LUISS

Dipartimento di Scienze Politiche
Cattedra: Sociologia della Comunicazione

Cyber security in Europa e la cooperazione tra settori pubblico e privato

RELATORE
Prof. Michele Sorice

CANDIDATO
Francesca Uricchio Matr. 086322

Anno Accademico 2019/2020

Indice

“CYBER SECURITY IN EUROPA E LA COOPERAZIONE TRA SETTORI PUBBLICO E PRIVATO”

Introduzione……pag.2

Capitolo 1: “ll quadro giuridico europeo sulla cyber security”:

1.1. Perché è importante a livello europeo il fenomeno……..pag.3
1.2. Direttiva NIS (2016) …… ……...pag.4
1.3. ENISA……...pag.5
1.4. Contenuto illegale sulle piattaforme online, comunicazione della Commissione europea…..... .pag.7
1.5. Fenomeno delle Fake News……..... pag.8
1.6. Normativa Italiana……..... pag.12

Capitolo 2: “Il caso studio di Facebook:

2.1. Regole dell’uso di Facebook e meccanismi di controllo…….....pag.15
2.2. Statistiche, video, uffici…….....pag.17
2.3. Critiche a Facebook→ …….....pag.17
2.4. Estremismo in Europa…….....pag. 19
2.5. Impatto Psicologico sugli operatori……pag.21

Capitolo 3: “Coronavirus: la nuova sfida digitale”

3.1. Coronavirus: perché non è solo un problema sanitario……...pag.23
3.2. App per il tracciamento del contagio: IMMUNI in Italia, pro e contro……..pag.28

Conclusioni…….....pag.33
Sitografia…….....pag.34
Abstract…….....pag. 37
Ringraziamenti…….....pag.43

Introduzione

Il presente elaborato intende chiarire le caratteristiche, le funzioni ed i meccanismi della cyber security, ovvero il campo della sicurezza informatica e di tutti i dispositivi volti alla protezione delle piattaforme online dagli attacchi informatici. In particolare, verranno analizzati gli interventi, le direttive ed i regolamenti dell'Unione Europea e dell'Italia, considerando Facebook come caso studio, e verranno elencati tutti i possibili rischi a cui vanno incontro gli individui, dalla condivisione di contenuti illegali alla diffusione delle fake news.

L'obiettivo di questo lavoro è in primo luogo quello di spiegare l'importanza di questa disciplina, che in un mondo sempre più digitalizzato, si è dimostrata fondamentale per la protezione degli utenti, dei cittadini e degli stessi paesi.

Ciò che mi ha spinto a decidere di parlare di questo argomento è stata la consapevolezza di quanto sia necessario che le persone conoscano la materia, che ci sia una buona informazione e che i governi tutelino i diritti fondamentali degli individui anche nell'utilizzo delle piattaforme online e dei social network, dal diritto alla privacy alla libertà di espressione e di opinione.

Nei primi due capitoli verranno trattate specificamente: la direttiva europea NIS (acronimo di Network and Information Security) del 2016 che impone a tutti gli Stati Membri dell'Unione Europea l'adozione di misure comuni per contrastare gli attacchi alle reti informatiche e per proteggere le piattaforme online, ed il ruolo dell'ENISA (acronimo di European Network and Information Security Agency), ovvero l'Agenzia europea creata per rendere maggiormente sicure le reti di telecomunicazione dei paesi europei.

Successivamente, per rendere più chiaro il mio studio ho deciso di portare il caso di Facebook, relativamente al suo funzionamento e alla protezione dei dati degli utenti. Essa è una piattaforma utilizzata in tutto il mondo che rende più facile l'interazione tra gli individui, ma che può costituire un pericolo se usata in maniera sbagliata e senza determinati limiti.

Per concludere, ho dedicato il terzo capitolo al tema del Covid-19, un virus partito dalla Cina che ha avuto enormi conseguenze sul sistema sanitario mondiale, sull'economia e sulla vita sociale di tutti noi, e che inoltre ha sottolineato l'esigenza di rafforzare la sicurezza online. Infatti, in questi mesi la tecnologia si è rilevata fondamentale e nel nostro paese si è parlato di un'applicazione chiamata "Immuni", creata per il tracciamento dei contagi e per facilitare il controllo del rispetto del distanziamento sociale, ma allo stesso tempo ha creato ancor di più la necessità di tutelare il diritto alla privacy e di rafforzare il sistema di sicurezza informatico.

Capitolo 1. Il quadro giuridico europeo sulla cyber security

1.1.Perché è importante a livello europeo?

Con il termine cyber security intendiamo la difesa di tutti i dispositivi elettronici, dei server, dei networks, dei siti online e dei dati di qualsiasi tipo.

Essa è un tema sempre più importante nell'ambito politico-economico, questo perché viviamo in una società fortemente influenzata e dipendente dalle nuove tecnologie. Nonostante esse ci portino vantaggi non trascurabili, come una comunicazione maggiormente facilitata tra i vari paesi, uno scambio illimitato di informazioni ed una maggior interconnessione, i rischi di attacchi informatici rendono invece difficile la vita dei paesi, ma non solo. Basti pensare alle banche, alle grandi e piccole aziende o agli ospedali. Per questo motivo, oggi la protezione dei dati e dell'informazione è diventato uno dei principali obiettivi dell'Unione Europea per garantire il corretto funzionamento dell'economia online. Secondo le ultime statistiche nel 2019 vi sono stati oltre 4.000 attacchi di ransonware (con questo termine intendiamo un tipo di malware che limita l'accesso a un dispositivo o ad un sito chiedendo all'utente un riscatto in denaro) al giorno e l'80% delle aziende europee ha dovuto fare i conti con incidenti di sicurezza informatica[1]. È nata quindi l'esigenza da parte dell'Unione Europea di creare una collaborazione tra gli Stati membri e di coordinare il settore privato con le istituzioni europee. Nella nostra società inoltre, è aumentato il fenomeno della disinformazione e delle cosiddette fake news, che contribuiscono al malfunzionamento delle democrazie moderne e ad esempio alla diffusione della paura per quanto riguarda il terrorismo, inoltre sono aumentati i pericoli sulle piattaforme online, infatti è sempre più facile rubare dati (come ad esempio i dati personali sui social network), accedere ad informazioni segrete di ogni governo arrivando in conclusione a destabilizzarlo.

