OSSERVATORIO CYBER SECURITY
EURISPES

Conferenza Nazionale Sicurezza e Legalità

Napoli, 16-18 Novembre 2018

TAVOLO TEMATICO CYBER SECURITY

RELAZIONE OSSERVATORIO CYBER SECURITY

(*Prof. Avv. Roberto De Vita, Avv. Valentina Guerrisi, Avv. Antonio Laudisa*)

IDENTITA' DIGITALE E RESPONSABILITA'

Quando viene evocato il concetto di cyber security, questo viene spesso immaginato e percepito in termini di problema tecnico e/o come risorsa per disciplinare e gestire minacce tecniche e massimizzare la sicurezza.

La centrale distinzione tra vulnerabilità strutturali (cui hanno sempre fatto riferimento gli attori del mondo della cyber security) e vulnerabilità comportamentali sta assorbendo i principali sforzi cognitivi e di sintesi nell'individuazione delle modalità di reazione ai rischi del cyber spazio: infatti, bisognerebbe partire dal drammatico assunto secondo cui la sicurezza informatica al 100% non esiste. Questo limite non incontra tanto le resistenze degli sviluppi tecnologici, quanto invece l'aspetto dell'interazione umana nell'ambito del contesto della cyber security: i rischi di ignoranza, errore, distrazione, tradimento e crisi di coscienza dell'essere umano hanno esposto anche le agenzie e i contesti considerati sicuri ed inaccessibili per definizione.

Questo pericolo non consente di calcolare, con precisione matematica, tutte le forme di vulnerabilità che gli ecosistemi digitali, partecipati necessariamente dall'uomo, possono manifestare.

D'altra parte, ulteriore rischio attiene alle ricadute che la mancanza di sicurezza digitale - e di responsabilità digitale - degli attori della rete possa generare in termini di "human security": tramite disinformazione e manipolazione del consenso, attraverso il

pericolo delle lesioni reputazionali (brand reputation ma anche personal reputation) le informazioni provenienti dalle risorse *cyber* possono manifestarsi quali rischi o minacce per individui, gruppi, organizzazioni o anche Stati.

Queste concrete minacce alle libertà democratiche e alla leale competizione imprenditoriale hanno severe ricadute in termini economici e sociali, purtroppo destinate ad aumentare: infatti, l'impiego dell'intelligenza artificiale, l'uso di algoritmi e decisioni automatizzate non potrà che amplificare la portata quantitativa e, soprattutto, qualitativa del fenomeno.

Tuttavia, la gran parte dei pericoli non è esclusiva conseguenza di condotte criminali o manipolatorie, ma di comportamenti (e cattive abitudini) di vita digitale, spesso guidati dall'idea – molto sociale - che quel che accade agli altri non accadrà a noi; l'internauta fatalista è anzitutto preda di una sorta di sindrome dissociativa che lo porta a comportarsi come se esistessero due mondi separati e poco comunicanti, quello digitale e quello reale: il primo, luogo delle libertà assolute (e dei pericoli relativi) e il secondo, quello delle convenzioni sociali tradizionali (e dei pericoli concreti).

In realtà, come sostenuto dal Prof. Gregory Simons, esistono tre tipi di ambiti nel regno umano: l'ambito fisico dove gli eventi accadono oggettivamente in uno spazio e tempo reali; l'ambito dell'informazione, dove gli eventi ed accadimenti dell'ambito fisico sono comunicati al pubblico globale, ma potrebbero non avere una descrizione oggettiva a causa del perseguimento di un programma politico o economico; e infine l'ambito cognitivo, che è quello in cui gli altri due ambiti vengono processati dalla mente umana che crea opinioni e percezioni delle informazioni ricevute.

Così, poco inclini a riconoscere l'unicità di sintesi del nostro io reale e digitale, ci dimostriamo diffidenti nella vita reale e disinibiti/ingenui in quella digitale: spesso, infatti, quando si parla di pericoli della rete, se ne considera più la dimensione tecnica e malevola, che quella comportamentale, tanto sul piano individuale quanto sul piano sociale.

Mano a mano che la società, le vite e i lavori diventano digitali e i pericoli camminano con le opportunità, il concetto di cyber crime rischia di divenire angusto e incapace di educare i comportamenti, se non su un piano tecnico.

Al contrario, il concetto di cyber risk – termine socialmente inclusivo e idoneo a rappresentare il punto di partenza per l'educazione al comportamento digitale – ben evidenzia come l'unico strumento effettivo di reazione ai pericoli della rete sia la consapevolezza del rischio e la cultura della prevenzione.

SOCIAL MEDIA E MANIPOLAZIONE DEL CONSENSO – WEB REPUTATION – INTELLIGENZA ARTIFICIALE

1. SOCIAL MEDIA E MANIPOLAZIONE DEL CONSENSO

Per comprendere portata e rilevanza del fenomeno *social* occorre prendere le mosse dai dati più recenti sulla diffusione di internet e dei social media: su circa 4 miliardi di utenti Internet (il 53% della popolazione mondiale), 3.196 miliardi di persone sono utenti attivi di social media e di questi 2.958 miliardi lo fa tramite dispositivo mobile; si stima che nell'ultimo anno la crescita dei fruitori di social media sia stata del 14%[1]. Basti pensare che soltanto Facebook vanta oltre 2,2 miliardi di iscritti, sebbene di recente sia cresciuta meno del previsto.

Numeri impressionanti, legati sicuramente alle incredibili potenzialità di interconnessione, condivisione e intrattenimento di internet e delle piattaforme social; accanto a questi, però, si collocano evidenti rischi di sottovalutazione dell'impatto degli stessi sulle garanzie democratiche e di libertà individuale.

Infatti, l'ubiquità della rete ed il predominante utilizzo di tali strumenti genera un'indiscriminata fiducia degli utenti in queste piattaforme e, più in generale, nel mondo digitale: sebbene un tempo fosse – giustamente – celebrata la libertà di espressione, di condivisione di contenuti e di manifestazione del proprio io, sempre più di frequente abbiamo assistito all'effetto opposto su libertà di pensiero e di partecipazione politica.

L'Oxford Internet Insitute ha, nel proprio rapporto di luglio 2018[2], denunciato in maniera sempre più forte il rischio attuale per la democrazia legata alla manipolazione del consenso: *"In tutto il mondo, una schiera di agenzie di governo e partiti politici sta impiegando le piattaforme social per diffondere notizie spazzatura e disinformazione, per esercitare censura e controllo, per minare la fiducia nei mezzi di informazione,*

[1] Report WeAreSocial, Gennaio 2018.
[2] O.I.I. – "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation", 2018.

nelle istituzioni pubbliche e nella scienza. In un periodo storico in cui la fruizione di notizie è sempre più digitale, l'intelligenza artificiale, le big data analytics e i c.d. "black box algorithms"[3] *vengono utilizzati per sfidare verità e fiducia: i capisaldi della nostra società democratica"*[4]*.*

L'indagine ha riscontrato che in 48 paesi nel mondo (a fronte dei 28 dello scorso anno) ci sono campagne organizzate di manipolazione dell'informazione sui social media e che in ognuno di tali Paesi c'è almeno un partito politico o un'agenzia di governo che utilizza i social media per manipolare l'opinione pubblica: spesso la diffusione di notizie spazzatura è volta ad orientare l'opinione pubblica nei periodi di elezioni e di campagne elettorali.

