, 2009, pp. 36 ss.

polizia, organizzato dall'*OSCE*: «nei loro sforzi per aumentare l'efficienza e l'efficacia e per stare al passo con le innovazioni tecnologiche, le autorità e le agenzie di *law enforcement* di tutto il mondo stanno esplorando sempre più i potenziali dell'*A.I.* per il loro lavoro. La crescente quantità di dati ottenuti e archiviati dalla polizia ha anche richiesto metodi e strumenti più sofisticati per la loro gestione e analisi, per l'identificazione di modelli (*pattern*), la previsione dei rischi e lo sviluppo di strategie per allocare le risorse umane e finanziarie dove sono maggiormente necessarie. Anche se l'uso dell'*A.I.* nel lavoro delle forze dell'ordine è un argomento relativamente nuovo, alcuni strumenti basati sull'intelligenza artificiale sono già stati testati e sono persino attivamente utilizzati dai servizi di polizia di diversi Paesi del mondo. Questi includono *software* di analisi di video e immagini, sistemi di riconoscimento facciale, di identificazione biometrica, *droni* autonomi e altri *robot* e strumenti di analisi predittiva per prevedere le "*zone calde*" del crimine o anche per identificare potenziali criminali futuri, in particolare i criminali ad elevata pericolosità»[25].

Dal momento che il controllo umano assurge a fattore determinante nella gestione delle tecnologie di intelligenza artificiale, è opportuno chiedersi se esso debba limitarsi alla scelta di obiettivi e monitoraggio, oppure debba spingersi sino al punto da compromettere le prestazioni del sistema. Un quesito di non facile risposta, cui, presumibilmente sarà attribuita una rimodulazione progressiva e dinamica in funzione del *target* di riferimento.

Da ciò ne consegue che del tutto diverso sarà l'impiego dei sistemi di *A.I.*, quali supporto nelle attività di contrasto a fenomeni criminali di particolare rilievo, nei settori della lotta al terrorismo internazionale e criminalità organizzata, rispetto ad usi finalizzati al contrasto di criminalità semplice o cosiddetta bagattellare.

Paradossalmente, è proprio in tali tipologie di attività che il coefficiente di tolleranza all'implementazione di tali sistemi sarà inversamente proporzionale al concreto pericolo di abuso nel loro impiego alla luce dei più sensibili aspetti

[25] *OSCE Annual Police Experts Meeting*: *Artificial Intelligence and Law Enforcement: An Ally or an Adversary?,* 23-24 September 2019, Vienn.

legati alle principali libertà fondamentali[26]. Tali tipologie di sistemi algoritmici dovranno essere soggette ad un monitoraggio costante, da un punto di vista non solo tecnico, ma, anche, giuridico, in modo da poter implementare un preciso assetto normativo che ne disciplini il legittimo impiego, nel pieno rispetto dei diritti umani.

La possibilità concreta che in futuro possano verificarsi situazioni di impiego dei sistemi di intelligenza artificiale nelle decisione giudiziarie in ambito penale ha allarmato il consiglio europeo al punto da spingerlo ad adottare *la Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia penale e nei relativi ambienti*[27], un documento elaborato dalla Commissione per l'efficacia della giustizia (*CEPEJ*), il 4 dicembre 2018 nella consapevolezza di un incremento dell'impiego dell'intelligenza artificiale nelle "*moderne società*".

Nella carta vengono specificate delle linee guida a cui dovranno «attenersi i soggetti pubblici e privati responsabili del progetto e sviluppo degli strumenti e dei servizi della *A.I.*».

Si tratta per l'appunto di principi riguardanti il *rispetto dei diritti fondamentali,* la *non discriminazione,* la garanzia di *qualità* e *sicurezza* dei sistemi, il rispetto dei principi di *trasparenza*, *imparzialità* e *correttezza* nel loro impiego e, in particolar modo la garanzia del costante *controllo umano*[28].

Come evidenziato anche dal documento esplicativo allegato alla carta, al 2018, anno in cui venne elaborato, «l'uso di algoritmi di intelligenza artificiale nei sistemi giudiziari europei rimane principalmente un'iniziativa commerciale del

---

[26] Si pensi, a titolo di esempio, al tema legato alla *privacy*, o più propriamente, alla tutela del trattamento dei dati personali, in considerazione della gran mole di dati che questi sistemi di *A.I.* (a volte equipaggiati per l'appunto di sensori e telecamere avanzate) possono acquisire in relazione alla vita, anche privata, dei cittadini coinvolti dal loro utilizzo nei più svariati ambiti. Situazioni in cui i dati oggetto del processo di elaborazione dell'algoritmo potrebbero essere in varie forme manipolati, sottratti o deformati, anche con notevole pregiudizio per le persone cui essi fanno rifermento. Al riguardo, si veda sul tema BASILE, Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine, in *Diritto penale e uomo*, rivista online, 29 settembre 2019.

[27] Si veda QUATTROCOLO, I*ntelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*, in www.lalegislazionepenale.eu, 18 dicembre 2018.

[28] Il cui fine è rivolto a «precludere un approccio deterministico» e ad «assicurare che gli utilizzatori agiscano come soggetti informati ed esercitino il controllo delle scelte effettuate». Virgolettati estratti dalla carta.

settore privato, rivolta a compagnie assicurative, uffici e studi legali, avvocati e privati».
Per quanto riguarda, invece, i procedimenti penali, nel documento è evidenziato che «anche se non sono specificamente progettati per essere discriminatori, l'uso di algoritmi basati sull'*A.I.* [...] ha mostrato il rischio di favorire la rinascita di teorie deterministiche a scapito delle teorie dell'individualizzazione della pena»[29].
Il rischio concreto di incorrere in fenomeni discriminatori o pericolosi automatismi durante l'impiego di sistemi algoritmici in ambito penale deriverebbe essenzialmente dal carattere accusatorio del processo nel contesto europeo, in cui il giudizio è basato principalmente su valutazione di prove dichiarative su cui un qualsiasi impianto tecnologico di valutazione avrebbe serie difficoltà a considerarne gli aspetti critici dovuti a menzogne, reticente od atteggiamenti emotivi.
Alla luce di quanto stabilito dall'art. 192, comma 2 c.p.p. sui requisiti di chiarezza, precisione e concordanza degli elementi di prova, sarebbe molto difficile per un sistema di intelligenza artificiale, ancorché in un processo di tipo indiziario, poter valute il grado di coerenza logica delle prove sulla base dei criteri richiesti. Del tutto impossibile per un sistema di intelligenza artificiale è l'applicazione della regola di giudizio stabilità dall'art. 533, comma del c.p.p. sull'*oltre ogni ragionevole dubbio,* in quanto, al momento, i *software* in questione hanno capacità di elaborazione solo con logiche binarie (bianco-nero; vero-falso; sì-no) o probabilistiche in %[30].
Chi sostiene la possibilità di un futuro utilizzo degli algoritmi di intelligenza artificiale nelle aule di giustizia muove dall'assunto che simili sistemi grazie all'elaborazione di dati ed autoapprendimento possano agevolare valutazioni di pericolosità più accurate ed esenti dai rischi umani di pregiudizio. Come ha potuto dimostrare anche l'esempio statunitense del sistema COMPAS,

[29] Rispettivamente pag. 16, 41 e 48 del documento.
[30] CANZIO, *Il dubbio e la legge*, in *Diritto penale contemporaneo*, 2018, pp. 1 ss.; GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Unite ed Europa*, in ivi, 2019, pp. 1 ss.; NATALE, Introduzione. *Una giustizia (im)prevedibile?*, in *Questione Giustizia*, fasc. 4, 2018, pp. 1 ss.; nello stesso fascicolo, v. pure i contributi di COSTANZI, *La matematica del processo: oltre le colonne d'Ercole della giustizia penale*, e di CASTELLI, PIANA, *Giustizia predittiva. La qualità della giustizia in due tempi.*

innumerevoli sono anche le perplessità relative a tali sistemi, con riguardo sia ad aspetti di accuratezza che di trasparenza degli algoritmi su cui si basano le decisioni.
Nel contesto europeo, almeno per il momento, non si intravede la possibilità di un ingresso degli algoritmi predittivi nelle aule penali, anche alla luce l'art. 15 della direttiva 95/46/CE, confluito nell'art. 22 del nuovo Regolamento europeo in materia di protezione dei dati personali, entrato in vigore il 25 maggio 201831.
A supporto del ragionamento, la Risoluzione del Parlamento europeo sulla robotica del 2017 fa leva esattamente sul principio della *trasparenza*, evidenziando la necessità che sia sempre possibile individuare la logica alla base di ogni decisione, cui sia coinvolto l'uso od aiuto dell'intelligenza artificiale, soprattutto, qualora tale decisione possa determinare un impatto significativo sulla vita di una o più persone coinvolte nel giudizio.
Di fatto, non si può ancora parlare di una vera e propria intelligenza, paragonabile a quella umana, piena di sfaccettature ed interazioni emotive difficilmente riproducibili da circuiti elettronici.
Prima di intraprendere il cammino frastagliato e tortuoso verso un affidamento del giudizio di valutazione ad una macchina, sia esso nella fase delle indagini preliminari, oppure nel momento cognitivo di valutazione della responsabilità, è bene tenere a mente i margini oggettivi entro cui fissare i poteri di intervento, onde evitare indebiti sconfinamenti verso lande desolate prive di umanità.