Negli ultimi anni abbiamo assistito alla comparsa di un nuovo concetto, quello delle "minacce ibride". Precedentemente la parola "ibride" era affiancata a quella di "guerre" in ambito militare, per indicare conflitti caratterizzati da misure non convenzionali. Possiamo citare il libro "Guerra senza restrizioni" nel quale si parla di "minacce ibride" per indicare conflitti armati in cui configurano elementi esterni al mondo militare[2]. Successivamente anche la NATO ha cercato di trovare una definizione: infatti, con questo concetto intende l'utilizzo di mezzi di ogni tipo, come mezzi di propaganda e cyber attacchi, volti a destabilizzare la società e i governi del paese interessato, intaccando i valori di libertà ed i diritti democratici. Ad oggi quindi il termine "minaccia ibrida" lo ricolleghiamo a qualcosa di più vicino a noi, nessun paese lo vede come un qualcosa di lontano o utopistico, ma è un rischio che corriamo tutti, dalle singole persone ai singoli governi. Nasce l'esigenza di tutelarsi, di sentirsi protetti e di contribuire alla difesa di ogni tipologia di dato. Per fare un esempio più vicino a noi cittadini, pubblicando una fotografia o un'informazione personale sui social network

[1] Cyber security Technology & Capacity Building. (2020) *Cyber Security*. Disponibile in: https://ec.europa.eu/digital-single-market/en/cyber-security

[2] Liang, Q., Xiangsui, W. (1999). *Unrestricted Warfare*. Pechino. PLA Lettere ed Arti Casa Editrice

vogliamo essere sicuri che queste rimarranno circoscritte a noi ed esclusivamente alle persone con cui decidiamo di condividerle.

Tuttavia, essendo un problema globale, non può essere risolto indipendentemente da tutto ciò che succede negli altri paesi, e per questa ragione l'Unione Europea ha deciso di introdurre questo argomento nella sua agenda.

È importante a tal proposito citare la comunicazione congiunta al Parlamento europeo e al Consiglio europeo del 6 aprile 2016[3], dove vengono elencate le principali azioni per contrastare tali minacce. L'azione primaria che ogni Stato membro è tenuto ad eseguire è quella di coordinarsi con la Commissione e con l'Alto rappresentante per individuare il pericolo. Per facilitare questo scambio di informazioni è nata una cellula UE presso il centro di analisi dell'intelligence (EU INTCEN) del Servizio europeo per l'azione esterna (SEAE). Essa studia le minacce ibride dei vari paesi interessati e inizializza quello che dovrebbe essere il processo strategico di repressione. Tra queste minacce ibride, come detto in precedenza, rientrano tutti gli attacchi informatici. È quindi necessario citare anche l'azione contro di essi, in particolare è giusto citare la direttiva sulla sicurezza delle reti e dell'informazione (SRI), riguardanti tutti i settori sensibili a questo argomento, dall'ambito sanitario a quello energetico come detto in precedenza.

1.2. Direttiva NIS (2016)

La direttiva NIS, adottata il 6 luglio 2016, ha rappresentato le prime norme dell'Unione Europea in ambito di sicurezza informatica[4]. L'obiettivo primario di essa è quello di garantire maggior cooperazione a livello nazionale ed europeo per reagire in maniera congiunta agli attacchi informatici. Essa si propone due compiti:

1) La creazione di un quadro comune di certificazione della sicurezza informatica di prodotti ICT e servizi digitali. Esso garantirà a livello europeo uno schema completo di regole, procedure e requisiti. Ogni sistema europeo dovrebbe certificare: le categorie dei prodotti e dei servizi, il tipo di valutazione ed il livello di garanzia. Bisogna però sottolineare che esso non istituisce schemi direttamente operativi. Infatti, essi saranno prima programmati dall'ENISA e poi adottati dalla Commissione europea con atti esecutivi. Questo vuol dire che solo successivamente le aziende interessate faranno domanda di certificazione per i propri prodotti e servizi, perciò l'uso della certificazione è e rimane volontario.

[3] Comunicazione congiunta al Parlamento Europeo e al Consiglio. (2016) *Quadro congiunto per contrastare le minacce ibride: La risposta dell'Unione Europea.* Bruxelles. Disponibile in: *https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52016JC0018&from=en*

[4] The Directive on security of network and information systems (NIS Directive) adopted by the European Parliament. (2016). Disponibile in: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

2) Rafforzare il ruolo ed il mandato dell'ENISA: l'Agenzia europea per la sicurezza delle reti e dell'informazione (di cui parleremo nel paragrafo successivo).

Il 13 settembre 2017 la Commissione europea ha adottato un pacchetto sulla sicurezza informatica[5], nel quale la principale misura consiste in un regolamento (per tale motivo direttamente applicabile a tutti gli Stati membri) pubblicato nella Gazzetta Ufficiale il 7 giugno del 2019, il cosiddetto Cyber Security Act che consiste in un quadro complessivo di regole che disciplinano gli schemi europei di certificazione e con il quale l'Unione Europea si impegna ad introdurre:

- Una strategia comune per rafforzare la sicurezza online
- Un mercato unico digitale, reso possibile dal quadro comune di certificazione online.
- Un centro europeo di ricerca e competenza in tale ambito, il quale aiuterà a coordinare il lavoro della rete e istituirà la Comunità europea in materia di cyber sicurezza. Inoltre, contribuirà a garantire supporto tecnico e finanziario alle start-up della sicurezza, sosterrà la ricerca e l'innovazione. L'organo decisionale di tale centro è il Consiglio di amministrazione, composto da tutti gli stati membri, tra essi solo chi contribuisce finanziariamente ha diritto di voto. Il Consiglio è appoggiato ed aiutato da un Comitato consultivo industriale e scientifico, il quale dialogherà con il settore privato e le organizzazioni dei consumatori.
- Un modello di reazione agli attacchi online, così da minimizzare i rischi
- Maggior solidarietà tra i paesi, che non esclude in futuro la possibilità di creare un Fondo europeo per la difesa informatica.
- Cooperazione a livello internazionale
- Applicazione del diritto penale, applicando sanzioni pecuniarie e penali a coloro che commettono azioni sbagliate e dannose, così da creare anche un disincentivo nell'adottare tali comportamenti.

1.3. ENISA

Il secondo compito della direttiva NIS è quello di rafforzare il ruolo ed il mandato dell'ENISA[6]. L'Agenzia europea per la sicurezza delle reti e dell'informazioni fu istituita nel 2004 con mandato temporalmente limitato. Inizialmente aveva semplicemente un ruolo di consulenza tecnica, infatti assisteva gli stati e le istituzioni europee nella scelta e nell'elaborazione di politiche nel campo della sicurezza, ma le decisioni, la gestione e la risoluzione di attacchi informatici rimaneva competenza esclusiva degli stati membri.

[5] *Cyber security act*, adopted by the European Commission. (2017) Disponibile in: https://ec.europa.eu/digital-single-market/en/news/cybersecurity-commission-scales-its-response-cyber-attacks

[6] Agenzia Europea per la sicurezza delle reti e dell'informazioni. (2004) Disponibile in: https://www.agendadigitale.eu/sicurezza/cybersecurity-act-ecco-cosa-ci-aspetta-dopo-la-direttiva-nis/

Nel 2016 invece tale agenzia riceve un mandato permanente e cambia quindi anche il ruolo che essa è tenuta a svolgere. Infatti, diventano di sua competenza anche le attività di supporto alla gestione di incidenti informatici.