In particolare, in cinque di questi quarantotto Paesi le campagne di disinformazione si realizzano tramite app di messaggistica istantanea (Whatsapp, Telegram, Wechat) e, più in generale, è sempre più diffuso l'utilizzo di bot e fake account, assieme all'impiego di indicizzazione e aggregatori logici, così da garantire l'automazione della "social media propaganda".

Ma qual è la portata economica di questo fenomeno? Dal 2010 ad oggi partiti politici e autorità governative hanno speso più di mezzo miliardo di dollari in ricerca, sviluppo e implementazione dell'attività di manipolazione dell'opinione pubblica tramite social media[5].

Un esempio evocativo di manipolazione da fake news, ormai datato, riguarda il referendum britannico Brexit, quando molti elettori britannici furono convinti dal tam-tam mediatico che con l'uscita dall'Unione Europea avrebbero risparmiato 350 sterline a settimana. Per quanto riguarda gli USA e la diffusione delle fake news nell'ultima campagna presidenziale americana, uno studio dell'Università di Stanford ha certificato la presenza di 115 notizie false pro-Trump e 41 pro-Clinton; le notizie false pro-Trump sono state condivise 30 milioni di volte su Facebook, quelle pro-Clinton 7,6 milioni[6].

Anche nei media italiani sono comparse, nel tempo, numerose fake news come, ad esempio, le presunte assunzioni a Palazzo Chigi di familiari dell'ex Presidente della Camera dei Deputati.

[3] Ossia quegli algoritmi di cui non si conosce la precisa logica di funzionamento.
[4] Cfr. Nota 2.
[5] Cfr. nota 2.
[6] H. Allcott, M. Gentzkow – Social media and fake news in the 2016 election, Journal of Economic Perspective, Vol. 31 n. 2, 2017 – Standford University.

L'attualità e potenza espansiva del problema della disinformazione è particolarmente avvertito anche dall'opinione pubblica: secondo i dati del 2018 Edelman Trust Barometer, il 63% delle persone intervistate (in oltre 28 Paesi) ha ammesso di non saper riconoscere se una notizia sia vera o sia falsa, mentre 7 intervistati su 10 hanno riconosciuto di temere le fake news al punto tale da considerarle "un'arma"[7].

D'altro canto, l'indagine dell'European Communication Monitor tra i professionisti della comunicazione ha evidenziato come i social media siano considerati la fonte principale di diffusione della disinformazione (59,6%), ma anche come i tradizionali mass media non si siano dimostrati immuni a questo tipo di fenomeno[8]; tanto che, sempre secondo l'EMC, questo dato dimostrerebbe come il recupero di fiducia nei confronti dei mass media tradizionali (dato emergente dallo studio Edelman) non ponga l'opinione pubblica a riparo da tale fenomeno.

Il tema della disinformazione ha quindi rappresentato, inevitabilmente, un fenomeno particolarmente allarmante a livello sociale, istituzionale e dei grandi player IT: in particolare, già da tempo questi ultimi hanno avviato iniziative volte ad introdurre meccanismi di fact-checking e di conseguente evidenziazione delle notizie "certificate", come ad esempio è avvenuto per Google e per Facebook.

A fronte di questi dati allarmanti, il 26 Aprile 2018 la Commissione Europea ha varato la propria Comunicazione sulla lotta alla disinformazione online, con cui si propongono diverse misure tra cui **"***la realizzazione di un codice di buone pratiche dell'UE sul tema della disinformazione, il sostegno a una rete indipendente di verificatori di fatti e l'adozione di una serie di azioni volte ad incentivare il giornalismo di qualità e promuovere l'alfabetizzazione mediatica***"**[9].

Sempre secondo la Commissione, la disinformazione consiste in un'"*informazione rivelatasi falsa, imprecisa o fuorviante concepita, presentata e diffusa a scopo di lucro o per ingannare intenzionalmente il pubblico, e che può arrecare un pregiudizio pubblico"*.

[7] https://www.edelman.com/trust-barometer
[8] European Communication Monitor, 2018.
[9] Commissione Europea – Comunicato Stampa del 26.04.2018

Gli studi a cui l'istituzione europea fa riferimento sono tratti dall' "*High Level Expert Group on Fake News and Online Disinformation*" [10], che con il report del Marzo 2018 suggerisce di promuovere l'alfabetizzazione mediatica per contrastare la disinformazione e di sviluppare strumenti che consentano di combatterla, portando avanti la ricerca sul tema e difendendo la diversità ed il pluralismo dei mezzi di informazione europei.

In particolare, tra i principi chiave segnalati dai 39 esperti, vi è l'invito alle piattaforme online a spiegare il funzionamento degli algoritmi che determinano la visibilità dei contenuti, ad una maggiore trasparenza sull'utilizzo dei dati personali per scopi pubblicitari e alla distinzione tra contenuti sponsorizzati e informazione; in ultimo, si auspica una maggiore visibilità delle fonti di informazione affidabili e la possibilità di rispondere sulle piattaforme con link a siti di fact-checking.

Il tema è particolarmente sentito proprio in vista delle prossime elezioni del Parlamento Europeo di maggio 2019, di cui si vuole garantire il corretto svolgimento, in assenza di condizionamenti esterni: proprio per questa ragione, la Commissaria Europea per l'Economia e per la Società digitali ha annunciato, a fine settembre 2018, che le principali piattaforme che operano in rete (Facebook, Google, Twitter e Mozilla) hanno aderito all'auspicato codice di auto-disciplina, che prevede l'adozione di specifiche strategie per combattere la disinformazione online.

Tra i vari bullet del Codice, ha primario rilievo il controllo dei bot e dei fake account: la materia desta, infatti, particolare interesse e preoccupazione; le stesse piattaforme *social* più importanti hanno dichiarato guerra agli account automatizzati. In particolare, Twitter ha di recente aperto alla possibilità di segnalare, da parte dell'utente, l'esistenza (o il sospetto dell'esistenza) di account automatizzati. Tuttavia, il report trimestrale di fine ottobre della società statunitense riporta come la base di utenti mensili sia scesa, globalmente, di ben 9 milioni: la stessa azienda aveva perduto, nel trimestre precedente, un milione di account.

Se questi sono le contromisure europee, in Italia – nonostante una discussione sul tema pressoché quotidiana, anche a fronte del recente episodio che ha visto il Presidente della Repubblica "sotto attacco" di alcuni account automatizzati che lanciavano offese e ne domandavano le dimissioni – le contromisure normative per i diffusori di fake news non sono andate oltre alcune proposte di legge, con cui si è

[10] Il Gruppo, nominato dalla Commissione nel Gennaio 2018, rifiuta la definizione ristretta di "fake news".

proposta l'introduzione di sanzioni per produttori e diffusori di notizie false, tramite l'introduzione di specifiche norme penali[11].

2. WEB REPUTATION AZIENDALE E INDIVIDUALE

È opportuno considerare come la disinformazione in rete non tenda solo alla manipolazione del consenso elettorale o politico, ma incida inevitabilmente sulle sorti economiche di imprese e aziende, che quotidianamente devono confrontarsi con la più grande delle chimere di questo secolo: la web reputation ed il reputation damage/risk.