6. *Il Trojan Horse quale strumento itinerante d'indagine*. Nel quotidiano dibattito politico sulla giustizia penale, caratterizzato da un meccanismo di riflesso condizionato azione-reazione, il più delle volte profondamente distaccato dal merito delle questioni oggetto di discussione, il tema delle intercettazioni, preventive di polizia o giudiziarie, qualunque sia il mezzo mediante cui vengono effettuate ed a prescindere dal tipo di reato interessato, è ormai divenuto un totem di ineludibile fascinazione mediatica, anche e, soprattutto, in virtù dell'enorme impatto assunto nell'immaginario collettivo, quale strumento di

[31] L'articolo, infatti, stabilisce il divieto di giudizi automatizzati basati esclusivamente sulla personalità del soggetto.

oppressione o abuso della macchina giudiziaria nei confronti di cittadini inermi ed impotenti dinanzi allo strapotere delle toghe[32].
Così, le intercettazioni tutte, a prescindere dal fine e dal tipo di strumento impiegato nelle modalità specifiche operative, nel corso del tempo, sono velocemente assurte al ruolo di nemico giurato delle libertà fondamentali dell'individuo e, non più, così come concepito fin dalla sua introduzione, utile strumento di ricerca della prova nel contrasto all'attività criminale[33].
E' innegabile il ruolo induttivo verso generali e generaliste percezioni dell'opinione pubblica, accentuato anche dalle più eloquenti manifestazioni di abuso od uso improprio di uno strumento così pervasivo e potenzialmente lesivo dei principi cardine di una società democratica.
Intere vite alla mercé del dibattito qualunquista massmediatico, interferenze più o meno pertinenti nella normale attività democratica del corpo elettivo, aspetti più intimi dell'agire umano oggetto di scherno e risentimento morale, sono solo alcune delle criticità emerse nell'uso improprio di tale strumento fin dalla sua introduzione nel codice di procedura.
Magistratura inquirente impunemente poco attenta al rispetto del segreto istruttorio, avvocatura mal posta nel suo ruolo di riequilibrio delle garanzie difensive o, peggio ancora, indotta ad approfittare delle prerogative di categoria nella gestione del materiale probatorio in suo possesso col fine poco dignitoso, dalla dubbia legittimità procedurale, di screditare la controparte, hanno

[32] Si veda NORDIO, Intervento al Senato, 6-7 dicembre 2022, laddove il Ministro ribadisce la necessità di procedere ad una «profonda revisione del sistema delle intercettazioni [giudiziarie]» ritenendo l'attuale disciplina «[...] un pericolo per la riservatezza e l'onore delle persone coinvolte [...] determina[ndo] sostanziali violazioni, quasi blasfeme, del dettato di cui all'art. 15 Cost.»

[33] Il Ministro Nordio ha richiamato i dati statistici, i quali dimostrerebbero che, nel solo 2021, le persone soggette a captazioni di vario genere sono stare pari a 70 mila, per un totale di 150.000 intercettazioni autorizzate sempre nello stesso anno di riferimento per un ammontare complessivo di spesa pari a 12.785.338,67 euro. La necessità prospettata dal ministro di ridurre anche gli ingenti costi delle attività di intercettazione ha comportato l'adozione di manovra di bilancio di una riduzione delle spese per le intercettazioni di 1.575.136 euro annui, a decorrere dal 2023 (art. 880, l. 197/2022). I dati sono rinvenibili anche su www.giustizia.it. Come parametro di riferimento isolato, inoltre, secondo il bilancio sociale 2020-2021, elaborato dall'Università degli Studi di Napoli "Federico II" di concerto con la procura della Repubblica presso il Tribunale di Napoli, nell'anno 2020 sono state 2.891 le richieste di autorizzazione a disporre, che sono arrivate a 4.672 nel 2021.

progressivamente inficiato il meritevole intento investigativo nelle scelte di politica criminale del legislatore34.
Alcuni strumenti, però, nati con l'evoluzione del processo digitale, hanno generato ulteriori perplessità e riserve da parte di addetti ai lavori e non solo, tanto da stimolare diverse volte rettifiche normative dal notevole impatto.
L'introduzione del captatore informatico (*Trojan*), fin dagli albori, ha generato significate criticità d'impiego, in virtù del notevole potere intrusivo nella vita delle persone sottoposte al suo screening35.
Di fatto, si tratta di una tecnologia subdola in grado di penetrare le più elementari attività quotidiane, svolte dalla maggior parte dei cittadini durante l'uso dei più diffusi strumenti digitali quali smartphone, pc, *smart tv* ecc. Inutile sottolineare quanto simili apparecchi tecnologici siano ormai divenuti riferimento imprescindibile nelle più elementari attività quotidiane, anche le più intime e riservate afferenti alla sfera privata della vita lavorativa, amorosa, sessuale, religiosa con tutto ciò che ne concerne in termini di vulnerabilità alla captazione esterna itinerante.
Nonostante le limitazioni operative e procedurali imposte dal legislatore, in linea di principio, non esiste limite tecnologico alla potenzialità intrusive anzidette e, come è facilmente intuibile, il praticabile è nemico giurato del non possibile, almeno in termini oggettivi.

---

[34] Sul punto si veda anche ANDOLINA, Le intercettazioni e i controlli preventivi sulle comunicazioni nel contrasto al terrorismo internazionale tra irrisolte criticità ed esigenze di riforma, in Arch. nuova proc. pen., 2016, f. 6, p. 575.

[35] Il primo uso del captatore nelle indagini è avvenuto in assenza di una norma di riferimento. La giurisprudenza, soprattutto quella di legittimità, è dovuta intervenire per definire i contorni di impiego dello strumento. Nella sentenza n. 27100 del 26.5.2015 (Musumeci), inerente un caso di impiego del *tojan horse* come strumento di ricerca della prova per reati di criminalità organizzata, avvenne la prima bocciatura dell'uso del captatore come strumento itinerante, infatti, la sesta sezione penale della Corte, ritenne opportuno chiarire che «l'intercettazione di conversazioni tramite il c.d. "agente intrusore", che consente la captazione "da remoto" delle conversazioni tra presenti mediante l'attivazione, attraverso il c.d. "*virus* informatico", del microfono di un apparecchio telefonico smartphone, dà luogo ad un'intercettazione ambientale che può ritenersi legittima, ai sensi dell'art. 266, comma secondo, cod. proc. pen. in relazione all'art. 15 Cost., solo quando il decreto autorizzativo individui con precisione i luoghi in cui espletare l'attività captativa». Al riguardo si veda anche ROSSI, *Trojan Horse: tornare alla riforma Orlando? Il difficile equilibrio nell'impiego del captatore informatico* SU, *questionegiustizia*, rivista *online*, 23/12/2022.

7. *Elementi critici dello strumento captativo (la pervasività).* Le esperienze pratiche fin qui maturate hanno sollevato non pochi dubbi sull'opportunità di rendere fruibile per la macchina investigativa l'uso del *trojan*, soprattutto nel contrasto ad attività criminale di tipo comune, caratterizzata da un basso gradiente di offensività, laddove si rende necessario un corretto equilibrio tra le esigenze di tutela della sicurezza collettiva a fronte del rispetto delle libertà fondamentali, proporzionalmente e tendenzialmente a favore delle seconde[36].
Il caso Palamara ha dimostrato quanto pervasivo possa essere lo strumento in questione e, malgrado tutte le garanzie operative, quanto tale tecnologia, anche in funzione delle complessità tecnico specialistiche indispensabili al suo impiego, sia potenzialmente idoneo a generare distorsioni nel diritto imprescindibile di difesa, difficilmente dimostrabili, sen non a fronte di costose attività peritali, cui, come è facile ipotizzare, non tutte le potenziali parti in causa di un eventuale processo penale possono accedere[37]. All'origine dell'articolata vicenda sull'uso del captatore informatico vi è, presumibilmente, la dialettica