Inoltre, essa si impegna ad attuare il quadro di certificazione europeo proposto dalla Commissione, aiutata dalla rete nazionale di squadre di risposta agli incidenti informatici (CSIRT). Quest'ultima si comporta come un "sito" dove i membri possono collaborare, scambiarsi opinioni, raccontare le proprie esperienze. Si discute e si decide quale sia la risposta più efficace ad eventuali problemi.

Le attività dell'Agenzia sono regolate dal programma annuale di lavoro, essa si impegna ad aiutare sia il settore privato che il settore pubblico. Infatti, delle sue azioni ne risultano avvantaggiati sia le istituzioni europee ed i governi, che le imprese, il mondo universitario e gli stessi cittadini. Si impegna a prevenire attacchi informatici, a creare una risposta collettiva e coordinata aiutando i governi degli stati membri, migliorando la cooperazione tra gli stessi.

1.4. Contenuto illegale sulle piattaforme online, comunicazione della Commissione europea

Bisogna ora soffermarsi sull'importanza di un utilizzo corretto delle piattaforme online. Potendo essere utilizzate da chiunque è necessario porre delle regole, in modo tale da poter tutelare la singola persona, l'ordine pubblico ed i governi. Bisogna porre dei limiti alle persone, non può essere considerato lecito tutto ciò che viene pubblicato. Basti pensare all'utilizzo dei social network, dove le persone si sentono autorizzate a condividere qualsiasi contenuto, sia esso un video violento, materiale pedopornografico o contenuti che possono essere ricollegati a ciò che chiamiamo cyber bullismo. Fino al 2017 non vi erano controlli, e questo faceva si che le piattaforme online fossero colme di contenuti illegali, infatti era in vigore la Direttiva UE n.31 dell'8 giugno 2000, che di fatto sottolineava l'assenza di un obbligo di sorveglianza in capo agli ISP (Internet service provider, ovvero i fornitori di servizi internet) nei confronti dei contenuti e dei materiali pubblicati sulle piattaforme da terzi[7]. Di questa direttiva è importante citare l'art 15: "*Gli stati non impongono ai prestatori un obbligo generale di informazione di sorveglianza sulle informazioni che trasmettono o memorizzano né un obbligo generale di recare attivamente fatti o circostanze che indichino la presenza di attività illecite. Gli stati membri possono stabilire che i prestatori di servizi della società dell'informazione siano tenuti ad informare senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi o a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati"*. Vigeva quindi il cosiddetto principio di neutralità, secondo cui i prestatori di servizi online non erano obbligati a controllare e sorvegliare i contenuti sulle proprie piattaforme.

[7] Direttiva (UE), 2000/31 del Parlamento europeo e del Consiglio. Disponibile in: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32000L0031&from=EN

Prendendo sempre di più coscienza di quanto pericoloso sia tutto ciò, venne successivamente concordata la comunicazione della Commissione europea del settembre 2017, dove viene incentivato il controllo. Infatti, è opportuno sottolineare che in tutte le piattaforme è necessario che ci sia la libertà di espressione e di opinione, ma bisogna anche tutelare gli altri diritti umani, e bisogna rendere illegali tutti i comportamenti online che sarebbero illegali anche al di fuori del web e quindi nella vita reale.

La svolta in questo particolare scenario avvenne il 1° marzo 2018 con una raccomandazione della Commissione Europea, volta ad incentivare la sorveglianza da parte dei providers, che non sono più liberi nelle loro decisioni ma sono responsabili socialmente di ciò che viene o non viene pubblicato da terzi[8]. Con questa raccomandazione infatti, vengono attuate misure aggiuntive che prevedono procedure di segnalazione e azione nei confronti di tutti i comportamenti ritenuti illeciti. Con essa si vuole tradurre l'impegno politico della comunicazione sopra citata, che aveva una forma giuridica non vincolante. Essa prevede un uso più responsabile di tutte le piattaforme, con una supervisione umana di un gruppo di esperti che si occupa ogni giorno di controllare, segnalare ed eliminare tutto quello che non è consentito, per garantire il pieno riconoscimento dei diritti umani e delle libertà di espressione. L'Unione Europea vuole quindi creare un approccio comune, per far si che tutti gli Stati membri abbiano lo stesso metodo di supervisione, così da rendere più efficiente l'intervento e la prevenzione.

In questo ambito non parliamo solo di comportamenti riconducibili, per esempio, alla violenza o alla pedopornografica come detto in precedenza, ma parliamo anche del materiale di incitamento al razzismo, della protezione della privacy e dei dati personali, della lotta alle truffe online, alla frode e alla cosiddetta diffamazione.

1.5. Il fenomeno delle fake news

Ricollegandoci a quanto detto nel capitolo precedente, ciò che quest'ultima raccomandazione ha come obiettivo è quello di rafforzare il controllo online anche nella lotta alla disinformazione. Sempre più numerose sono quelle che comunemente vengono chiamate fake news. Capita ogni giorno, per esempio su Facebook, di imbatterci in articoli con titoli che citano un determinato fatto, dove però all'interno niente è a questo riconducibile, ma molte persone si limitano alla lettura del titolo così da rimanere fuorviati da esso. Un altro esempio può essere quello del terrorismo psicologico online, infatti in molte occasioni i social network sono utilizzati come canale di diffusione del terrore, basti pensare a quando ogni articolo citava informazioni sbagliate riguardanti gli attacchi terroristici, oppure le fake news riguardanti malattie. Quello che si innesca nelle persone che lo leggono è un sentimento di paura che viene sfruttato da tutti coloro che pubblicano questi contenuti per pubblicarne di altri. Esistono anche articoli o addirittura e-mail che vengono utilizzati per

[8] Raccomandazione (UE), 2018/334 della Commissione Europea sulle misure per contrastare efficacemente i contenuti illegali online. Disponibile in: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32018H0334&from=FR

commettere truffe online, per esempio può capitare di ricevere nella posta elettronica messaggi che inducono, con scuse credibili, le persone ad inserire le credenziali della propria carta di credito o del proprio telefono, così da poter rubare denaro e dati. Questo è un fenomeno in continua diffusione e che necessita di un limite per poter appunto proteggere sia le persone che i governi dei vari paesi.

A proposito di ciò l'Unione Europea si è impegnata a delineare il Codice di condotta sulla disinformazione[9], ovvero il primo insieme di norme che trattano di questo argomento, al fine di autoregolamentare, attraverso una firma volontaria, l'utilizzo delle piattaforme online e dei social network più rilevanti tra tutti gli Stati membri. Tutti coloro che hanno firmato tale codice, avevano l'intenzione di regolare ed agire in cinque aree specifiche:

1) Interruzione delle entrate pubblicitarie di determinati account e siti Web che diffondono disinformazione
2) Rendere più trasparenti la pubblicità, anche quella politica
3) Agire ed eliminare gli account falsi
4) Consentire a chi utilizza tali piattaforme, di denunciare e segnalare la disinformazione, migliorando i contenuti e accedendo a più fonti di notizie
5) Rendere possibile alla comunità di ricerca di controllare il fenomeno della disinformazione attraverso l'accesso consentito alla privacy e ai dati delle piattaforme.