Il rischio di "brand reputation damage" rappresenta, secondo i rapporti delle più importanti agenzie assicurative del pianeta, il principale pericolo che corrono società ed imprese; in un'indagine dello scorso anno, è emerso come il rischio reputazionale**,** insieme a quello operativo, fosse quello più temuto dai CEO di 10 Paesi, in 11 diversi settori industriali[12].

Ormai da qualche anno organizzazioni come il World Economic Forum ed il Reputation Insitute, collocano il rischio reputazionale al vertice dei rischi maggiormente percepiti a livello globale.

Il concetto di reputazione, dunque, sebbene rappresenti un rischio collaterale che tutte le moderne organizzazioni devono valutare e gestire, per quanto sia difficilmente quantificabile, diventa una priorità.

La rilevanza economica del fenomeno è evidente negli ambiti più disparati: basti pensare a commenti e recensioni online e al tema della responsabilità dell'Internet Service Provider, alla diffusione di fake news sui social media che hanno affossato la reputazione di grandi multinazionali, al danno reputazionale come ulteriore conseguenza per una compagnia vittima di data breach.

Con riferimento al primo esempio citato, il panorama dei giuristi comunitari si domanda se il provider debba essere considerato una figura neutra, oppure un vero e

[11] D.D.L. S. 2688 del 7.02.2017.
[12] KPMG - *2017 Global CEO Outlook.*

proprio "giudice" del servizio che offre: è così difficile imporre al provider un obbligo di sorveglianza sui contenuti pubblicati?

Sul punto, recenti pronunce della Corte di Giustizia UE tendono a riconoscere una più intensa responsabilità dell'ISP, con specifico riferimento alla tutela del diritto d'autore[13]: questi ultimi, secondo la Corte, non svolgono soltanto una funzione di intermediazione, ma spesso svolgono una attività di gestione e amministrazione delle varie piattaforme e ulteriori attività non esclusivamente automatiche, come l'indicizzazione ed il filtraggio dei contenuti.

D'altro canto, anche la reputazione di ognuno di noi è costantemente esposta ai medesimi rischi: cyberbullismo alimentato da fake news, revenge porn, sexual extortion sono solo alcuni dei rischi che ogni individuo interconnesso affronta.

Ciò considerato in materia di rischi politici, strategici ed economici, il dato più preoccupante dovrebbe provenire dalla seguente considerazione: l'innovazione tecnica e scientifica ci sta concretamente introducendo pian piano nel mondo degli algoritmi e delle decisioni automatizzate, rendendo possibile quello che nel secolo scorso era materia di pura fantascienza.

L'applicazione dell'intelligenza artificiale ai preoccupanti temi della creazione e diffusione di falsa informazione, capace di alterare il consenso e l'opinione pubblica, è in grado di determinare conseguenze esponenzialmente superiori a quelle finora analizzate, dal punto di vista numerico e fenomenologico.

3. INTELLIGENZA ARTIFICIALE E ALGORITMI

"*Dalla polizia, ai sistemi di welfare, al dialogo online e all'assistenza sanitaria - per citare alcuni esempi - i sistemi che impiegano tecnologie di machine learning possono cambiare o rafforzare ampiamente e rapidamente le strutture di potere o le disuguaglianze su scala senza precedenti. Con danni significativi ai diritti umani. Vi è un insieme sostanziale e crescente di prove per dimostrare che i sistemi di apprendimento automatico, che possono essere opachi e includere processi*

[13] Corte di Giustizia, Sentenza C-610/15 del 14 giugno 2017.

inspiegabili, possono facilmente contribuire a pratiche discriminatorie. O altrimenti repressive se adottate senza le necessarie salvaguardie."[14]

Così si apre la Dichiarazione di Toronto (punto n. 4 del Preambolo), presentata da *Amnesty International* e *Access Now*, redatta al fine di tutelare l'uguaglianza e la non discriminazione nei sistemi di apprendimento automatico, che lancia in maniera decisa un allarme sull'utilizzo di algoritmi (e big data).

Sebbene l'impiego di algoritmi, così come di tecniche di *machine learning* e *deep learning* possa avere utilizzi pressoché sconfinati, due sono le macro aree su cui insistono i principali problemi etici e normativi: l'individuazione di un principio di responsabilità (*accountability*) e di un insieme di regole rispetto alle attività eseguite da un sistema informatico, sulla base dei propri calcoli e del proprio conseguente apprendimento; il rischio che l'impiego di decisioni automatizzate (sulla base di algoritmi sconosciuti o difficilmente comprensibili) possa determinare diseguaglianze e discriminazioni.

Infatti, l'AI pensa attraverso gli stessi schemi della mente umana, come le architetture cognitive e le reti neurali, agisce come gli esseri umani, giungendo all'elaborazione del linguaggio naturale, alla rappresentazione della conoscenza, al ragionamento automatico e all'apprendimento: ad esempio, gli ultimi prodigi della tecno-scienza hanno permesso di conoscere programmi in grado di utilizzare algoritmi che non solo creano il bit-rate delle canzoni, ma anche il testo, cioè tutto ciò di cui una canzone parla; oppure, un nuovo tipo di intelligenza artificiale, basata su reti neurali capaci di comprendere la musica in tempo reale, potendo conoscere il codice di improvvisazione di un musicista.

La centralità di queste sfide etico-normative è evidente se ci si confronta con i dati prognostici di natura economica legati al fenomeno AI: secondo il McKinsey Report 2018 entro il 2030 l'AI contribuirà al PIL mondiale per una quota di circa 13 trilioni di dollari e la crescita più consistente si realizzerà tra il 2026 ed il 2030[15], con un valore medio dell'1,2 % annuo. PWC invece, nel suo rapporto, ha ipotizzato che l'AI aggiungerà al PIL globale 15,7 trilioni di dollari entro il 2030[16], con un aumento del 14%.

[14] "The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning system".
[15] McKingsey Global Institute - Notes from the AI frontier, 2018
[16] PWC – 2018 AI Predictions

Paesi leader nel mondo nell'applicazione dell'AI sono sicuramente Cina e Stati Uniti: sempre secondo PWC, nel 2017 la Cina rappresentava il 48% dei fondi investiti in Intelligenza artificiale, mentre gli Stati Uniti il 38%. È proprio il paese asiatico a volersi issare quale leader dell'economia mondiale del settore: dal medesimo rapporto, si apprende che Cina e Stati Uniti conseguiranno guadagni pari circa – rispettivamente – al 26% e al 14% del proprio PIL grazie all' AI, raggiungendo la somma di 10,7 trilioni di dollari, ossia il 70% dell'impatto economico su scala globale.

Numerosi sono i settori attinti dall'impatto dell'AI, con le conseguenti ricadute anche in ambito individuale, sociale, democratico e di tutela dei diritti umani: tra questi vi sono il ramo sanitario, i servizi finanziari, il settore manifatturiero, l'automotive, l'energia, la tecnologia, le comunicazioni e l'intrattenimento.