[36] La proposta di modifica legislativa del Senatore Zanettin, del gruppo di Forza Italia, verte sulla sfera di applicazione del captatore informatico. Il disegno di legge del Senatore è intitolato «Modificazioni agli articoli 266 e 267 del codice di procedura penale e alla legge 9 gennaio 2019, n.3 in materia di utilizzo del captatore informatico nei procedimenti per i delitti contro la pubblica amministrazione» con cui si propone di sopprimere agli artt. 266 e 267 del codice di procedura penale, le voci che disciplinano rispettivamente "limiti di ammissibilità" e "presupposti e forme" del provvedimento che dispone le attività di intercettazione per i «delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni.....». Nella relazione al d.d.l. aggiunge che «Se da un lato l'utilizzo del trojan, introdotto nell'ordinamento penale italiano con la legge 23 giugno 2017, n. 23 - c.d. riforma Orlando - rappresenta lo strumento più penetrante ed efficace nel contrasto alla commissione di reati ritenuti di particolare gravità di tipo associativo e di terrorismo, dall'altro è lo strumento che più vìola la sfera di intimità dell'intercettato, con l'evidente rischio di una diversa destinazione d'uso atto a violare la privacy degli individui, nonostante la Corte di Cassazione (Cass. Pen., sez. V, 30 settembre 2020, n. 31064) abbia confermato che vada esclusa la riconducibilità del trojan agli strumenti di pressione sulla libertà fisica e morale il cui uso è vietato dall'articolo 188 del codice di procedura penale».
[37] Il ministro Nordio, sempre nella sua relazione in commissione al Senato ha affermato quanto segue: "Credete che tutte le intercettazioni del *trojan* di Palamara siano state trascritte nella forma della perizia? Sono state selezionate, pilotate e diffuse secondo gli interessi di chi le diffondeva, e non sono ancora tutte state rese pubbliche"

tecnologica tra coloro che delinquono da una parte e magistratura e polizia giudiziaria dall'altra38.
Il progresso esponenziale delle tecnologie informatiche e telematiche, di pari passo con la capacità captativa delle stesse, genera allo stesso tempo una indiscutibile opportunità elusiva delle reti criminali, le quali affidano lo svolgimento delle loro attività alla impenetrabilità degli apparecchi impiegati, alla inaccessibilità delle reti, nonché, non meno importante, all'adozione di sistemi di criptazione della messaggistica. Da ciò ne deriva che le eventuali valutazioni circa il potenziale intrusivo dei captatori non possono prescindere dal costante affinamento di canali di comunicazione altrettanto efficaci delle reti criminali.
L'uso dei captatori, tra le molteplici capacità intrusive, nella tradizionale funzione di intercettazioni di conversazioni mediate l'attivazione del microfono nella disponibilità dell'apparecchio infettato, potrebbe essere considerato un recupero dell'efficacia intrusiva, oramai perduta, delle tradizionali tecniche investigative.
I programmi di captazione informatica sono sviluppati per introdursi in modo subdolo negli apparecchi interessati dall'attività intercettiva, senza rivelare la loro presenza, acquisendo poteri di gestione e funzionamento proprio di una microspia telematica39. Operando e comunicando attraverso le reti internet i dati raccolti in modalità occulta al centro operativo di comando e controllo, essi possono raccogliere qualunque cosa venga digitata sulla tastiera, visualizzata sullo schermo o, altrimenti detto, in prossimità delle capacità uditive del

[38] Nel suo ultimo saggio nello Rossi afferma che: «Nell'ambito delle tecnologie informatiche e nel campo della telematica progrediscono infatti con straordinaria velocità e quasi di pari passo tanto le tecnologie di "captazione", che si fanno via più sofisticate ed invasive, quanto le tecniche di "elusione" di ogni captazione possibile, che si affidano di volta in volta alla impenetrabilità degli apparecchi utilizzati, alla inaccessibilità di particolari reti di comunicazione o alla adozione di sistemi di criptazione dei messaggi scambiati. Le valutazioni sul potenziale invasivo dei più moderni meccanismi di captazione devono perciò essere sempre compiute avendo presente che parallelamente e contemporaneamente si affinano e si moltiplicano anche i mezzi e i canali di comunicazione strutturati in modo da sottrarsi ai tradizionali strumenti di acquisizione. Mezzi e canali che spesso fondano la loro diffusione - oltre che sulla facilità dei contatti e sulla gratuità del servizio offerto, di regola compensato dagli introiti pubblicitari o dal valore delle informazioni sulla utenza raccolte attraverso di esse - proprio sulla loro vera o presunta inaccessibilità». Così ROSSI, *Trojan Horse: tornare alla riforma Orlando? Il difficile equilibrio nell'impiego del captatore informatico* SU, *questionegiustizia*, rivista *online*, 23/12/2022.
[39] Si veda TESTAGUZZA, *I sistemi di controllo remoto: fra normativa e prassi*, in *Dir. Pen. e Processo*, 2014, p. 759 e ss.

microfono. Allo stesso tempo, possono acquisire ogni tipo di file memorizzato fisicamente o per *cloud* sull'apparecchio infettato o negli altri legati allo stesso dalla rete *internet*.
In grado di *bypassare* molti dei più quotati applicativi *antivirus* o di sfruttare alcune vulnerabilità non note del sistema operativo i *trojan* possono divenire vere e proprie cimici o microspie per intercettazioni ambientali itineranti, essendo legate fisicamente alla disponibilità dell'apparecchio al soggetto *target*. Forme evolute del *software* riescono ad operare autonomamente sulla base degli indicativi di istruzione preimpostati al momento dell'inoculazione.
Le informazioni raccolta con l'attività di intercettazione vengono inoltrati ai *server* delle sale di controllo sfruttando la connettività del dispositivo infettato e, laddove non disponibile, memorizzati in remoto per un successivo inoltro al momento di riaggancio. Le eventuali difficoltà fisiche di inoculazione materiale del *virus* possono essere tranquillamente superate sfruttando la collaborazione dovuta dei gestori di servizi di rete, messaggistica o *social network* mediante invio di comunicazioni di posta elettronica ed aggiornamenti di software o applicazioni[40].
Le differenti modalità di ricerca *on line search* od *on line surveillance* consentono rispettivamente di fare copia delle unità di memoria del dispositivo trasmettendo i dati raccolti in tempo reale o ad intervalli agli investigatori oppure di captare il flusso informativo delle periferiche di video, *webcam*, microfono, schermo (*screenshot*) tastiera (*keylogger*) permettendo al centro di controllo un monitoraggio *real time* del *target*[41].

---

[40] Si veda TORRE, *Il virus di Stato nel diritto vivente tra esigenza investigative e tutela dei diritti fondamentali*, in *Dir. Pen. e Processo*, 2015, p. 1163 e ss.

[41] Nella sentenza Cass. Sez. I, Sent. 7 ottobre 2021 (dep. 1° febbraio 2022), n. 3591, Pres. Tardio, est. Liuni, ric. Romeo, I giudici di legittimità hanno dato credito ad un orientamento in base a cui equipara tutte le attività di *online surveillance* ad intercettazioni informatiche o telematiche, legittimandone perciò l'uso. Per quanto attiene alle operazioni di *screenshot*, nella sentenza in questione si afferma la rilevazione del *file Excel*, "*fotografato"* su *personal computer* tramite il malware inoculatovi, avendo riguardato «esclusivamente la captazione di flussi di dati in fieri, cristallizzati nel momento stesso della loro formazione», integra «un'attività di mera "*constatazione*" dei dati informatici in corso di realizzazione», i quali, «pur non costituendo una "comunicazione" in senso stretto», costituiscono «certamente [...] un comportamento c.d. "*comunicativo*"». In quanto tale, si sostiene la legittimità della captazione mediante inserimento di agente intrusore all'interno di un personal computer in applicazione della disciplina delle

La possibilità di apporre alcuni limiti tecnici preventivi all'attività di captazione non può far eludere le potenzialità ad origine *omni*comprensive dello strumento suscettibile di un potere invasivo esercitabile, in assenza delle dovute cautele e garanzie tecnico giuridiche, senza limiti ed in modo incontrollato.

8. *Un quadro normativo non uniforme*. Fin dalle origini, l'impiego del *trojan* nelle attività di indagine è avvenuto in mancanza di un adeguato quadro normativo di riferimento.
Nelle more del *vulnus* regolatorio, è emerso sempre di più il ruolo fondamentale della giurisprudenza di merito e di legittimità nel disciplinarne l'impiego42.
Quella che poteva essere considerata a tutti gli effetti una forma di intercettazione itinerante, ha subito una prima risposta di segno negativo dal giudice di legittimità nel caso Musumeci43, allorquando venne specificato come l'attività di intercettazione, mediante agente intrusore, potesse essere considerata legittima, nel rispetto dei principi dell'ordinamento, solo qualora fossero stati indicati con chiarezza i luoghi in cui espletare l'attività investigativa nel decreto di autorizzazione.
Dunque, una bocciatura del metodo investigativo ubiquitario ed itinerante, legittimo solo con specificazione dei luoghi.
L'elemento di discrimine, utile a comprendere l'evoluzione interpretativa in senso ampio, del possibile impiego nei casi di attività volte al contrasto dei fenomeni di criminalità organizzata o terrorismo, emerse qualche anno dopo nel

---

intercettazioni di comunicazioni informatiche o telematiche di cui all'art. 266 bis c.p.p., così richiamando i precedenti arresti giurisprudenziali in tema di legittima utilizzabilità del captatore informatico quale strumento esecutivo di tale tipo d'intercettazione (Cass. Sez. 5, 30.5.2017 n. 4837, Occhionero, Rv. 271412). Così FOVA, L*a Cassazione sulla riconducibilità all'art. 266 c.p.p. degli screenshot tramite captatore informatico,* su *Sistemapenale,* rivista *online*, 02/06/2022.

[42] la Corte di cassazione ha chiarito nella sentenza n. 35010 del 30 settembre 2020 ha chiarito che per le intercettazioni ambientali a mezzo di captatore informatico ("*trojan*"), ogni riferimento al luogo di esecuzione dell'attività di intercettazione non è un presupposto di autorizzabilità ai fini del rispetto dell'art. 8 CEDU secondo l'interpretazione della giurisprudenza della Corte EDU, ritenendo, in via alternativa, consentito far ricorso alla semplice indicazione del destinatario, in virtù della natura dinamica ed "itinerante" della captazione, prescindere dalla specificazione dei luoghi. Da ciò ne deriva che non vi è contrasto con la disciplina normativa dall'art. 8 della Convenzione ma rimane comunque opportuna una discussione politica inerente l'uso proporzionato del ricorso al *Trojan* fuori dai casi di criminalità organizzata.