L'obiettivo è quindi quello di rendere trasparente l'utilizzo dei siti Web, ma anche le pubblicità, per proteggere il consumatore e incentivare un comportamento sano e conforme alle regole. Nonostante questi interventi, seppur importanti, ai giorni d'oggi è sempre più difficile controllare il comportamento di tutti gli utenti delle piattaforme. Basti pensare all'utilizzo di Instagram, dove molte persone utilizzano profili falsi per commentare contenuti di altre persone, per minacciare o per truffare persone più deboli e meno attente, come per esempio gli anziani.

Tra firmatari del Codice di condotta abbiamo: Facebook, Twitter e Google, ai quali nel 2019 la Commissione europea ha richiesto di riferirle ogni mese le loro azioni, questo per migliorarne la coordinazione, assicurare la trasparenza della pubblicità politica e non, e per garantire la lotta contro i profili falsi.

Ciò che spinge i firmatari a partecipare è il fatto che si voglia raggiungere, all'interno dei propri siti e canali, la credibilità delle notizie. In un mondo dove si leggono in continuazioni notizie false, il lettore è spinto ad utilizzare i social network e i motori di ricerca più sicuri, per avere la certezza di ciò che leggono e per avere la sicurezza di ciò che intendono pubblicare. Questi siti online, aderendo al progetto della Commissione europea, si autotutelano e tutelano l'integrità dell'Unione Europea, perciò è qualcosa che va a giovare ad

[9] Dipartimento per le politiche europee. (2018) *Disinformazione online, codice di condotta per le piattaforme digitali*. Disponibile in: http://www.politicheeuropee.gov.it/it/comunicazione/notizie/disinformazione-online-codice-di-condotta-per-le-piattaforme-digitali/

entrambe le parti. Quest'ultima in particolare, ha tra i suoi obiettivi primari la sicurezza, e questa deve essere traslata necessariamente anche al mondo del web. Per fare ciò però, ci deve essere un rapporto diretto con i cittadini, ovvero con coloro che utilizzano i siti e usufruiscono dei social network. Sono state consultate quindi le persone comuni per avere un riscontro riguardo le fake news, integrando anche un sondaggio, con l'utilizzo dell'Eurobarometro, ovvero uno strumento per misurare la percezione ed i sentimenti dell'opinione pubblica riguardo questo argomento. A ciò si aggiungono un colloquio volto a coordinare l'azione e la repressione di tali notizie ed infine un gruppo ad alto livello (HLG), ovvero un gruppo di esperti che fornisce consulenza nel campo.

È importante tenere informati i cittadini, fargli capire quali siano i pericoli di un utilizzo sbagliato di Internet, così come è fondamentale coordinare a livello europeo e mondiale l'intervento di coloro che si occupano di eliminare tali contenuti. È necessario che tutti coloro che utilizzano le piattaforme sappiano come si utilizzano, sappiano come interagire con le altre persone e sappiano soprattutto quali sono gli articoli attendibili e quali no, quali siano i siti sicuri e quali no e quali siano i contenuti certi e quali no. C'è bisogno della cosiddetta "alfabetizzazione mediatica", che in un mondo sempre più interconnesso è fondamentale, che deve riguardare diversi media come la radio o la stampa, e diversi canali, come appunto Internet ed i social media, ma soprattutto essa deve riguardare tutte le fasce d'età della popolazione, per far si che possano essere protetti gli interessi di tutti, dai bambini agli anziani, che sono le due categorie più a rischio. Viene istituito un gruppo di esperti che si riunisce ogni anno per discuterne, per facilitare la cooperazione e sostenere le azioni dell'UE.

A tal proposito la Commissione europea ha introdotto una nuova iniziativa, la settimana europea dell'alfabetizzazione, questo ci fa capire quanto importante sia, e che sia un requisito importante per le democrazie e per gli stati membri

A conclusione di questo argomento bisogna riconoscere che gli interventi per limitare la diffusione di notizie false sono stati tanti e rilevanti, ma bisogna fare affidamento anche alle sanzioni per tutti coloro che le diffondono e alla coscienza di ognuno di noi.

L'articolo 19 della Dichiarazione universale dei diritti dell'uomo stabilisce che: *"Ogni individuo ha diritto alla libertà di opinione e di espressione; questo diritto include la libertà di esprimere opinioni senza interferenze e di cercare, ricevere e impartire informazioni e idee attraverso qualsiasi mezzo di comunicazione e indipendentemente dalle frontiere"*. A questo fa riferimento l'UNESCO, che a tal fine promuove e sostiene l'alfabetizzazione mediatica e dell'informazione (MIL)[10], nata dalla collaborazione tra il settore della comunicazione e dell'informazione dell'UNESCO con il settore dell'istruzione e l'Ufficio internazionale dell'istruzione. Essa a sua volta promuove il diritto dell'individuo di esprimere e comunicare liberamente le

[10]Unesco, *Media and information literacy curriculum fot teachers.* Disponibile in: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/media_and_information_literacy_curriculum_for_teachers_en.pdf

proprie idee ed i propri pensieri e ciò deve essere accompagnato da una piena ed esaustiva conoscenza dei media e di tutte le piattaforme digitali che diffondono informazioni.

Il MIL riconosce la vitale importanza dei mezzi di comunicazione e di informazioni per i cittadini nelle società democratiche, e proprio per questo essi devono garantire i diritti fondamentali dell'uomo, quali la libertà di espressione e di opinione, in quanto servono anche a improntare, diffondere ed esporre credenze ed atteggiamenti. I cittadini a loro volta devono saper utilizzare tali mezzi e devono poter conoscere tutti gli aspetti di essi, le funzioni e le finalità. È importante quindi che anche gli insegnanti e gli educatori dei diversi settori sappiano come utilizzarli, in un mondo sempre più digitalizzato anche per quanto riguarda il lavoro, come la professione del giornalismo.

Possiamo capire il forte interesse per tale questione, citando una parte della Costituzione dell'UNESCO che esplica: "*Gli stati parti di questa Costituzione, credendo nella piena e pari opportunità di educazione per tutti, nella ricerca illimitata della verità oggettiva e nel libero scambio di idee e conoscenze, sono concordati e determinati a sviluppare e accrescere i mezzi di comunicazione tra i popoli e impiegare questi mezzi ai fini della comprensione reciproca e di una conoscenza più vera e perfetta delle vite reciproche…".*

Tutto questo è legato alla prevenzione e alla lotta alla disinformazione e alle fake news, infatti l'alfabetizzazione mediatica è un processo che si organizza in base a cinque temi principali[11]: partecipazione dei giovani, formazione degli insegnanti e risorse curriculari, sostegno dei genitori, iniziative politiche e costruzione di prove. Ovviamente, come tutti i processi, anche esso presenta dei limiti strutturali e delle sfide che possono avere più o meno dei risultati positivi. Proprio per questo sono state fatte cinque precise raccomandazioni: bisogna innanzitutto prendere in considerazione l'ambiente circostante ed adattare ad esso le nuove tecnologie, creare un rapporto interdisciplinare per esempio con la sociologia e le scienze politiche, migliorare la lotta appunto alla disinformazione, creare una base centralizzata e stabile di dati su cui fare le valutazioni ed infine sviluppare corsi di approfondimento per creare risposte adatte alle nuove sfide in questo campo. Quest'ultimi vogliono creare il concetto di responsabilità individuale, per far si che i mezzi comunicativi siano utilizzati nel modo corretto.