Tuttavia, l'impiego di algoritmi ed intelligenza artificiale si riflette anche in scelte di natura strettamente politica, come l'utilizzo, sempre da parte della stessa Cina, di sistemi di elaborazione tramite algoritmi dei Big Data al fine di adottare decisioni di politica estera: in caso di decisioni importanti e urgenti da prendere, l'AI aiuta a vagliare i diversi scenari possibili e offre diverse opzioni, sulla base dell'enorme mole di dati raccolta dallo stesso governo cinese.

In ambito geopolitico, economico e decisionale (si pensi alla sfera della giustizia predittiva), l'intelligenza artificiale si caratterizza per la capacità di analizzare enormi quantità di dati scientifici e tecnologici in tempi stretti e, soprattutto, per l'altrettanto rilevante possibilità di analizzarli senza l'incidenza di fattori emotivi ed etici propri di un essere umano.

Sebbene questo aspetto possa avere degli indubbi vantaggi in materia di aumento di efficienza nei sistemi produttivi, i rischi di utilizzi distorti si affacciano con la medesima rapidità degli entusiasmi dei più ottimistici fautori della superiorità dell'intelligenza artificiale.

È così che sovviene immediatamente l'opinione di Nick Bostrom, docente alla Oxford University e direttore del Future of Humanity Insitute, che nella sua ultima grande opera "Superintelligenza"[17], analizza i pericoli di un'intelligenza artificiale che è destinata a superare le capacità cognitive dell'intelligenza umana, imparando dai propri errori e costruendo un nuovo modo di pensare.

[17] N. Bostrom, "Superintelligenza – Tendenze, pericoli, strategie", Bollati Boringhieri 2018.

Lo stesso Bostrom suggerisce la possibile adozione di due differenti percorsi di gestione dell'A.I., ovvero la limitazione "fisica" delle capacità di calcolo ed elaborazione di informazioni, oppure la selezione delle c.d. motivazioni, cioè di un insieme di regole etiche – secondo vari e diversi modelli – che impediscano l'azione indiscriminata della superintelligenza.

Attratti dalle innumerevoli potenzialità e al contempo preoccupati dai rischi paventati, numerosi Paesi (tra cui Stati Uniti, Cina, Francia, India, Italia, Giappone, Singapore, Corea del Sud, Svezia, Emirati Arabi) stanno studiando o sviluppando strategie nazionali sull'intelligenza artificiale.

Negli Stati Uniti a dicembre 2017, è stata presentata una proposta di legge[18] tesa alla creazione di un piano globale per promuovere, governare e regolare l'intelligenza artificiale; da tale normativa, è interessante trarre il dato definitorio del concetto di intelligenza artificiale, che racchiude contesti e sviluppi non ancora esplorati di sistemi tanto in ambito software, quanto hardware : "*Qualsiasi sistema artificiale che esegua attività in circostanze variabili e imprevedibili, senza una supervisione umana significativa o che possa apprendere dalla propria esperienza e migliorare le proprie prestazioni […]*".

Inoltre, sempre negli USA è in discussione una proposta di legge in materia di intelligenza artificiale[19], nel settore della sicurezza nazionale e dell'intelligence, tesa alla creazione di una Commissione di sicurezza nazionale indipendente sull'intelligenza artificiale.

Per quanto riguarda la Cina, lo scorso anno il Governo ha lanciato il suo piano per guidare il mondo nell'intelligenza artificiale entro il 2030, puntando a far divenire la Cina il leader mondiale dell'intelligenza artificiale.

Anche l'Unione Europea, con la comunicazione "*L'Intelligenza artificiale per l'Europa*" del 25 Aprile 2018, sta proponendo agli Stati membri un approccio coordinato, sottolineando come uno dei fattori decisivi per la crescita economica passi proprio dall'adozione dell'Intelligenza artificiale in tutti i settori economici[20].

Tale comunicazione è stata preceduta da una Dichiarazione di cooperazione relativa alla materia, datata 10 aprile 2018, firmata da 24 Paesi membri dell'UE più la

[18] https://www.congress.gov/bill/115th-congress/house-bill/4625/text
[19] https://www.congress.gov/bill/115th-congress/house-bill/5356/text
[20] https://ec.europa.eu/digital-single-market/en/news/eu-member-states-sign-cooperate-artificial-intelligence

Norvegia, che contiene l'impegno a dare luogo a una strategia comune finalizzata a cogliere sfide ed opportunità dell'AI.

Per tale ragione, la Commissione ha nominato l'"*High-Level Expert Group on Artificial Intelligence*"[21], composto da 52 esperti, tra cui 4 italiani, con il compito, tra gli altri, di redigere delle specifiche linee guida sui principali temi etici e giuridici che coinvolgono l'AI: dallo sviluppo del mercato del lavoro, alla trasparenza, al futuro della democrazia; per affiancare gli esperti individuati, l'UE ha lanciato la "*European AI Alliance*", una piattaforma volta a favorire il confronto e la partecipazione, tramite contributi di cittadini, imprese e studiosi sul tema.

L'Italia sta pian piano comprendendo la rilevanza tecnica, economica e giuridica del fenomeno e attraverso il Ministero dello Sviluppo Economico sta costituendo un gruppo di esperti che lavorerà alla redazione di una Strategia Nazionale IA italiana[22].

Tuttavia, è altrettanto concreto il pericolo che le decisioni automatizzate mettano (e stiano già mettendo) in crisi la complessa ed altrettanto delicata struttura su cui si fonda l'odierno sistema di diritti umani e libertà fondamentali.

È il Consiglio d'Europa a rilevare l'importanza del tema e le potenziali ricadute, sottoponendo la Convenzione Europea dei diritti dell'Uomo ad una sorta di prova di resistenza, da cui è emerso un rapporto frutto del lavoro di una commissione mista, composta tanto da esperti della materia quanto da rappresentanti delle piattaforme digitali[23].

Tra le varie conclusioni a cui giunge il Consiglio d'Europa, acquisisce primaria centralità il tema del sostegno alla ricerca – rispetto ad utilizzo di algoritmi e implicazioni giuridiche – e della responsabilizzazione delle autorità pubbliche per le decisioni assunte sulla base di algoritmi, della necessaria realizzazione di una "*human rights impact assessment*" in tutte le aree decisionali coinvolte dall'impego di algoritmi, nonché l'adozione di sistemi di monitoraggio della nuova tecnologia nei periodi di elezioni e di campagne elettorali.

[21] https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence

[22] Da non sovrapporre alla task force AgID, improntata allo studio di come la diffusione di soluzioni e tecnologie di Intelligenza Artificiale possa essere applicata alla gestione dei servizi pubblici, al fine di migliorare il rapporto tra PA e cittadini. Questa task force ha condotto alla pubblicazione del Libro Bianco sull'intelligenza artificiale di AgID.

[23] "Algorithms and human rights – Study on the human rights dimension of automated data processing techniques and possible regulatory implications" – Council of Europe study DGI (2017)12.

D'altra parte, il COE tiene a sottolineare che l'innovazione tecnologica potrà essere correttamente gestita e governata solo attraverso la possibilità di stimolare il dibattito e la consapevolezza di tutti gli attori della società: tuttavia, per quanto importante, il coinvolgimento generalizzato dell'opinione pubblica su questo tema non sarà sufficiente laddove non preveda la collaterale creazione di nuove istituzioni, nuovi spazi di confronto e nuovi network attraverso cui mettere in contatto tutti gli stakeholder, pubblici e privati, che si approcciano alla nuova fonte di guadagno.