[43] Sentenza n. 27100 del 26.5.2015

caso Scurato44. Ai tempi della controversia, la disciplina speciale prevista dall'art. 13 del D.l. N 152/1991 giocò un ruolo determinante nella decisione del giudice di legittimità, in quanto, in deroga a quanto previsto dall'art. 267 del c.p.p. venne considerato possibile sottoporre gli indagati ad "*intercettazione tra presenti*" anche nei luoghi di privata dimora fissati come limite dall'art. 664 c.p.p. per tutte le altre ipotesi diverse dai reati di criminalità organizzata o terrorismo.

Dal momento che nessuna preclusione era rinvenibile in ordine alle attività di intercettazione svolte nei luoghi pubblici od aperti al pubblico, nel caso delle attività di captazione presso il domicilio del destinatario, oltre alla possibilità ordinaria di acquisizione mediante motivato provvedimento autorizzativo, la disciplina derogatoria avrebbe giocato un ruolo decisivo nell'estensione del confine per ragioni investigative legate alla gravità del reato perseguito, senza necessità di ulteriori autorizzazioni45.

Il vero elemento di perplessità sorgeva, tuttalpiù, in ordine alla possibilità, molto plausibile, che il target portasse con se l'apparecchio inoculato presso altri domicili, ma, i giudici di legittimità, anche in tale aspetto, chiarirono come il legislatore aveva dato con la disciplina derogatoria prevista per i reati di criminalità organizzata, seppur in un contesto tecnologico differente, chiaro indirizzo di politica criminale, escludendo il requisito autorizzativo previsto dall'art. 266 c.p.p..

La norma configurava nella sua ratio una logica di contemperamento degli interessi in gioco in cui la tutela della segretezza delle comunicazioni e l'inviolabilità del domicilio subivano una compressione, proporzionata alla particolare attitudine offensiva per individui e collettività dovuta al contrasto dei reati di particolare allarme sociale.

La necessità di rendere disponibili per gli inquirenti mezzi di ricerca della prova intrusivi in funzione del carattere immanente dei reati di criminalità

[44] Sentenza delle Sezioni Unite Scurato (n. 26889 del 28 aprile 2016).

[45] Le Sezioni Unite affermarono che «l'intercettazione di comunicazioni tra presenti mediante l'installazione di un captatore informatico in un dispositivo elettronico è consentita nei soli procedimenti per delitti di criminalità organizzata per i quali trova applicazione la disciplina di cui all'art. 13 del D.L. n. 151 del 1991, convertito dalla legge n. 203 del 1991, che consente la captazione anche nei luoghi di privata dimora, senza necessità di preventiva individuazione ed indicazione di tali luoghi e prescindendo dalla dimostrazione che siano sedi di attività criminosa in atto».

organizzata, caratterizzati da attività svolte in tutti i luoghi generalmente frequentati dagli autori, ha reso necessaria, nell'ottica del legislatore, una compressione molto più accentuata dei diritti rispetto alle normali attività investigative per il contrasto di altri reati, pur gravi.
Con la disciplina derogatoria, il legislatore sembra aver accettato il rischio di intrusione nei luoghi di privata dimora anche nei casi dalla dubbia definizione indiziaria assumendo, quale conseguenza necessaria, la possibilità di intercettazioni domiciliari dovute alla particolare mobilità dell'apparecchio sede del captatore. Le Sezioni Unite giungevano alla conclusione che «l'intercettazione di comunicazioni tra presenti mediante l'installazione di un captatore informatico in un dispositivo elettronico è consentita nei soli procedimenti per delitti di criminalità organizzata per i quali trova applicazione la disciplina di cui all'art. 13 del D.L. n. 151 del 1991, convertito dalla legge n. 203 del 1991, che consente la captazione anche nei luoghi di privata dimora, senza necessità di preventiva individuazione ed indicazione di tali luoghi e prescindendo dalla dimostrazione che siano sedi di attività criminosa in atto».
L' enorme incisività nell'uso del captatore, in assenza di un quadro normativo specifico sui limiti di impiego, condusse alla riforma Orlando delle intercettazioni del dicembre 2017 (d.lgs. n. 216/2017).
La novella legislativa prese in considerazione esclusivamente la possibilità di inoculare il virus sul dispositivo tralasciando, volutamente o meno, la regolamentazione del suo possibile uso per i fini ulteriori di *on line surveillance* (attivazione *webcam*, *keylogger, screeshot*, acquisizione comunicazioni tramite *instant messaging* ecc.). La novella, infatti, si limitò a ribadire, aggiungendo il comma 2 bis all' art. 266 c.p.p, quanto contenuto nella disciplina derogatoria anzidetta, stabilendo, nei delitti di criminalità organizzata, la legittimità delle intrusioni con impiego del captatore informatico nei luoghi di privata dimora[46].
Al di fuori dei procedimenti per reati di mafia e terrorismo, permaneva la disciplina, ordinaria, del requisito di criminalità in atto presso tali luoghi.

[46] (c.d. Legge "spazza-corrotti" o "anticorruzione") con la quale sono state introdotte nuove misure tese ad «affrontare in modo efficace il fenomeno corruttivo e, in generale, per assicurare una maggiore incisività all'azione di contrasto dei reati contro la pubblica amministrazione».

La disciplina duale nell'uso del captatore spia tra le differenti categorie di delitti ha recepito parzialmente l'orientamento delle Sezioni unite Scurato, laddove era stato ritenuto legittimo l'uso anche per i delitti «comunque facenti capo ad un'associazione per delinquere, con esclusione del mero concorso di persone nel reato».
La complessa e travagliata vicenda si conclude con l'adozione della l. 9 gennaio 2019, n. 3 (c.d. Legge "*spazza-corrotti*" o "*anticorruzione*").
La vicenda, anche in virtù della legislatura da cui è scaturito il provvedimento, caratterizzata, per via delle componenti politiche di maggioranza, da un forte populismo giudiziario, ha rappresentato immediatamente un elemento di dibattito e discussione per addetti ai lavori e non solo.
Ufficialmente introdotta per combattere il fenomeno corruttivo nella pubblica amministrazione, la legge ha apportato modifiche agli art. 266 comma 2 - *bis* e 267 comma 1, c.p.p., estendendo la disciplina derogatoria sull'uso dei captatori informatici, prevista per i delitti di mafia e terrorismo, alle ipotesi di reato commesse dai pubblici ufficiali od incaricati di pubblico servizio contro la pubblica amministrazione, punibili nel massimo in modo non inferiore ai 5 anni, così come previsto dall'art. 4 c.p.p.
Allo stato attuale, la possibilità di intercettare mediante uso del *trojan* le conversazioni tra presenti anche nei luoghi di privata dimora, vale non solo per le ipotesi di reato dal particolare allarme sociale e gravità, ma, in virtù della "*spazzacorrotti*", anche per ipotesi di reato comuni quali quelli commessi nei confronti della pubblica amministrazione dai pubblici ufficiali.
Le recenti esternazioni del guardasigilli Nordio[47], lasciano intendere la possibilità di un ridimensionamento dello strumento, in particolar modo per questi ultimi reati, senza dubbio, poco avvezzi ad una ottica di compressione delle garanzie fondamentali in rapporto alla pericolosità intrinseca degli stessi. Dalle ulteriori iniziative legislative della maggioranza, soprattutto il ddl Zanattin, sembrerebbe emergere tale indirizzo programmatico.

9. *Gli spazi di equilibrio*. Ragionando su tale articolata problematica, è di fondamentale importanza superare elementi emotivi o di pregiudizio caratteristici

[47] Si guardi sempre la relazione al senato del 6-7 dicembre 2022.

del dibattito mediatico e politico, partendo, però, dal necessario presupposto tecnico che il potenziale intrusivo del *trojan* è senza ombra di dubbio di gran lunga superiore a qualsiasi altro strumento di captazione fin ad ora impiegato nelle più disparate attività investigative, eccetto per quelle riguardanti i sevizi di *intelligence*, di cui, nostro malgrado o per fortuna, non è dato conoscere più di tanto lo stato dell'arte in merito.
Si tratta di fatto una attività di intercettazione itinerante, idonea ad essere svolta in qualsiasi luogo, anche in contesti ed alla presenza di soggetti estranei all'attività criminosa.
Tale forza intrusiva richiede necessariamente un contemperamento delle opposte esigenze di tutela della sicurezza collettiva e delle libertà fondamentali estremamente rigoroso48.
Allo stesso tempo, l'evoluzione delle modalità operative delle organizzazioni criminali suscettibili, per loro intrinseca natura, di essere ideate, programmate e portate a compimento in una moltitudine di luoghi, rende all'occorrenza ipotizzabile, durante l'attività investigativa, una proporzionata compressione di alcune garanzie legali afferenti alla vita privata.
La combinazione di tali contrapposte esigenze rende evidente come l'uso del *trojan* possa essere tollerato, in una società democratica, solo in ristrettissimi casi di gravissime ipotesi delittuose, ma eccessivamente sproporzionato in tutte le altre, seppur molto gravi.
A parere dello scrivente, le ragioni poste nella logica di politica criminale in supporto della Legge Spazzacorrotti e la conseguente possibilità di impiego del captatore non sono sufficienti a giustificare una compromissione di valori così pregnanti a garanzia dell'individuo. La disciplina convenzionale dei diritti dell'uomo, all'art. 8 prevede la possibilità di comprimere la sfera privata solo nell'ipotesi del perseguimento di un fine legittimo, previsto dalla legge in modo rigoroso nell'interesse di un bene superiore imperativo, proporzionato al fine medesimo. Una proporzione che, semmai suscettibile di essere adeguata