A conclusione di questo argomento bisogna riconoscere che gli interventi per limitare la diffusione di notizie false sono stati numerosi e rilevanti, ma bisogna fare anche affidamento alle sanzioni per tutti coloro che le diffondono e migliorare le nostre conoscenze da cittadini per evitarle.

[11] Bulger, M., Davison, P. (2018) *The Promises, Challenges, and Futures of Media Literacy.* Disponibile in: https://digital.fundacionceibal.edu.uy/jspui/bitstream/123456789/227/1/DataAndSociety_Media_Literacy_2018.pdf

1.6. Normativa italiana

Arrivati a questo punto dell'elaborato è doveroso soffermarci sul caso del nostro paese, per capire come le direttive e raccomandazioni europee sono entrate in vigore in Italia.
Prima di tutto bisogna sottolineare che la cyber security è considerata un'emergenza europea, se non mondiale, rilevante. Infatti, è inserita tra le prime tre emergenze da contrastare, insieme al cambiamento climatico e all'immigrazione.

Il problema della cyber security è che basta poco per creare un problema più grande, basta un click per creare una catastrofe. Bisogna quindi considerare quello che in materia viene chiamato "anello debole", ovvero il fattore umano.

Il volume a cui stiamo facendo riferimento per questo particolare studio è "Il futuro della cyber security in Italia: Ambiti Progettuali Strategici"[12]. Esso vuole innanzitutto analizzare il problema a livello nazionale, europeo e internazionale, e vuole avviare nuovi meccanismi di ricerca e di azione con i rispettivi progetti operativi, sia nel campo privato che in quello pubblico. Per ogni progetto si deve far riferimento ad una precisa area operative, gli studiosi ne hanno identificate cinque:

1) Infrastrutture e centri: è necessario proteggere in ordine di priorità la rete Internet nazionale e i data center della Pubblica Amministrazione.
2) Azioni abilitanti: rendere quindi più sicura la difesa da eventuali minacce, prevedendo azioni che salvaguardino per esempio le applicazioni critiche e più importanti del nostro paese.
3) Tecnologie abilitanti: utilizzate per ridurre gli attacchi e proteggere i dati, come principalmente la creazione e l'individuazione di Hardware specifici.
4) Tecnologie da proteggere: come i servizi Cloud e la comunicazione wireless.
5) Azioni orizzontali: la protezione dei dati personali.

Affidandoci ai dati della tabella 1.1, la Banca d'Italia ha registrato tra il 2015 e il 2016 che circa il 45% delle aziende italiane ha subito attacchi informatici. Si individuano quindi i soggetti più a rischio, ossia le grandi imprese, gli esportatori e le industrie ad alta intensità tecnologica. Tuttavia, non si devono escludere le piccole e medie imprese, che rischiano di diventare anche loro un soggetto ad alto rischio.

Tabella 1.1: Attacchi subiti da imprese italiane, 2015-2016

Area geografica:

Nord Ovest: 44,2

Nord Est: 47,3

[12] Baldoni, R., De Nicola, R. e Prinetto, P (2018) *Il futuro della cyber security in Italia: Ambiti Progettuali Strategici.* Roma. Cyber security National Lab. Disponibile in: http://doc989.consiglioveneto.it/oscc/resources/Libro-Bianco-2018.pdf

Centro: 52,3

Sud e Isole: 35,9

Numero di addetti:

20-49: 42,7

50-199: 48,4

200-499: 48,8

500 e oltre: 43,8

Intensità tecnologica:

Alta e medio alta: 48,8

Bassa e medio bassa: 43,8

Incidenza delle esportazioni sul fatturato:

Meno di 1/3: 43,0

Tra 1/3 e 2/3: 51,8

Più di 2/3: 48,5

Percentuale sul totale delle aziende: 45.

Per quanto riguarda i costi, per interrompere gli attacchi e ripristinare il sistema, a livello monetario sono ancora bassi. Il problema è che molto spesso a rimetterci non è il proprietario, ma il pubblico. Anche per questo motivo è stato necessario attuare le direttive, raccomandazioni e norme UE a livello nazionale.

La direttiva NIS è entrata in vigore in Italia il 24 gennaio 2013, con l'utilizzo di un modello istituzionale di tipo temperatamente decentrato. Infatti, per quanto riguarda le autorità competenti NIS vi sono cinque ministeri: salute, ambiente, economia, infrastrutture e trasporti, sviluppo economico. Negli anni precedenti era in vigore il DPCM Monti (2013), in un periodo dove non vi era ancora tanta attenzione nei confronti della materia, e vi era molta difficoltà per quanto concerne l'attivazione della repressione degli attacchi informatici, perché non esisteva una risposta coordinata né a livello nazionale né tantomeno a livello europeo. Con il DPCM Gentiloni del febbraio 2017 viene cambiato l'approccio alla materia[13]. Innanzitutto, viene dato un ruolo rilevante al Dipartimento delle informazioni per la sicurezza (DIS), che funge da collegamento verso l'UE e coordinamento con le autorità competenti in materia negli altri Stati membri.

In sostanza il DIS coordina le varie attività, monitora e trasmette al Presidente del Consiglio tutte le informazioni, elabora analisi strategiche, si coordina con le Forze di Polizia. All'interno dello stesso vi sono quattro uffici: ufficio centrale ispettivo, centrale degli archivi, centrale per la segretezza e la scuola di formazione.

Inoltre, vengono istituiti il Nucleo Sicurezza Cibernetica (NSC) ed il centro di valutazione e certificazione nazionale, al fine di controllare la sicurezza dei prodotti e dei dispositivi.

[13] Decreto del presidente del Consiglio Gentiloni. (2017) Disponibile in: https://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/dpcm-17-febbraio-2017.html

È stato necessario a seguito di numerosi attacchi informatici, sviluppare un nuovo piano nazionale per la protezione dei dati e per la sicurezza informatica, per riordinare i casi in ordine di priorità, così da favorire l'azione e la segnalazione degli attacchi informatici più gravi e complessi, che vengono definiti APT (Advanced Persisistent Threat). Con essi si deve far fronte ad un problema di asimmetria temporale, infatti coloro che compiono gli attacchi riescono a farlo in un arco di tempo molto ristretto, mentre la risposta, seppur coordinata, impiega più risorse e molto più tempo per reprimerli.