Gli impatti dell'intelligenza artificiale e dell'impiego di algoritmi saranno ad amplissima portata, anche in relazione al trattamento e alla protezione dei dati personali: su questo vasto tema, l'Unione Europea ha da tempo varato un piano di data protection delle persone fisiche, composto dal noto Regolamento 679/2016 (G.D.P.R.), dalle direttive n. 680/2016 e 681/2016[24].

L'Unione Europea si è dunque preoccupata di tutelare le persone fisiche dal trattamento dei dati, con una normativa "elefantiaca", che spesso risulta difficile comprensione ed applicazione/adeguamento ai casi concreti e dei singoli Paesi: tuttavia, questo rappresenta un decisivo passo in avanti rispetto al passato.

In particolare, la citata direttiva n. 680/2016 aveva l'obiettivo di disciplinare il "*trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica*"[25].

In materia di trattamenti automatizzati, la direttiva prevede all'art. 11 che "*una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, che produca effetti giuridici negativi o incida significativamente sull'interessato sia vietata salvo che sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che preveda garanzie adeguate per i diritti e le libertà dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento*".

L'apparente generale divieto di trattamenti automatizzati in ambito penale incontra un temperamento nell'indicazione di eventuali autorizzazioni del diritto dell'Unione o degli Stati Membri, ritenendolo possibile in caso di garanzie adeguate e di previsioni volte a favorire l'intervento umano da parte del titolare del trattamento.

[24] L'Italia ha recentemente recepito le due direttive con i D. Lgs. 51/2018 e 53/2018, mentre il D. Lgs. 101/2018 ha segnato l'adeguamento del Codice Privacy (D. Lgs. 196 del 2003) al GDPR.
[25] Direttiva UE 680/2016.

Di recente, l'Italia si è adeguata a tale direttiva, adottando il D. Lgs. 51 del 2018, in cui si affronta lo spinoso tema delle decisioni automatizzate in ambito penale: in particolare, l'art. 8 – ricalcando la previsione della direttiva – replica, allo stato, il divieto di profilazione a fini penali.

Tuttavia, vi sono delle eccezioni: pur escludendo i trattamenti discriminatori e prevedendo che debba essere garantito il diritto dell'interessato all'intervento umano del titolare del trattamento, in presenza di disposizioni di legge che legittimino tale trattamento e tutelino i diritti dell'individuo si potrebbe accogliere il trattamento di dati in forma automatizzata, rendendo concreta l'introduzione del meccanismo anche in materia penale e di pubblica sicurezza.

Tutti questi temi aprono scenari sconfinati e accendono dibattiti etici, giuridici e filosofici: può la libertà dell'individuo essere limitata sulla scorta del calcolo operato da un algoritmo? Quest'ultimo può essere effettivamente conosciuto e compreso da tutti? L'elaborazione di dati potrà mai sostituire il ragionamento inferenziale e indiziario dell'Autorità Giudiziaria?

Ma soprattutto: qual è il costo dell'errore e chi ne pagherà le conseguenze?

Rivolgersi a questo nuovo potente strumento potrebbe condurre ad una vera e propria implosione del sistema, se non si ricorre a dei validi strumenti di normazione e controllo: proprio come nell'evocativa favola introduttiva dell'opera di Bostrom, dove l'autore si domanda se la comunità dei passeri debba cercare un gufo (inteso quale essere superiore e più avanzato) per migliorare la propria vita e la propria gestione delle risorse, oppure se l'introduzione di un'entità difficile da ammansire e potenzialmente ingovernabile possa condurre alla distruzione del gruppo stesso.

CYBER SECURITY E CYBER CRIME

GIOVANI E MONDO DIGITALE: PEDOPORNOGRAFIA, SFRUTTAMENTO SESSUALE, CYBERBULLISMO

Il rapporto Unicef "Figli dell'era digitale" ha analizzato la condizione dell'infanzia nel mondo al 2017 ed i modi in cui la tecnologia digitale ha cambiato la vita e le opportunità dei bambini e le loro prospettive per il futuro:

"*Se utilizzata correttamente e resa universalmente accessibile, la tecnologia digitale può segnare una svolta per i tanti bambini emarginati – a causa della povertà, della discriminazione etnica, razziale e di genere, delle disabilità, e per motivi geografici (sfollamento e isolamento) – collegandoli a un mondo di opportunità e fornendo loro le competenze necessarie per avere successo nel mondo digitale.*
Ma senza un accesso garantito a tutti, la tecnologia digitale può creare nuovi divari che impediscono ai bambini di esprimere le loro potenzialità. E se non si agisce prontamente per restare al passo con i rapidissimi cambiamenti tecnologici, i pericoli del mondo virtuale possono rendere i bambini a rischio ancora più vulnerabili allo sfruttamento, all'abuso e perfino al traffico di esseri umani – nonché a una serie di fattori latenti che minacciano il loro benessere"[26].

Il 71% dei giovani nel mondo è on line e i dati provenienti da paesi ad alta connettività suggeriscono che i bambini iniziano ad usare internet in età sempre più precoce, soprattutto attraverso l'uso di mobile devices; non è raro infatti che i bambini non ancora adolescenti possiedano un cellulare tutto loro. Però la maggior parte dei bambini – e dei genitori – ha una consapevolezza molto limitata, a volte nulla, dei rischi e pericoli digitali ed i soggetti più vulnerabili possono subire gravissimi danni. La connettività digitale, infatti, ha reso i minori più avvicinabili dagli autori di reati sessuali, i trafficanti ed i bulli, i quali possono contattare un maggior numero di vittime (attraverso ad esempio l'uso di profili social non protetti o forum di giochi on line), così ampliando la loro rete di vittime ed i loro profitti, ma restando anonimi.

Uno dei fenomeni più allarmanti, anche a causa delle nuove modalità con le quali si manifesta, è sicuramente quello della **pedopornografia e dello sfruttamento sessuale dei minori**. Secondo la Internet Watch Foundation (IWF) nel 2016 ben 57.335 URL contenevano materiale pedopornografico: di questi, il 60% era ospitato su server in Europa e il 37% in Nord America. Il 92% degli URL contenenti materiali

[26] Figli dell'era digitale – La condizione dell'infanzia nel mondo 2017 - UNICEF

pedopornografici identificati dall'IWF era ospitato su server di 5 paesi: Paesi Bassi, Stati Uniti, Canada, Francia e Russia.

Dal rapporto emerge che il 53% delle vittime di abusi ha 10 anni o meno (in calo rispetto all'anno precedente), tuttavia il numero di immagini di bambini da 11 a 15 anni è aumentato. Uno dei motivi di questo incremento è rappresentato dai contenuti autoprodotti condivisi on line. Nel 2016 il rapporto NetClean, un'indagine di polizia condotta in 26 paesi, ha rivelato che il materiale esaminato raffigura principalmente bambini provenienti dall'Europa e dal Nord America, da paesi con numerosi dispositivi internet a persona e servizi internet affidabili, e paesi senza un'adeguata legislazione che vieti i reati sessuali e l'accesso nei confronti dei minori.