[48] Le modifiche apportate al codice dal Decreto legge n. 161 del 30 Dicembre 2019 (riforma Bonafede), non sembra essere andata in questa direzione. Al riguardo si veda PRETTI, *La metamorfosi delle intercettazioni: la contro-riforma Bonafede e l'inarrestabile mito della segretezza delle comunicazioni,* su, *sistemapenale,* rivista *online*, 14 Febbraio 2020. Per una ricostruzione delle critiche mosse alla riforma Orlando si veda anche SANTALUCIA, *Vero e falso nelle ragioni della annunciata controriforma delle intercettazioni*, in Cass. pen., 2018, 9, pag. 2761 ss.

nell'ipotesi di contrasto alla criminalità organizzata, con tutte le riserve del caso, difficilmente può essere tollerata in ipotesi comuni.
Nella stesura di una nuova disciplina, si potrebbe tenere in considerazione la possibilità di modulare la captazione del *trojan* in funzione delle circostanze criminose concrete progressivamente nella disponibilità conoscitiva degli investigatori, anche riferite a luoghi specifici, evitando l'acquisizione itinerante ed indiscriminata.
L'attitudine ad eludere le garanzie di segretezza delle risultanze investigative, impiegando i risultati delle attività di intercettazioni in contesti ulteriori e poco attente alle esigenze di tutela della riservatezza, dovrebbero indurre a riflettere sul pericolo di disattenzione al tema e soprattutto, sull'idea che tale problematica riguardi sempre chiunque, buono o cattivo, eccetto noi49.

10. *La gestione dei dati ed il ruolo determinante nel contesto investigativo.*
Come si è potuto osservare anche nelle circostanze inerenti l'impiego dell'intelligenza artificiale, i dati, generalmente intesi, giocano un ruolo fondamentale nell'implementazione delle decisioni umane, sia nel caso di elaborazioni automatizzate tese alla razionalizzazione di contenuto, sia nel caso in cui i dati grezzi vengano gestiti in modo selettivo e circostanziale.
La costante esposizione della società odierna alla digitalizzazione comporta, inevitabilmente, la possibilità oggettiva di recuperare ogni genere di informazione relativa alle abitudini o necessità più intime degli individui.
Ogni giorno, le società digitalmente evolute effettuano una moltitudine di attività nel cyberspazio, il cui impatto, il più delle volte, difficilmente è percepito nel suo insieme dall'utente finale[50].

---

[49] In proposito, cfr. DINACCI, *Intercettazioni e riservatezza tra ampliamenti di disciplina, inconcludenze operative e restrizioni difensive*, in MAZZA (a cura di), *Le nuove intercettazioni*, Torino, 2018, pag. 32. Si veda anche ALONZI, *Contenuti e limiti del diritto di difesa*, in GIOSTRA e ORLANDI (a cura di), *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, Torino, 2018, pag. 93 ss.

[50] Nei tre commi dell'articolo 8 della carta di Nizza, dal titolo "Protezione dei dati di carattere personale" si asserisce che "1. *Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo*

Chiunque ha potuto, banalmente, constatare in prima persona alcuni degli effetti di un simile processo di aggregazione, nel momento in cui si è trovato a ricevere offerte pubblicitarie mirate sul proprio smartphone solo per aver condotto qualche ricerca in rete di un prodotto a cui si è interessati o, magari, solo perché è stato digitato ingenuamente un *like* di gradimento in una pagina *social* di *facebook, twitter, instagram* ecc.

Milioni, se non miliardi, di conversazioni telematiche viaggiano ogni giorno nell'interspazio da un continente all'altro, *e-mail*, *instant messaging*, cinguettii e bacheche di ogni genere pullulano di informazioni inerenti alla vita di ogni persona anche solo connessa in rete, alcune volutamente riservate, altre alla mercé di qualsiasi soggetto possa trovarsi in un dato momento a verificarne il contenuto pubblico[51].

Alcune volte mi è capitato di sperimentare in prima persona, con spirito critico di approfondimento, quello che i sociologi moderni chiamerebbero etnografia digitale. È sufficiente, infatti, dedicare alcuni minuti alla lettura delle interazioni pubbliche di una qualsiasi bacheca *social* o, ancora più nello specifico, in stesure infinite di commenti ai post di personaggi di tendenza per scoprire un universo senza confini di informazioni utili a carpire ogni genere di attitudine alle cose.

Tutto ciò può avvenire senza l'impiego di alcun sofisticato software di elaborazioni dati od alcuna formazione specialistica di carattere investigativo.

Ogni giorno, tramite i nostri spostamenti, forniamo dati precisi sulla posizione geografica in un dato momento mediante le più svariate applicazioni di geolocalizzazione, utili, il più delle volte, a consigliarci il rifornitore meno costoso dell'area oppure il tabacchino più vicino, o, perché no, un potenziale partner disposto a condividere esperienze di ogni tipo mediante avviso preimpostato.

Whatsapp, telegram, messangers ecc., tutti sistemi in apparenza riservati, ma, capaci in ogni istante di fornire informazioni utili a carpire il luogo da cui avvengono le conversazioni degli utenti più avveduti, senza necessità di particolari

---

ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente".

[51] l'articolo 12 della "Dichiarazione Universale dei Diritti dell'Uomo" che recita: "Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni".

prerogative investigative od autorizzazioni giudiziarie in merito, ma per semplice e consapevole scelta di fruire del servizio. Aggiungiamo pagamenti digitali con carte od applicazioni nei punti vendita, tabulati telefoni di inoltro e destinazione delle chiamate giornaliere, tessere di sconto ed offerte dedicate al supermercato dietro l'angolo ed il brodo di coltura delle dinamiche di vita personale è pronto ad essere impiegato nelle più svariate finalità, lecite o meno[52].
L'enorme mole di dati precedentemente appena accennati costituisce in larga misura ciò che comunemente è identificato come insieme di "*dati esterni*" al traffico telematico. Una pletora informativa fino a qualche tempo fa, prima dell'intervento della giurisprudenza europea sul tema, facilmente acquisibile dalle procure, durante l'espletamento delle attività investigative mediante un semplice decreto del P.M., in quanto sua prerogativa con requisito motivazionale minimo o nullo.
Per essere più precisi, alcune delle attività di acquisizione, come ribadito dalla giurisprudenza di legittimità interna, quali la geolocalizzazione od il *positioning*, sono ancora nella disponibilità della polizia giudiziaria senza alcun tipo di autorizzazione[53].

11. *L'evoluzione normativa sul tema.* Il tema dell'acquisizione dei dati esterni ai fini investigativi ha rappresentato per lungo tempo il grimaldello alle garanzie di riservatezza delle comunicazioni poste 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 possibilità, fino alla pronuncia della Corte di Giustizia, ed alla conseguente novella del legislatore nazionale, del P.M., di disporre l'acquisizione dei cd.

[52] Dal *"digital repor*t" del 2020 scritto da Roberta Zanon si evince che «Sono quasi 4,54 miliardi le persone che oggi sono connesse a *internet* e circa la metà della popolazione mondiale, 3,8 miliardi di persone, utilizza regolarmente i *social network*». Inoltre, «più del 60% della popolazione mondiale è o*nline* e le ultime tendenze rivelano che oltre la metà della popolazione totale del mondo utilizzerà i social *media* entro giugno. Sempre per quanto riguarda i *social*, si denota un incremento del 2,4% per gli accessi da mobile, portando complessivamente a più del 90% la percentuale degli utenti che accede direttamente da telefono e confermando sempre di più l'importanza del "*mobile first*"». Per ulteriori approdonfimenti si veda *Report Digital: lo scenario nel mondo e in Italia*, di, Zanon, su *digital dictionary*, sito online, 20 Febbraio 2020.
[53] Cass. pen., Sez. II, 04/04/2019, n. 23172, rv. 276966 e Cass. pen., Sez. II, 13/02/2013, n. 21644, rv. 255542. Cass. pen., Sez. I, 13/05/2008, n. 21366, rv. 240092.