Per quanto riguarda le sanzioni che colpiscono coloro che non adottano comportamenti conformi alle direttive dipendono da paese a paese. Infatti, la direttiva NIS lascia un margine di discrezionalità. In Italia per quanto riguarda le sanzioni amministrative si arriva fino a 150.000 euro quando si parla di violazione da parte di operatori di servizi essenziali o fornitori di servizi digitali.

Invece per quanto concerne i compiti di natura tecnica, il decreto prevede l'istituzione all'interno della Presidenza del Consiglio dei Ministri di un CERT (Computer Emergency Response Team), ovvero una squadra che si occupa di prevenire e rispondere ad incidenti informatici in cooperazione con gli altri CERT degli altri Stati membri.

Accanto al DPCM Gentiloni è importante citare la normativa GDPR del 23 maggio 2018, ovvero il Regolamento Generale sulla protezione dei dati, un regolamento dell'Unione Europea riguardante la legislazione in materia di protezione e circolazione dei dati personali e della privacy. Con esso si vuole creare un sistema di gestione dei dati per prevenire ed evitare la diffusione o la perdita degli stessi. Vige il principio della "data protection by design", si deve quindi prendere in considerazione la protezione dei dati fin dalla progettazione e dalla creazione dei vari sistemi.

Per tutte le aziende che non rispettano tali vincoli sono previste sanzioni pecuniarie.

Abbiamo visto quindi come si applicano le normative europee direttamente nel nostro paese, nel capitolo successivo affronteremo il caso specifico di Facebook, il social network maggiormente utilizzato nella nostra società e che è stato oggetto di accuse per quanto riguarda la protezione dei dati personali e dell'utilizzo sbagliato della suddetta piattaforma.

Capitolo 2: Il caso studio di Facebook

2.1. Regole dell'uso di Facebook e meccanismi di controllo

Andremo ora ad analizzare l'utilizzo e le caratteristiche di una delle più importanti piattaforme digitali al mondo, ovvero Facebook, che fu fondata nel 2004 da uno studente di Harvard, Mark Zuckerberg. Essa viene utilizzata tutti i giorni dalla maggior parte di noi, ma spesso non si conoscono fino in fondo i pericoli a cui, involontariamente o meno, si può andare incontro. Stando alle ultime statistiche, per quanto riguarda il nostro paese, Facebook conta 29 milioni di utenti iscritti[14], questo ci fa capire quanto sia diffuso il suo impiego e quanto siano necessarie delle misure di prevenzione per quanto riguarda sia la diffusione di materiale illegale sia la disinformazione e protezione della privacy. Queste misure devono essere coordinate a livello nazionale ed europeo, facendo cooperare il settore privato con quello pubblico.

Analizzeremo prima di tutto il meccanismo di funzionamento, basandoci sulle stesse informazioni fornite nelle impostazioni di Facebook. Innanzitutto, per la creazione del proprio account, questo social network non richiede un pagamento da parte dell'utente, ma riceve un compenso in denaro da tutte le aziende e le organizzazioni che si accordano con esso per mostrare agli utenti inserzioni relative all'utilizzo dei propri servizi e prodotti. Ovviamente, all'utente verranno mostrate le pubblicità più inerenti ai suoi interessi, tramite lo studio che Facebook fa sui contenuti pubblicati e gli interessi dimostrati da chi lo utilizza.

L'utente però in cambio è tenuto ad usare il proprio nome e cognome, fornire informazioni essenziali per l'utilizzo, e non concedere a nessun altro l'accesso al proprio profilo. Inoltre, è vietato l'accesso ai minori di tredici anni e a tutti coloro che per determinati precedenti hanno il divieto di accedere in base alla normativa della piattaforma. Bisogna però sottolineare che ad oggi, nonostante tali divieti, vi è una presenza determinante di account falsi, ed è sempre più diffuso la presenza su di essa da parte di bambini non autorizzati secondo le regole. Proprio a tal proposito Facebook si serve di un gruppo di esperti che ogni giorno si impegna nella rimozione di materiale illegale e di account ritenuti non conformi alle direttive. Quindi è giusto sottolineare che nonostante viviamo in una società sempre più digitalizzata, è necessaria la supervisione umana al fine di contrastare comportamenti e contenuti illeciti. Tratteremo nei prossimi paragrafi l'impatto psicologico che questi contenuti hanno sugli addetti ai lavori.

Ritornando alle possibilità che ha chi usufruisce della piattaforma, possiamo dire che l'utente ha la facoltà di decidere chi può vedere e condividere le proprie foto, i propri post o i propri video, in base alle opzioni fornitegli: amici, amici più stretti, conoscenti o tutto il mondo.

[14]Russo, F. (2020) *Social Media in Italia: ecco alcuni dati per il 2020*. Disponibile in: https://www.franzrusso.it/condividere-comunicare/social-media-italia-dati-2020/

L’obiettivo che la piattaforma dichiara è quello di raccogliere quante più informazioni dai profili delle persone, per migliorare i propri prodotti e per fornir loro suggerimenti, che possono riguardare gruppi o eventi ad esempio. Essendo inoltre possibile condividere la propria posizione, Facebook giustifica l’utilizzo delle informazioni relativa ad essa, volendola utilizzare sempre per i medesimi fini di miglioramento.

Dichiara quindi in ogni modo di non abusare e condividere i contenuti privati, ma di proteggerli in base al consenso concesso al momento dell’iscrizione.

Abbiamo detto nei precedenti capitoli, che il controllo delle piattaforme online nel tempo è aumentato, e a tal proposito è necessario citare nuovamente il GDPR, ovvero il Regolamento generale sulla protezione dei dati. Ogni utente può in qualsiasi momento accedere ai propri dati, cambiarli o eliminarli. Inoltre, tutti noi abbiamo il cosiddetto diritto di opposizione ed il diritto di limitarne l’utilizzo.

Dall’altra parte Facebook si impegna a non divulgare e diffondere volontariamente tali contenuti e a garantire un ambiente sicuro per chi usufruisce dei suoi servizi. Bisogna però sottolineare che la piattaforma non accetta responsabilità in relazione a comportamenti, contenuti o perdite di dati che non siano riconducibili alle proprie azioni.

Nell’ambito delle controversie, esse vengono risolte in maniera diversa in base all’appartenenza o meno all’Unione Europea. Interessandoci a quest’ultimo aspetto, possiamo constatare che nel caso di uno Stato membro si devono applicare le leggi dello Stato in questione e la controversia può essere risolta davanti a un qualsiasi tribunale competente dello stesso.

Facebook vuole garantire la libertà di opinione e di espressione sulla propria piattaforma, ma nel caso in cui fosse certo di una violazione dei propri principi, la sua community può decidere di sospendere o eliminare definitivamente l’account di un utente, o di richiedere a quest’ultimo la rimozione di determinati contenuti o la sospensione di un comportamento ritenuto illecito nei confronti di essa o di un altro utente.