Una nuova sfida nell'individuazione di materiale pedopornografico è l'analisi di materiale sessualmente esplicito autoprodotto, che viene spesso accorpato al sexting consensuale ma che può includere anche materiale prodotto in seguito ad istigazione, adescamento e ritorsione sessuale. Un rapporto dell'IWF del 2015 sui "contenuti sessuali prodotti dai giovani" ha evidenziato la facilità con cui si può perdere il controllo degli stessi una volta messi on line: l'89,9% delle immagini e dei video valutati nello studio era stato "prelevato dalla postazione di caricamento originario e ridistribuito da siti web di terze parti". Lo studio ha anche evidenziato l'elevata percentuale di contenuti che mostravano bambini fino ai 13 anni[27].

Uno studio del 2018 sulla distribuzione di immagini sessuali di minori da web streaming (il c.d. fenomeno della "pedopornografia dinamica") ha evidenziato che il 98% delle immagini/video in circolazione riguarda bambini di età pari o inferiore a 13 anni, il 96% riprende minori in ambienti familiari, come il proprio letto o la propria stanza e il 100% dei contenuti analizzati sono stati ridistribuiti da terze parti diverse dal luogo di caricamento originario[28].

La distribuzione di immagini autoprodotte conduce ad ulteriori fenomeni allarmanti, soprattutto negli ultimi tempi, come il **revenge porn** e il **cyberbullismo**.

Il primo, in costante aumento anche nei confronti di vittime maggiorenni, per la maggior parte donne, ha portato paesi come l'Inghilterra ad introdurre nel 2015 il reato di divulgazione di immagini sessuali private senza consenso e, da ultimo, a pubblicare nuove linee guida per i tribunali che si occupano di questi casi, fornendo precise

[27] IWF – Emerging Patterns and Trends Report#1 On line Produced Sexual Content – 10.03.2015
[28] IWF – Trends in On line child sexual exploitation: Examining the Distribution of Captures of Live-streamed child sexual abuse – Maggio 2018.

istruzioni a garanzia di trattamenti durissimi nei confronti di coloro che diffondono materiale esplicito, che creano falsi profili per vendicarsi e umiliare le loro vittime o che ricattano con la minaccia di mettere on line foto private.[29]

In Italia, a differenza di paesi come gli Stati Uniti, Israele, Germania o Regno Unito, non esiste una legge specifica che tuteli la vittima e punisca in modo effettivo l'autore di tali reati, soprattutto perché si considera consensuale il momento della produzione del materiale (ma non la sua diffusione!), ricadendo così i fatti nelle fattispecie di diffamazione aggravata, tentata estorsione, violazione della privacy o illecito trattamento di dati. La stessa Corte di Cassazione, sulla base di tale presupposto, in un caso relativo alla diffusione di immagini intime di una minore da parte di un compagno di classe ha escluso che potesse configurarsi il reato di cui all'art. 600 ter c.p. (pornografia minorile). A settembre 2016 è stata presentata una proposta di legge[30] per l'introduzione del reato di diffusione di immagini e video sessualmente espliciti, con pene da uno a tre anni, aumentate se il fatto è commesso dal coniuge o da persona che è o è stata legata sentimentalmente alla vittima. Ma delle sorti di tale proposta ancora non è dato sapere.

Anche sul tema del **cyberbullismo** i dati sono allarmanti e le recenti ed importanti novità introdotte con la Legge 29 maggio 2017 n. 71 (come la definizione chiara del termine cyberbullismo, l'introduzione di specifiche procedure per la rimozione o oscuramento dei contenuti da parte dei gestori dei siti web o il particolare ruolo attribuito alle istituzioni scolastiche) non sono state ancora pienamente implementate.

Secondo l'ultimo rapporto di EU Kids Online 2017, pubblicato dal MIUR a gennaio 2018, il 10% dei ragazzi oggetto di studio ha dichiarato di essere stato vittima di atti di bullismo e cyberbullismo e il 19% di essere stato testimone di tali episodi (tuttavia la metà di essi ha dichiarato di non aver fatto nulla per aiutare la vittima o contrastare gli episodi). Il cyberbullismo inoltre incide maggiormente nei ragazzi di età 15-17 e 11-12 anni, i quali hanno dichiarato di sentirsi molto (27%) o abbastanza (52%) turbati da tali accadimenti.

Lo stesso rapporto Unicef 2017, inoltre, ha evidenziato le conseguenze negative degli episodi di cyberbullismo sui minori i quali, nella quasi totalità dei casi, sono portati a ricorrere all'uso di alcool e sostanze stupefacenti, a soffrire di bassa

[29] Sentencing Council – Intimidatory Offences Definitive Guideline – Ottobre 2018.
[30] Proposta di Legge d'iniziativa della deputata Sandra Savino del 27.09.2016 – Camera dei Deputati n. 4055.

autostima e ad abbandonare la scuola, fino ad arrivare al suicidio o al forte desiderio di tentarlo.

Le iniziative tra MIUR, istituti scolastici e Forze dell'Ordine sono in crescita, ma è necessario un intervento sempre più diretto dei big player della rete, con strumenti e forme di collaborazione sempre più efficaci volti a prevenire, limitare e contenere gli effetti di tutti questi comportamenti dannosi per i minori, ma non solo.

CRIMINALITA' ORGANIZZATA 4.0: NUOVI MECCANISMI DI RICICLAGGIO – VENDITA ON LINE DI DROGHE E FARMACI – TRAFFICO DI ARMI, DROGA, ESSERI UMANI – CYBERTERRORISMO E DIFFUSIONE DELL'ODIO

1. NUOVI MECCANISMI DI RICICLAGGIO: IL *CYBERLAUNDERING*

Secondo un rapporto di luglio 2018 del FATF[31] (Financial Action Task Force – un ente indipendente intergovernativo che sviluppa e promuove azioni a protezione del sistema finanziario globale contro il riciclaggio, il finanziamento del terrorismo e la proliferazione degli strumenti di distruzione di massa), esistono ormai i c.d. Professional Money Launderers (PML), ovvero professionisti nel riciclaggio, dotati di specifiche competenze ed abilità messe al servizio della criminalità organizzata. Il loro principale task consiste nel facilitare il riciclaggio di denaro sporco attraverso l'organizzazione e la fornitura di intere infrastrutture dedite alle operazioni illecite (dalla individuazione dei luoghi più favorevoli per gli investimenti e le operazioni bancarie, alla creazione di società e soggetti schermo, al reclutamento di money mules, cioè corrieri di denaro, nonché alla fornitura di servizi legali a supporto di tutte le operazioni).

I PML possono essere singoli individui, organizzazioni di professionisti o interni network composti da molteplici professionalità, tutte coinvolte nelle singole fasi delle operazioni (commercialisti, contabili, notai, avvocati, bancari, brokers, providers di trust e servici societari nonché di servizi finanziari, esperti di transazioni elettroniche e criptovalute).