"*dati esterni al traffico telematico*", direttamente dai gestori dei servizi di comunicazione, senza il preventivo o successivo vaglio di legittimità del giudice, ha costituito un fondamentale escamotage propulsivo al formante probatorio durante le prime fasi delle indagini.
Entrare nella disponibilità di una così articolata e consistente mole di storico informatico, senza particolari riserve, ha evidentemente generato per lungo tempo nel legislatore e, ancor di più, nell'opinione pubblica, un pericoloso sonnambulismo, in virtù delle ricadute estremamente perniciose del materiale acquisito, sia per le parti del processo che per eventuali terzi estranei.
Immaginate un soggetto coinvolto in attività di indagine per reati di mafia cui si è resa necessaria, *prima facie*, l'acquisizione dei tabulati telefonici o del traffico telematico esterno delle conservazioni su *instant messaging*. Un primo approfondimento ha evidenziato la circostanza di un continuo interscambio di comunicazioni verbali e di testo con alcuni soggetti, di cui uno, in particolar modo, anche nelle ore notturne. Il successivo approfondimento con strumenti intercettivi ritenuti più intrusivi, l'autorizzazione dei quali necessitava di un gradiente indiziario consistente, nonché l'autorizzazione giudiziale, ha, però, mostrato come, ad un vaglio più attento, gli scambi in questione fossero di natura perfettamente legittima, per lo più di tipo commerciale, ma, alle evidenze logiche, uno di natura *extraconiugale*.
Da un punto di vista processuale, il tutto è andato nel migliore dei modi per il soggetto indagato in quanto, infatti, dall'approfondimento investigativo, è emerso, nelle sue articolazioni per fasi, la legittimità delle condotte, perlomeno dal punto di vista penale, la cui inevitabile conseguenza procedurale è stata la richiesta di archiviazione. Allo stesso tempo, però, considerata anche la funzione pubblica del soggetto, alcune falle all'interno delle procure o la scarsa deontologia professionale degli avvocati interpellati durante le attività garantite, hanno in qualche modo permesso l'emersione del materiale investigativo, seppur parzialmente riferito ai soli tabulati.
È evidente come dallo stesso emerga, però, in modo assai subdolo la circostanza della relazione *extraconiugale*, avvalorata anche dall'assenza di condotte criminose del soggetto nelle dinamiche interessate.
Si potrebbe obiettare che il materiale in questione abbia garantito le prerogative dell'indagato, il quale, mediante le naturali fasi delle attività di indagine, ha visto

infine concludere il procedimento a suo favore. Allo stesso tempo, gli inquirenti hanno avuto la possibilità di effettuare i dovuti accertamenti con strumenti in progressione più invasivi, ma legittimi e destinati ad appurare la possibilità di condotte criminali dal consistente valore criminale.
Entrambe le considerazioni sono vere, resta il fatto che, nonostante il soggetto veda cessare ogni ipotesi di accusa nei suoi confronti, il suo matrimonio giungerà probabilmente a conclusione con tutto ciò che ne consegue in termini di ripercussioni nella vita privata.
Si potrebbe obiettare che le ripercussioni personali di una libera scelta, moralmente riprovevole, ma penalmente legittima, non possano inficiare il regolare svolgimento delle necessarie attività di contrasto alla criminalità e che la libera determinazione della vita privata, nel necessario contemperamento degli interessi in gioco, debba assumere una consistenza cedevole rispetto al primario interesse alla sicurezza collettiva. La verità, come nella maggioranza delle cose sta probabilmente nel mezzo.
Il *vulnus* di tutela, in tal caso, risiede non tanto nella possibilità per gli inquirenti di accedere ai dati in questione, necessari il più delle volte alla conduzione delle indagini, quanto nel potenziale intrusivo delle tecnologie impiegate e su come un cattivo uso delle stesse, per scarsa consapevolezza dello strumento o, peggio ancora, per volontà lesiva, possano impunemente distruggere da un giorno all'altro la vita privata delle persone, anche senza particolari conseguenze sul piano penale.

12. *L'intervento dei giudici europei.* La consapevolezza dei giudici europei di Lussemburgo, circa le criticità anzidette, ha evidentemente spinto la giurisprudenza unitaria ad accelerare il processo di integrazione dei sistemi giuridici nazionali, spingendo verso un adeguamento ai canoni di riferimento di carte e trattati, comunemente accettati[54].
I principi posti a supporto della decisione del marzo 2022 sono di primaria importanza nel complesso equilibrio delle garanzie poste a supporto dei cittadini europei contro gli abusi delle autorità pubblica nel corso delle indagini.

[54] Si veda sul tema RINALDINI, Data retention e procedimento penale. Gli effetti della sentenza della Corte di giustizia nel caso H.K. sul regime di acquisizione dei tabulati telefonici e telematici: urge l'intervento del legislatore, in Giurisprudenza Penale Web, 2021.

Il legislatore nazionale, dopo i primi tentennamenti di una giurisprudenza poco incline ad acquisire senza remore i nuovi principi di diritto eurounitario stabiliti dalla Corte di Giustizia[55], si è, giustamente, premurato di innovare la disciplina in modo conforme a quanto stabilito dalla sentenza, senza trascurare le evidenti esigenze investigative delle procure e l'importanza di acquisire, quando realmente necessario, previa valutazione terza ed imparziale di un giudice completamente indipendente dalle parti in causa, un così delicato complesso informativo56.

L'esigenza garantista era, quantomai, indifferibile ed il caso estone, nonostante i dovuti distinguo con il contesto italiano, ha fornito, senza ombra di dubbio, un'occasione d'oro per i giudici europei di definire una serie di confini invalicabili per una società democratica[57].

L'indirizzo, d'altro canto, sembra essere oramai consolidato e senza possibilità di ripensamento, come si può anche evincere dalle successive decisioni ed in

---

[55] nel provvedimento del GIP del Tribunale di Tivoli «deve essere confrontata con l'assetto normativo attualmente delineatosi nel nostro ordinamento e, in particolare, con il consolidato orientamento della Suprema Corte secondo cui, in tema di acquisizione dei dati contenuti nei cd. *"tabulati telefonici"*, la disciplina italiana di conservazione dei dati di cui all'art. 132 d. lgs. 196/2003 deve ritenersi compatibile con le direttive in tema di *privacy*, e ciò poiché la *deroga stabilita dalla norma alla riservatezza* delle comunicazioni è prevista dall'art. 132 cit. per un periodo di tempo limitato, ha come esclusivo obiettivo l'accertamento e la repressione dei reati ed è subordinata alla emissione di un provvedimento di una autorità giurisdizionale indipendente (come è in Italia il PM)».

[56] Come si può leggere nel preambolo del decreto, l'intervento è stato motivato dalla "straordinaria necessità ed urgenza di garantire la possibilità di acquisire dati relativi al traffico telefonico e telematico per fini di indagine penale *nel rispetto dei principi enunciati dalla Grande sezione della Corte di giustizia dell'*Unione europea nella sentenza del 2 marzo 2021, causa C-746/18, e in particolare di circoscrivere le attività di acquisizione ai procedimenti penali aventi ad *oggetto forme gravi di criminalità* e di garantire che dette attività siano soggette al *controllo di un*'autorità giurisdizionale".

[57] Come noto, la Corte di giustizia dell'Unione Europea ha affermato il principio secondo cui «l'articolo 15, paragrafo 1, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 deve essere interpretato nel senso che esso *osta ad una normativa nazionale*, la quale consenta l'*accesso di autorità pubbliche ad un insieme di dati relativi al traffico o di dati relativi 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*, e ciò indipendentemente dalla durata del periodo per il quale l'accesso ai dati suddetti viene richiesto, nonché dalla quantità o dalla natura dei dati disponibili per tale periodo».

particolar modo con la recente decisione per un caso francese, inerente al tema della "*Data managment*"[58].
Il percorso, iniziato con la dichiarazione di invalidità della direttiva 2006/24/CE cd. "*Frattini*", nel caso "*Digital Rights Ireland"*, ha perseguito il fine di assicurare una adeguata protezione contro le ingerenze della forza pubblica nella sfera privata dei cittadini, al fine di contrastare la criminalità, mediante la crescente richiesta di acquisizione e conservazione dei dati gestiti e generati dagli erogatori dei servizi di telecomunicazione[58]. La Corte, nel rispetto del ruolo di unico interprete del diritto unitario, ha circoscritto, sempre di più, la facoltà dei legislatori nazionali di adeguare in modo discrezionale il proprio diritto interno sul tema delle limitazione al diritto di tutela dei propri dati fondamentali fornendo, anzi, di volta in volta, ha introdotto una serie di strumenti utili a contemperare le contrapposte esigenze delle istante in gioco, cercando di instaurare un equilibrio dinamico in ragione delle circostanze concrete di applicazione del diritto interno.
Nel caso francese, così come in quello Estone, i giudici sono stati chiamati a decidere il limite entro cui agire, nel rispetto dei diritti fondamentali dei cittadini europei, allorquando le autorità decidano d'intervenire sulla disciplina inerente alla conservazione e l'accesso ai dati personali, riguardanti il traffico e l'ubicazione dei fruitori di servizi di telecomunicazione, da parte delle autorità pubbliche nazionali, nelle attività di accertamento e contrasto alla criminalità.
Il caso in questione, in verità, riguardando una fattispecie di reato comune, è stato definito con il principio di una 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.
La Corte, anche in tale occasione, ha ribadito ancora il principio del "*primato del diritto dell'unione"* sul diritto degli stati membri. Il corollario logico

[58] Corte di Giustizia UE (Grande Sezione), 5.4.2022. Si tratta della decisione su un rinvio pregiudiziale volto a stabilire se il regime di conservazione generalizzata e indifferenziata dei dati relativi al traffico e all'ubicazione, ai fini di lotta alla criminalità grave, istituito dalla legge nazionale del 2011 (di recepimento della direttiva 2006/24/CE del 15.3.2006, riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione che modifica la direttiva 2002/58/CE), nonché il regime di accesso a tali dati da parte della polizia nazionale previsto da tale legge, potessero ritenersi compatibili con il diritto dell'Unione.

giuridico sarà la disapplicazione automatica della disciplina nazionale non conforme da parte del giudice senza attendere la rimozione del diritto interno da parte del legislatore, spettando soltanto alla corte, nelle more di un ipotetico rinvio pregiudiziale, la possibilità di una sospensione temporanea negli effetti del diritto interno. Resta inalterato il rispetto dei principi di equivalenza ed effettività cui è soggetto il giudice nazionale nella procedura di acquisizione del materiale probatorio raccolto in contrasto alla normativa europea sul tema59.
La Corte, infatti, ha specificato come si debbano escludere come prove delle 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...*"[60].
La Corte, con la recente sentenza, conferma l'orientamento intrapreso dalla giurisprudenza unitaria, dalla quale si evince che, nell'ottica di un corretto equilibrio tra le esigenze di tutela della sicurezza collettiva ed il rispetto delle libertà fondamentali, la chiave di volta sia rappresentata dal rispetto del principio di proporzionalità, inteso come limite alla capacità intrusiva delle normative nazionali in tema di accesso ai dati inerenti la vita privata degli utenti di comunicazioni elettroniche[61].