Bisogna quindi sottolineare che l’intenzione di Facebook è quella di un’armoniosa condivisione di interessi, contenuti e informazioni, al fine di agevolare la connessione tra i vari paesi e i vari utenti e di trarre guadagno dalle inserzioni e dalle varie aziende proprietarie. Nelle pagine successive andremo ad analizzarne le statistiche per poi arrivare allo scandalo che ha investito Facebook nell’ultimo periodo, Cambridge Analytica, e le conseguenze che esso ha portato al mondo della cyber security.

2.2. Statistiche, contenuti, uffici

In questo ambito è giusto fare una breve analisi di quanti contenuti vengono pubblicati al giorno, da chi e quante persone lavorano all'interno di Facebook, questo per comprendere al meglio la sua diffusione e il suo meccanismo. Possiamo far riferimento a statistiche risalenti al 31 dicembre 2019, secondo cui al mondo ci sono 2.5. miliardi di utenti attivi mensilmente (MAU) e 1.66 miliardi di utenti attivi al giorno (DAU)[15]. Questo per far capire al lettore quanta importanza ha questa piattaforma su scala globale e quanto è fondamentale che funzioni nel modo giusto e che sia utilizzato soprattutto secondo le regole.

Tra tutti gli utenti l'88% accede tramite il cellulare e molto spesso viene condivisa anche la posizione dalla quale il post, ad esempio, viene pubblicato. Questo è un particolare da non sottovalutare, perché può rendersi pericoloso se dall'altra parte dello schermo vi sono persone che sfruttano queste informazioni con fini sbagliati. Per quanto riguarda gli account falsi, Facebook si è impegnato ad eliminarne 1.3. miliardi, ciò è sicuramente un inizio ma ad oggi questi profili hanno raggiunto un numero sempre più alto e vengono utilizzati per vari scopi, come ad esempio le truffe online o la divulgazione di materiale illegale. A tal proposito Facebook sta assumendo sempre più personale con una crescita annua del 26% per far fronte a queste minacce e per rispondere alle sempre più articolate esigenze degli utenti, che sono circa 400 in più al minuto.

Facebook porterà sicuramente tanti benefici a chi ne usufruisce, grazie a questa piattaforma si può comunicare facilmente e velocemente con tutto il mondo, si possono condividere i propri interessi e le proprie passioni, ci si può informare su quello che accade intorno a noi, e dall'altro lato essa stessa guadagna miliardi di euro attraverso le inserzioni pubblicitarie. Ma come la maggior parte delle cose, nasconde un lato oscuro.

2.3. Le critiche a Facebook

Lo scandalo che ha trovato coinvolto Facebook nel 2018 ha cambiato per sempre il suo rapporto con gli utenti. Stiamo parlando del caso di Cambridge Analytica, una società di consulenza per il marketing online, che si occupa di analizzare i dati dei consumatori e adattarli alla scienza comportamentale, per capire quali e quante persone sono affini ai target di determinate aziende o organizzazioni, e per creare quindi pubblicità fortemente personalizzate su ogni individuo[16]. Come primo passaggio, prende in esame quanti mi piace mette un determinato utente, a quali contenuti e da che luogo. Successivamente, queste informazioni passano attraverso algoritmi e modelli e viene così creato un profilo per ogni singolo utente, così come avviene nel campo della psicologia, e vengono fatte pubblicità in base a ciò che sono riusciti a reperire attraverso tali dati.

15 *Statistiche e fatti di Facebook*. (2020). Disponibile in: https://www.websitehostingrating.com/it/facebook-statistics/ ; https://investor.fb.com/investor-events/default.aspx

16 Manietti, E. (2018) *Il caso Cambridge Analytica, spiegato bene.* Disponibile in: https://www.ilpost.it/2018/03/19/facebook-cambridge-analytica/

Ogni giorno, ognuno di noi lascia delle informazioni su queste piattaforme, e ciò rende più pericolosa la nostra esistenza, in quanto possiamo far sapere agli altri dove viviamo, cosa ci piace fare, in che luoghi andiamo spesso e così via. Dal 2014 però questa società è stata accusata di utilizzare dati per scopi ben diversi da quelli dichiarati. Tutto è partito da un'applicazione chiamata "thisisyourdigitallife", ovvero questa è la tua vita digitale, creata da un ricercatore dell'Università di Cambridge, Aleksandr Kogan. Per accedere ad essa gli utenti potevano farlo attraverso il login di Facebook, accettando di condividere con essa dati come l'indirizzo e-mail, l'età ed il sesso, il che era consentito a quel tempo dagli stessi termini d'uso, se non fosse che insieme alle proprie informazioni venivano reclutate anche quelle degli amici dell'iscritto senza che essi fossero informati o che acconsentissero. Quando Facebook capii la pericolosità a cui potevano andare in contro i propri utenti, decise di interrompere tale pratica, ma ormai l'applicazione era riuscita a raccogliere una grande quantità di dati, che decise di condividere con Cambridge Analytica, violando quelle che sono invece le regole.

Molti dati presi dall'applicazione di Zuckerberg vennero utilizzati per la propaganda elettorale di Donald Trump negli Stati Uniti. Infatti, tramite l'utilizzo della piattaforma vennero diffuse notizie false e contenuti contro Hilary Clinton, portando quindi il consenso dall'altra parte. Stessa cosa si presuppone che sia stata fatta per la Brexit, influenzando l'opinione pubblica.

Non possiamo dimostrare ad oggi la buona o cattiva fede di Facebook in questa vicenda, ma possiamo sicuramente sottolineare il fatto che nonostante le sue regole è ancora troppo facile rubare dati ed informazioni degli utenti senza il loro consenso, ed è ancora troppo semplice divulgare notizie false o materiali illegali.

In questo contesto, è bene ora sottolineare che il problema non sia solo quello della privacy, ma anche quello della disinformazione su tale piattaforma, che ad oggi costituisce un grave pericolo per la democrazia. A tal proposito la Commissione propone misure per contrastarla[17]:

- Un codice di buone pratiche sulla disinformazione, come detto nei capitoli precedenti: tutte le piattaforme online dovranno applicarlo e rendere più trasparenti i propri contenuti, soprattutto per quanto riguarda gli aspetti della politica e della propaganda. Deve essere concesso a terzi il controllo per avere la piena consapevolezza di agire nella maniera corretta.
- Una rete europea indipendente di verificatori di fatti: per rendere possibile un approccio comunitario e questi verificatori verranno scelti tra i membri dell'UE.
- Una piattaforma UE online sicura sulla disinformazione: la quale aiuterà la rete europea di verificatori a raccogliere ed analizzare più dati possibili.
- Promozione dell'alfabetizzazione mediatica.
- Sostegno agli Stati membri nel garantire equi e solidi processi elettorali: per far fronte sia alla disinformazione che agli attacchi informatici
- Promozione di sistemi di identificazione online volontari: per creare maggior trasparenza e affidabilità delle interazioni online.

[17] *Lotta alla disinformazione online: proposta della Commissione di un codice di buone pratiche dell'UE. (*2018). Bruxelles. Disponibile in: https://ec.europa.eu/commission/presscorner/detail/it/IP_18_3370

- Sostegno dell'informazione diversificata e al giornalismo di qualità.
- Attività di sensibilizzazione per contrastare il fenomeno delle fake news.