Le forme classiche di riciclaggio (investimenti immobiliari e nel settore della ristorazione e delle strutture turistiche e ricettive) sono ormai quasi superate dalle

[31] FAFT Report – Professional Money Laundering – July 2018

nuove possibilità di ripulire il denaro attraverso gli strumenti che il mondo digitale offre: dalle micro transazioni effettuate attraverso i furti di identità (**smurfing**) alle imponenti operazioni attraverso la rete delle scommesse on line e le piattaforme di videogiochi multiplayer.

Già nel 2017 l'UIF nel rapporto annuale per l'anno 2016[32] ha segnalato il crescente aumento e consolidamento delle consorterie criminali nel settore del **gioco on line**, delle slot machines e delle scommesse sportive, soprattutto attraverso la gestione di piattaforme illegali, i cui server sono collocati all'estero, o attraverso l'acquisizione ed il controllo indiretto di entità legali già esistenti ed operanti sul mercato.

La sempre maggiore diffusione delle criptovalute ha aperto nuove frontiere al money laundering. Come si legge nel rapporto IOCTA 2018 dell'EC3 di Europol[33], il cyberlaundering attraverso le criptovalute è diventato sempre più raffinato e complesso e la fase di placement si caratterizza per l'inserimento nel circuito economico di capitali di provenienza illecita già disponibili su conti on-line, senza necessità di alcun contatto materiale tra il riciclatore ed il contante. Così, l'acquisto di criptovaluta sulle piattaforme di intermediazione offre la possibilità di "polverizzare" ingenti quantità di denaro nel più totale anonimato. Vi sono, inoltre, moltissimi operatori che offrono servizi di mixing in grado di disperdere le tracce di una transazione lungo la blockchain attraverso operazioni intermedie di ramificazione del flusso di criptomoneta.

La Commissione Europea ha recentemente espresso la propria preoccupazione per la nuova dimensione del fenomeno del cyber laundering; nella proposta di Direttiva per la modifica della c.d. quarta direttiva sul riciclaggio relativa "alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo", si legge come operazioni in valute virtuali beneficino di un tal grado di anonimato rispetto ai classici trasferimenti di fondi, che le organizzazioni terroristiche potrebbero facilmente abusarne per nascondere e trasferire denaro. Altri rischi potenziali riguardano l'irreversibilità delle operazioni, la gestione delle operazioni fraudolente, la natura opaca e tecnologicamente complessa di questo settore e la mancanza di garanzie regolamentari.

[32] UIF – Rapporto annuale dell'Unità di Informazione Finanziaria, maggio 2017
[33] IOCTA – Internet Organised Crime Threat Assessment 2018 – Europol EC3

Il dato più allarmante riguarda la totale assenza di regole o discipline generali, lacuna che andrà quanto prima colmata, soprattutto a livello europeo e internazionale.[34] In Italia il D. Lgs 90 del 2017 ha esteso le fattispecie di abusivismo finanziario già previste dal TUB e dal TUF anche alle attività di prestatori di servizi relativi a valute virtuali (trading, mining e mixing), tuttavia si tratta di ipotesi illecite di tipo amministrativistico e non di sanzioni penali. Una visione più armonica e unitaria dal fenomeno consentirà sicuramente un presidio più efficace per la prevenzione ed il contrato dei crescenti fenomeni illeciti correlati.

2. ON LINE DRUGS SALE

Il commercio on line di droghe (intese sia quali sostanze stupefacenti che farmaci) è in costante incremento, nonostante le continue azioni di Forze di Polizia internazionali (Europol, Interpol, FBI, DEA etc) cerchino di contrastare il fenomeno, agendo sui market places presenti nel dark web. Secondo recenti studi dello European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) ed Europol, i principali paesi europei che costituiscono base di darknet per la fornitura di sostanze (in termini di guadagno e di volume d'affari) sono la Germania, i Paesi Bassi e il Regno Unito[35] e che i venditori di sostanze come la cannabis e la cocaina sono concentrati soprattutto in paesi con alto numero di consumatori. I dati confermato poi che la maggior parte del volume di affari e di transazioni riguarda piccole quantità destinate soprattutto ai singoli consumatori. Nel corso del 2017 le Forze di Polizia hanno smantellato due dei più grandi mercati di sostanze illecite ovvero AlphaBay e Hansa, i quali insieme al Russian Anonymous Marketplace (RAMP), gestivano l'87% di tutte le attività di marketplace sul darkweb. In particolare, AlphaBay ospitava 40.000 venditori e 200.000 utenti, con più di 250.000 annunci relativi a sostanze stupefacenti, psicotrope e sostanze chimiche tossiche e con un volume d'affari stimato di 1 bilione di dollari dalla sua apertura nel 2014. RUMP era il secondo market place per grandezza ma nel giugno 2017 è stato smantellato dalle autorità russe.

Inoltre, secondo l'ultimo rapporto dell'UNODC (United Nation Office on Drugs and Crime) il valore dell'on line drugs sale dal 2011 al 2015 è stato pari a 44 milioni di dollari all'anno e nella prima parte del 2016 le vendite si sono attestate tra i 14 ed i 25 milioni al mese, che corrispondono a circa 170-300 milioni di dollari l'anno[36].

[34] L. D'Agostino - Operazioni di emissione, cambio e trasferimento di criptovaluta: considerazioni sui profili di esercizio (abusivo) di attività finanziaria a seguito del D.Lgs. 90/2017, rivista di Diritto Bancario, Gennaio 2018.
[35] Cfr. IOCTA 208 cit.
[36] UNODC – World Drug Report 2018 - Executive Summary, Conclusions and Policy Implications.

In Italia la vendita di farmaci on line è stata regolamentata dall'articolo 112-quater del decreto legislativo n. 219 del 24 aprile 2006 e dalle circolari emanate dal ministero della Salute a gennaio e maggio del 2016. Nelle norme è specificata innanzitutto la tipologia di medicinali ammessi alla vendita online: è possibile l'e-commerce per i farmaci senza obbligo di prescrizione (Sop) e i farmaci da banco (Otc), presenti in un apposito elenco disponibile sul sito dell'AIFA. È vietata invece la vendita sul web dei farmaci che necessitano di ricetta medica, per i quali è possibile l'acquisto solo in farmacie fisiche. Secondo l'elenco del ministero della Salute, nel nostro Paese si contano 518 farmacie e 94 esercizi commerciali autorizzati a vendere farmaci online, con un fatturato annuo di circa 150 milioni di Euro[37]. Tuttavia, nel 2016 sono state bloccate oltre 20.000 farmacie sul web perché illegali e 6.000 quelle chiuse nei primi mesi del 2017.

L'accesso sempre più facile al mondo digitale da parte dei giovani e degli anziani aumenta in maniera esponenziale il rischio di tali condotte, ecco perché le Forze di Polizia che già operano sul campo necessitano di maggiori strumenti di cooperazione e, soprattutto, di un law enforcement unitario e sovranazionale che riesca a contrastare in maniera efficace il fenomeno.

3. TRAFFICO DI ARMI, DROGA ED ESSERI UMANI

La criminalità organizzata è un fenomeno in continuo cambiamento ed è sottoposto allo studio costante di organismi ed enti sia nazionali che sovranazionali che cooperano tra loro per rafforzare l'azione di contrasto; tra questi sicuramente l'UNODC (United Nation Office on Drugs and Crime), l'Interpol, l'Europol, unitamente alle Forze di Polizia nazionali. La globalizzazione e la facilitazione degli scambi informativi e dei flussi finanziari, agevolati ancor di più dalla tecnologia digitale, offrono ulteriori strumenti di azione alle grandi organizzazioni criminali di tutto il mondo che – per necessità – non si identificano più con un singolo stato o una singola regione ma richiedono interventi da parte di soggetti sovranazionali.