13. *Il principio di proporzionalità quale elemento cardine dell'agire (la risposta italiana di politica criminale).* Nell'architettura dell'ordinamento europeo, dunque, il principio di proporzionalità assume il ruolo di criterio dominante nell'attività di adeguamento della disciplina nazionale al diritto eurounitario, il rispetto del quale comporta una invalicabile impossibilità di sconfinamento entro un certo limite nella gestione della materia della vita privata di ciascun cittadino.

---

[59] Per una disamina delle decisioni di merito nazionali intervenute successivamente alla sentenza della Corte UE, 2 marzo 2021, *H.K.*, si veda i Corte Suprema di Cassazione – Ufficio del Massimario e del Ruolo n. 55/21, *"Relazione su novità normativa. Misure urgenti in tema di acquisizione dei dati relativi al traffico telefonico e telematico ai fini di indagine penale"*, 13 ottobre 2021, §4 e ss.
[60] v. in tal senso, 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
[61] Come specificato nel Regolamento (UE) 2016/679, il rispetto dei dati personali "*va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità*" (considerando n. 4).

Eventuali restrizioni dovranno essere necessarie e proporzionate e, soprattutto, funzionali al raggiungimento di un determinato fine legittimo per una società democratica62.
La tutela della sicurezza pubblica, quale interesse collettivo della generalità dei consociati, dovrà essere perseguito, tra le varie forme possibili, nel modo più idoneo a garantire un accesso ed una gestione dei dati di traffico degli utenti con minor sacrificio possibile per la riservatezza della vita privata.
La grande sezione della corte di giustizia, anche nel caso irlandese,63 aveva già ribadito come i dati di traffico fossero intrinsecamente suscettibili di fornire informazioni delicate in merito alla vita privata degli individui interessati dalla loro gestione, rivelando dettagli significativi sulle normali abitudini della vita di ogni giorno, nonché sui luoghi, ambienti e persone frequentate.
Da ciò ne consegue che, già di per sé, l'accesso a tali dati da parte di terzi costituisca una significativa ingerenza nei diritti fondamentali stabiliti dalla carta europea, ingerenza suscettibile di abuso in caso di una gestione non ben garantita64. Nel garantire la proporzionalità, la normativa nazionale dovrebbe prevedere norme chiare e precise, supportate dalla previsione di criteri oggettivi di accesso ai dati.
La portata invasiva della misura prescelta nell'attività di contrasto alla criminalità in proporzione alle finalità per le quali il legislatore nazionale ha

[62] Nella pronuncia del 5 aprile 2022, la Corte, ribadisce che riservatezza e vita privata «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 (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).
[63] Cfr. Corte di Giustizia UE (Grande Sezione), 5.4.202
[64] All'art. 52, paragrafo 2, la Carta 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».

legittimamente scelto la sua adozione, preordinata e chiara, rappresenta il punto di equilibrio tra le opposte esigenze di tutela con il corollario che, oltre ad essere proporzionata, la misura sia anche necessaria e adeguata in una società democratica.

Mentre la salvaguardia della sicurezza nazionale potrebbe, in linea di principio, essere considerato obiettivo idoneo a giustificare una conservazione generalizzata ed indifferenziata dei dati in possesso dei gestori di servizi di telecomunicazione, sempre che ciò avvenga sotto la supervisione di una autorità terza ed imparziale e per lo stretto necessario, la proporzionalità impone che ciò non avvenga nel caso della prevenzione ed accertamento della generalità dei reati. In quest'ultimo caso, l'ingerenza nella vita privata delle persone trascenderebbe il limite del tollerabile per una società democratica.

I principi maturati dalla giurisprudenza europea non sono rimasti, come era giusto attendersi, inascoltati e privi di effetti nel contesto nazionale. Le modifiche al codice di procedura introdotte con la legge 23 novembre 2021, n. 178 di conversione del D.L. 30 settembre 2021, n. 132, tra le altre disposizioni, specifica le nuove modalità di acquisizione dei dati di traffico esterno nel processo penale, definendo confini di legittimità del processo acquisitivo del materiale interessato.

La novella, come chiarito al 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*".

L'art. 132 del codice della *privacy*, relativo ai requisiti di accesso e conservazione dei dati in possesso ai gestori di telecomunicazione, in ottemperanza alle statuizioni della Corte, ha subito un adeguamento negli aspetti di tipo procedurale, col fine di limitare l'applicazione della norma ai procedimenti inerenti gravi forme di reato, predeterminati nel quantum di pena, sotto stretto

controllo di accesso da parte dell'autorità giurisdizionale, eccetto per i casi di urgenza65.
Dal punto di vista sostanziale, permangono perplessità in ordine al rispetto della proporzionalità indicata dalla Corte circa le tempistiche di conservazione dei dati e l'identificazione dei soggetti interessati dal trattamento dei dati.
La novella mantiene inalterato il richiamo alle deroghe previste dall'articolo 24 della legge 20 novembre 2017, n. 167, nei casi di contrasto al terrorismo, estendendo gli ordinari termini di 24 mesi (traffico telefonico), 12 mesi (traffico telematico) e 30 giorni (chiamate senza risposta) estendendolo fino alla considerevole durata di 72 mesi.
Per quanto riguarda il divieto di conservazione "*generalizzata*" e "*indifferenziata*", pone ulteriori perplessità, laddove, diversamente da quanto indicato dalla Corte, prevede un regime di conservazione relativo ad ogni mezzo di comunicazione impiegato senza alcuna distinzione o eccezione.
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 di criminalità che presentino un forte rischio per la sicurezza pubblica o nazionale, sempre per lo stretto tempo necessario66.

---

[65] L'attuale versione dell'art. 132 del Codice *Privacy* prevede: il *potere di controllo preventivo del giudice* (che deve autorizzare l'acquisizione, per finalità di accertamento e repressione dei reati su richiesta dal pubblico ministero o su istanza del difensore dell'imputato, della persona sottoposta a indagini, della persona offesa e delle altre parti private con decreto motivato, fatti salvi i casi di urgenza in cui è prevista una convalida *ex post*). Quanto ai presupposti che legittimano l'acquisizione, la novella prevede che può essere disposta solo se sussistono "*sufficienti indizi di reati*" e soltanto con riferimento ad alcune tipologie di reati, per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni e di reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi.
[66] Per un'ampia illustrazione della riforma introdotta con il D.l. 30.9.21 n. 132, si veda Corte Suprema di Cassazione-Ufficio del Massimario e del Ruolo, Rel. 55/21, *"Relazione su novità normativa. Misure urgenti in tema di acquisizione dei dati relativi al traffico telefonico e telematico ai fini di indagine penale"*, 13.10.21.

Nel caso irlandese, la Corte precisa che gli stati potranno adottare misure conservative solo nell'ipotesi di precedente identificazione dei soggetti, giustificata dal fatto di essere "*sottoposte ad indagine o ad altre misure di sorveglianza in corso o sono iscritte nel casellario giudiziario nazionale ove è menzionata una condanna precedente per atti di criminalità grave che possono comportare un elevato rischio di recidiva*" o, con riferimento ai luoghi interessati dall'indagine solo "*qualora le autorità nazionali competenti ritengano, sulla base di elementi oggettivi e non discriminatori, che sussista in una o più zone geografiche, una situazione caratterizzata da un rischio elevato di preparazione o di commissione di atti di criminalità grave. Tali zone possono essere, in particolare, luoghi caratterizzati da un numero elevato di atti di criminalità grave, luoghi particolarmente esposti alla commissione di atti di criminalità grave, quali luoghi o infrastrutture frequentati regolarmente da un numero molto elevato di persone, o ancora luoghi strategici, quali aeroporti, stazioni o aree di pedaggio*"[67].
Ne deriva che l'attuale regime normativo, recentemente novellato per le giuste ragioni di adeguamento del diritto interno all'ordinamento unitario, non parrebbe essere compatibile con i principi di proporzionalità e stretta necessità ribaditi dai giudici europei, legittimando intrusioni nella sfera privata del cittadino oramai non più tollerabili neanche per le ragioni di carattere generale quali il perseguimento di reati dal particolare allarme sociale.
Il legislatore nazionale potrebbe agevolmente introdurre correttivi di adeguamento in linea con le indicazioni eurounitarie, apportando modifiche alla disciplina inerente alle modalità di conservazione, delimitandola sulla base di criteri più mirati, oggettivi e, soprattutto, non discriminatori.