Secondo Europol sono circa 5.000 le grandi organizzazioni criminali oggetto di indagine, con il coinvolgimento di 180 stati diversi. Il 60% dei soggetti sospettati di far parte di una organizzazione criminale è di paesi europei. La principale attività – con il maggior guadagno – è il traffico di droga, seguono il traffico di migranti, i reati contro

[37] About Pharma n. 154 – Health Publishing and Services – Gennaio 2018.

la proprietà, le frodi sui dazi e le importazioni, il traffico di esseri umani. Il 45% delle organizzazioni valutate nel 2017 è coinvolto in più di una attività criminale, con costante incremento delle attività di contrabbando soprattutto dei migranti. Il 70% agisce in più di tre stati, mentre il 10% gestisce attività che coinvolgono più di 7 paesi. L'espansione dei black market in rete e la possibilità di utilizzare i vantaggi derivanti dalle criptomonete e dalle blockchain sta facendo sì che il traffico illecito on line non costituisca più un diverso modus operandi ma un vero e proprio nuovo mercato, dinamico ed in continua espansione, che sta gradualmente soppiantando quello fisico tradizionale[38].

4. CYBERTERRORISMO E DIFFUSIONE DELL'ODIO

Secondo il rapporto Europol IOCTA 2018, la perdita di territori da parte dell'IS nel 2016-2017 non è coincisa con una perdita di autorità tra i seguaci né ha condotto ad un decremento degli attacchi. Al contrario, il gruppo ha continuato e continua tuttora ad utilizzare internet per promuovere la sua dottrina ed ispirare azioni terroristiche.
Dal 2016 i simpatizzanti dell'IS hanno spostato le loro comunicazioni dai social media (Facebook e Twitter) ai canali criptati di comunicazione offerti da piattaforme come Telegram, Threema e Signal, i quali offrono la possibilità di creare chat chiuse o a tempo. Inoltre, la loro evoluzione tecnologica si è adeguata perfettamente alle opportunità offerte dal dark web e dalle criptomonete, divenute il principale strumento di finanziamento delle loro azioni.

Le azioni di cyberterrorismo non si esauriscono con la diffusione dello jihadismo o di altre forme di fondamentalismo islamico ma contengono al loro interno tutti i tipi di attacchi su larga scala per finalità economiche, di cyber spionaggio (tra privati, imprese o perfino Stati) o anche per finalità politiche e geopolitiche (cyber warfare). Secondo la definizione data dall'FBI il cyber terrorismo è "any "*premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents."* Tuttavia, molti ritengono troppo ristretta tale definizione, poiché non include anche azioni che non possano considerarsi "violente" nel senso comune del termine ma che comunque arrechino un danno significativo (anche non fisico, come ad es. la perdita di vite umane). Secondo la NATO invece il cyber terrorismo è "*a cyberattack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an*

[38] Fonte Europol – Defining serious and organised crime

ideological goal". Ad ogni modo, è certo che il cyber terrorismo è solo una componente del più grande concetto di cyber warfare.

Le preoccupazioni per il sempre maggiore impatto che azioni di **cyberwar** e **cyber warfare** possono avere, hanno portato ad una maggiore attenzione ed analisi del fenomeno. Atteso che il concetto di cyber warfare è considerato in continua evoluzione, in genere si analizzano e si suddividono gli attacchi mirati a sottrarre/esfiltrare informazioni da quelli che invece sono finalizzati alla distruzione/corruzione/interruzione dei dati, dove gli autori sono di tipo governativo (Stati o enti statali e soggetti sponsorizzati o che hanno alle spalle Stati) i quali agiscono per finalità di spionaggio ovvero per compiere vere e proprie azioni di cyber warfare[39].

In ogni caso, le azioni fin qui richiamate possono anche non riguardare stati o coinvolgere soggetti istituzionali o pubblici (es. infrastrutture critiche, ospedali, ecc.), ma consumarsi nell'ambito di confini più ristretti, nei confronti di soggetti privati i quali vengono attaccati per ragioni politiche o ideologiche. Ciò non toglie comunque che vi sia una finalità terroristica – nella accezione ampia utilizzata dalla NATO – qualora l'attacco abbia ad oggetto una grossa multinazionale, ovvero ancora una piccola azienda, o anche il singolo soggetto, ed il danno conseguente sia solo di tipo economico.

Accanto al proselitismo ed al cyber terrorismo, il web favorisce la diffusione dei c.d. **reati d'odio**, ovvero per come definiti nella Decisione Quadro dell'Unione Europea 2008/913/JHA del 28.11.2018, "*all conduct publicly inciting to violence or hatred directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin*". La Commissione Europea è intervenuta in maniera specifica sull'argomento adottando nel giugno 2016 un Codice di Condotta[40] che è stato siglato inizialmente da Facebook, Twitter, YouTube e Microsoft (da ultimo si sono aggiunti anche Google+ e Instagram), tuttavia c'è ancora molto da fare. Il terzo monitoraggio effettuato dalla Commisione a gennaio 2018 ha evidenziato che, fin dalla adozione nel 2016 "in media, le società informatiche hanno rimosso il 70% di tutti i messaggi illegali di incitamento all'odio loro notificati dalle ONG e dagli enti pubblici che hanno partecipato alla valutazione. La percentuale è aumentata costantemente dal 28% nel primo ciclo di controlli nel 2016 e dal 59% nel secondo ciclo del maggio 2017"; inoltre "*oggi, tutti le imprese informatiche partecipanti*

[39] RAND – Estimating the global cost of cyber risk – Gennaio 2018
[40] https://ec.europa.eu/info/files/code-conduct-countering-illegal-hate-speech-online_en

soddisfano pienamente l'obiettivo di verificare la maggior parte delle notifiche entro 24 ore, con una media di oltre l'81%.Questa percentuale è raddoppiata rispetto al primo ciclo di controlli ed è aumentata rispetto al 51% delle notifiche verificate entro 24 ore registrato nel precedente ciclo di controlli". Servono però ulteriori miglioramenti e implementazioni e, in particolare: "il feedback agli utenti è ancora insufficiente per quasi un terzo delle notifiche in media, con diversi tassi di risposta da parte delle varie aziende informatiche. La trasparenza e il feedback agli utenti sono ambiti in cui occorre prevedere ulteriori miglioramenti" e "il codice di condotta integra la legislazione contro il razzismo e la xenofobia, che prevede un efficace perseguimento degli autori dei reati di incitamento all'odio, sia online che offline. In media, un caso su cinque notificato alle aziende informatiche è stato anche segnalato dalle ONG alla polizia o alla giustizia". Serve pertanto maggiore collaborazione e scambio tra i vari soggetti coinvolti e uno scambio specifico tra stati e aziende informatiche[41].

[41] https://ec.europa.eu/italy/news/20180119_UE_contrasta_incitamento_odio_on_line_it