14. *La prevalenza dei principi unitari.* Nelle more di una complessiva rivalutazione del tema da parte del legislatore nazionale, le criticità relative all'utilizzabilità dei dati già acquisiti impegneranno la giurisprudenza interna, chiamata a decidere sui casi concreti. Il giudice nazionale deve garantire la corretta applicazione ed osservanza del diritto dell'unione nell'ordinamento interno e, allo stesso tempo, ha il potere-dovere di disapplicare la normativa interna non

[67] Corte di Giustizia dell'Unione Europea (Grande Sezione), 5.4.2022, cit. punti da 78 a 81.

conforme, anche qualora il contrasto derivi dalle decisioni della Corte di giustizia europea.
La validità *erga omnes* delle sue statuizioni, anche pregiudiziali, è elemento consolidato68 nella giurisprudenza eurounitaria e riconosciuta, a livello interno, sia dalla Corte di Cassazione69 che dalla Corte Costituzionale[70]. Quest'ultima, in linea con altre Corti costituzionali europee, non ha mancato di manifestare recentemente alcuni ripensamenti in contrario71.
Dovendosi attribuire alla decisione della Corte «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»[72], le stesse dovrebbero produrre i loro effetti anche relativamente alle situazioni ancora in corso, fatta salvo il potere sospensivo degli effetti del diritto interno nelle decisioni pregiudiziali.
Le ragionevoli considerazioni ostative all'applicazione diretta delle statuizioni della Corte di alcuni giudici[73], prima che intervenissero le novelle del legislatore nazionale, d'altro canto, non sono sufficienti a determinare il consolidato orientamento in ordine alla prevalenza del diritto unitario e la sua interpretazione conforme derivante dalle statuizioni della Corte.

---

[68] Corte di Giustizia UE, 27.3.1980, Causa 61/79
[69] Cass. Pen. 17.5.2019 n. 13425
[70] Sentenze gemelle n. 113/85 e 389/89
[71] *"obiter dictum"* della sentenza della Corte Cost. 269/17, nel quale si era affermato che "laddove una legge sia oggetto di dubbi di illegittimità tanto in riferimento ai diritti protetti dalla Costituzione italiana, quanto in relazione a quelli garantiti dalla Carta dei diritti fondamentali dell'Unione europea in ambito di rilevanza comunitaria, debba essere sollevata la questione di legittimità costituzionale".
[72] Cass. Sez. 5, 11.12.2012, n. 22577; cfr. Cass. 2.3.2005 n. 4466 e Cass. 30.08.2004 n. 1735.
[73] Nell' ordinanza del 5.5.21 il GIP del Tribunale di Roma sostenne che ai principi espressi dalla Corte, "*vada attribuito 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*" (così: Cass. 17 maggio 2019, n. 13425; e v. anche Cass. n. 22577/ 2012*)... tale valore di fonte del "significato e dei limiti di applicazione" delle norme comunitarie, proprio delle sentenze della CGUE, possa determinare l'efficacia immediata e diretta delle interpretazioni che indicano solo laddove per effetto di tali interpretazioni non residuino negli istituti giuridici regolati concreti problemi applicativi e profili di discrezionalità che richiedano necessariamente l'intervento del legislatore nazionale , e ciò tanto più laddove si tratti di interpretazione di norme contenute in Direttive*" .

Sarebbero da escludere a priori forzature interpretative di disapplicazione *to court* del novellato art. 132 da parte del giudice nazionale per non operare in scelte eccessivamente discrezionali, lesive della riserva di Legge.
Il principio di autonomia procedurale degli Stati membri, nella definizione del regime di acquisizione delle prove, dovrebbe indurre a ritenere plausibile la competenza esclusiva nella determinazione delle regole di ammissibilità nel processo delle informazioni raccolte mediante la conservazione generalizzata dei dati esterni a condizione, però, che le eventuali regole di diritto interno rispettivo il principio di equivalenza, ovvero 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)[74].
La Corte di Giustizia, nel caso *"Prokuratuur*", ha tenuto a precisare come l'obiettivo del principio di effettività è quello "*di evitare che informazioni ed elementi di prova ottenuti in modo illegittimo arrechino indebitamente pregiudizio a una persona sospettata di avere commesso dei reati*" precisando 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*"[75].
Il corollario logico giuridico determinerà che il giudizio di ammissibilità dovrà essere condotto sulla base della disciplina processuale interna, ma nel limite di acquisizione del materiale su cui i soggetti interessati hanno potuto esercitare un certo margine di controllo e, eventualmente, le rispettive facoltà difensive sulla genuinità ed autenticità dello stesso.
Un ordinamento, realmente garante del rispetto dei principi fondamentali del giusto processo, dovrebbe quantomeno prevedere, per le parti oggetto della richiesta di acquisizione dei dati nella disponibilità delle società di comunicazione, la possibilità, nel contraddittorio, di formulare eccezioni ed opposizioni,

[74] 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.
[75] Corte Giustizia UE, 2 marzo 2021, *Prokuratuur*, C-746/18, EU:C:2021:152, punto 43 e 44.

o, altrimenti, la prova contraria col ricorso a testi e prove a discarico. L'estrema ratio, in assenza dei suddetti profili di garanzia sarebbe rappresentata dalla dichiarazione di inutilizzabilità.
Nell'attesa di un auspicabile ulteriore intervento del legislatore, è di fondamentale importanza il superamento delle significative resistenze già manifestate dalla giurisprudenza nazionale a recepire puntualmente gli impulsi evolutivi delle Corti europee sul tema dell'accesso ai dati esterni.
In un quadro d'incertezza di lungo termine, si corre il rischio di sminuire il valore della statuizione della Corte in ordine alla tutela delle libertà fondamentali nel delicato equilibrio con le contrapposte esigenze di garanzia della sicurezza collettiva e ciò a scapito della coesistenza pacifica in una società democratica.
Gli orientamenti unitari mostrano inequivocabilmente la determinazione verso orizzonti più garantisti in tema di *data retention,* anche dinanzi alle irrinunciabili esigenze della sicurezza collettiva sul suolo europeo.
Nell'epoca caratterizzata dalla esplosione del fenomeno digitale, non si può sottovalutare il pernicioso rischio di intrusioni insopportabili nella sfera soggettiva di ciascun individuo e non si può far altro che condividere le preoccupazioni dei giudici unitari quando affermano che "*L'Internet ha sconvolto le tradizionali strutture del mercato, fornendo un'infrastruttura mondiale comune per la fornitura di un'ampia serie di servizi di comunicazione elettronica. I servizi di comunicazione elettronica accessibili al pubblico, attraverso l'Internet, aprono nuove possibilità agli utenti, ma rappresentano anche nuovi pericoli per i loro dati personali e la loro vita privata*"[76].

15. *Conclusioni.* Il tema dirimente è cercare un punto di equilibrio tra le esigenze di tutela della sicurezza collettiva e la necessaria tutela delle libertà fondamentali, poste costantemente in pericolo da spinte emotive di gestione del rischio, legalo alla potenziale lesione di beni giuridici fondamentali quali la vita e l'ordine pubblico, soggetti a creativi fenomeni di criminalità organizzata, il più delle volte indefinita nel tempo e nello spazio, ma anche oggetto di un pronto ed attento interesse del legislatore, affascinato spesso e volentieri da facili

[76] Cfr. Corte di Giustizia UE, 5 aprile 2022, *Commissioner of the Garda Síochána*, Causa C-140/20, punto 3.

soluzioni di breve durata a prescindere dalle conseguenze di lungo termine nell'architettura degli equilibri democratici dei moderni stati di diritto.
L'obiettivo della ricerca, partendo da un'analisi delle esperienze già maturate nella gestione di emergenze transnazionali in ambito terroristico e non solo, è stato affrontare più nello specifico il processo evolutivo deteriore caratterizzante il ventennio post attentato delle torri gemelle, da alcuni ritenuto il vero *change moment* nella inversione del paradigma garantista a fronte di una *security evolution* in chiave totalizzante ed incurante di conquiste secolari nella tutela di libertà fondamentali, ritenute quasi scontate come il giorno e la notte in una *inversion attitude* volta a sgretolare pilastri dell'architettura etica e giuridica moderna.
Attraverso l'analisi dell'evoluzione legislativa ed alcuni *case studies* di notevole importanza è stato possibile approcciare ai moderni strumenti di *justice supplies* quali i *captatori informatici* ed i*ntelligenza artificiale* in modo critico e scevro da preconcetti formativi nell'esclusivo interesse di evidenziarne sia aspetti utili nella gestione giudiziaria del fenomeno criminale che innumerevoli rischi nel loro uso improprio a scapito delle conquiste di civiltà giuridica maturate anche nel sangue dei nostri padri fondatori.
L'auspicio è che forti e pressanti esigenze di tutela della sicurezza collettiva non diventino mai espedienti improvvisati ed artificiosi di fenomeni prevaricanti ed annichilenti del pensiero liberale di cui è necessario mantenerne intatto il radicamento nei moderni sistemi democratici. Insomma, bene la tecnologia, bene il supporto di innovativi strumenti alle attività di *intelligence*, investigative o giudiziarie, ma attenzione a non permettere che le stesse possano prevaricare il limite dell'umano tollerabile in una visione manichea del bene contro il male, anche a costo del sacrificio di noi stessi e dei nostri fondamentali valori di convivenza democratica.