Un altro problema da non sottovalutare è la diffusione, sopra tale piattaforma, di materiale volto alla divulgazione di movimenti estremisti e di incitazione all'odio e alla violenza, utilizzati per persuadere specialmente i giovani, che cercando ancora la loro strada ed il senso della loro esistenza sono più facilmente influenzabili. Tratteremo di questo argomento nel capitolo successivo.

2.4. Estremismo in Europa

I giovani sono i soggetti più a rischio in questo campo, poiché sono maggiormente influenzabili e più facilmente reclutabili da organizzazioni, movimenti o partiti estremisti. Anche per quanto riguarda questo argomento le piattaforme online e più precisamente i social network sono canali attraverso cui l'estremismo cerca di diffondersi in Europa, servendosi di filmati, fotografie o altri contenuti di vario genere.

Gli adolescenti, non avendo ancora idee chiare su cosa vogliono fare nella vita, e soprattutto non avendo ancora orientamenti politici o religiosi precisi e chiari, tendono ad essere persuasi da persone che si occupano di propaganda online, il più delle volte pubblicando contenuti che sono contrari ai termini d'uso, nel nostro caso, di Facebook. Si tratta molto spesso di contenuti volti a catturare velocemente la loro attenzione, come ad esempio canzoni, vignette, articoli di satira, immagini, che mettono in evidenza gli aspetti negativi della nostra società, della democrazia, e dall'altro lato esaltano il comportamento dell'estremismo, creando così una sorta di opposizione tra ciò che è bene e ciò che è male. Per questo motivo, i giovani sono spinti a rendersi conto di quali sono i punti deboli delle nostre democrazie, quali sono gli esponenti da criticare, e sono attratti invece da qualcosa di nuovo e sconosciuto che attraverso i video e i social appare loro genuino ed interessante.

Dall'altro lato invece, queste persone utilizzano i canali web per diffondere il panico e il terrore nelle nostre società. Infatti, molto spesso è stato utilizzato Facebook per diffondere notizie false, come ad esempio i prossimi possibili attacchi terroristici al Vaticano per quanto riguarda Roma, oppure in luoghi affollati, come può essere il Duomo di Milano o luoghi di aggregazione di giovani. Molto spesso, queste notizie vengono condivise nuovamente dagli utenti per avvertire a loro volta i loro amici, e in poco tempo la paura è entrata nelle nostre case. È proprio questo uno degli obiettivi dell'estremismo: mettere paura.

Facebook ha da sempre preso le distanze da tali contenuti, ed ha sempre cercato di rimuoverli, ma con il tempo sono diventati un numero spropositato ed importante, e questo ha reso necessario un maggior intervento da parte dei singoli operatori, ed una coordinazione a livello nazionale ed europeo.

Per rispondere a tale problema, l'Unione Europea ha deciso di sostenere e finanziare all'interno del "quadro Orizzonte 2020" (un programma di finanziamento creato dalla Commissione, per promuovere la ricerca in Europa), il progetto DARE (Dialogue about Radicalisation and Equality), che comprende 17 partner in 13 paesi europei, tra cui la Francia, la Germania ed il Regno Unito, e che rimarrà attivo per i prossimi quattro anni[18]. L'intento di tale progetto è quello di analizzare i comportamenti e le scelte dei giovani di età compresa tra i 12 ed i 30 anni, proprio per i motivi citati precedentemente, ovvero perché sono i soggetti più facilmente influenzabili. Prenderanno in esame i canali dove i giovani esprimono maggiormente i propri messaggi, e faranno uno studio anche psicologico, per capire perché siano spinti verso l'estremismo e in che modo, così da poter sviluppare un programma più forte nella lotta alla radicalizzazione. DARE è strettamente collegato alle politiche dei vari paesi aderenti, poiché attraverso le loro statistiche essi possono sviluppare dei programmi indipendenti educativi, basti pensare all'istruzione che nel nostro paese si occupa di educare i giovani all'interno della nostra società.

Nel tempo inoltre c'è stata un'evoluzione nel campo dell'estremismo, e questo progetto è volto a scoprire tutti i nuovi aspetti, per poter coordinare una risposta efficace a tale fenomeno e per capire come contrastare la sua diffusione nei soggetti più a rischio, e soprattutto per capire come coordinare una risposta tra enti privati ed enti pubblici.

Possiamo riscontrare che oltre ai contenuti estremisti, molto spesso vengono condivisi video che incitano all'odio, al bullismo, alla violenza ed al razzismo, ed anche in questo caso sono coinvolti maggiormente i giovani. Bisogna quindi trovare una soluzione appropriata, poiché attraverso questi contenuti si creano stereotipi sbagliati da seguire, si creano ideologie radicalizzate e si rischia di diffondere un messaggio sbagliato dell'utilizzo dei social, i quali invece dovrebbero essere usati nella maniera corretta e sfruttati al meglio, sia per quanto riguarda gli aspetti lavorativi sia per quelli di divertimento e di svago.

Secondo un'analisi condotto dal National Whistlevlower Center, Facebook non starebbe lavorando nella maniera corretta per evitare la diffusione di tali contenuti. I ricercatori infatti, hanno monitorato nel corso di cinque mesi le pagine sul social network di Zuckerberg, e hanno constatato che sono circa tremila gli utenti affiliati ad organizzazioni estremiste e terroristiche[19]. Utilizzando Facebook, possiamo sapere che ogni anno lo stesso social mette insieme i nostri momenti più significativi, foto e video con gli amici, per celebrare l'anno nuovo, e in molti casi Facebook fa lo stesso con gli utenti estremisti, così da condividere esso stesso contenuti che dichiara da sempre illegali. Questo ci fa capire che molto spesso non vi è il controllo che ci dovrebbe essere, e nonostante siano stati ed individuati tantissimi account illegali, il problema non si riduce ma anzi, non si riescono ad individuare tutti.

Negli anni precedenti la risposta a tali minacce su Facebook avveniva attraverso l'utilizzo di algoritmi di intelligenza artificiale specifici, ma essendo aumentato il pericolo ha dovuto necessariamente introdurre la

[18] European Union's Horizon 2020. (2020). *Dialogue About Radicalisation and Equality.* Disponibile in: *http://www.dare-h2020.org*

[19] *Perché Facebook sta perdendo la battaglia contro l'Isis e il terrorismo online.* (2019). Disponibile in: https://www.wired.it/internet/social-network/2019/05/14/facebook-isis-terrorismo/

vigilanza umana, perciò ha assunto nuovo personale, che si occuperà del controllo della piattaforma, della rimozione di contenuti illegali e non idonei, e delle possibili sanzioni nei confronti di chi li condivide.

2.5. Impatto psicologico sugli operatori

Negli ultimi anni per contrastare queste minacce è stato quindi necessario l'intervento della supervisione umana. A questo fine, Facebook si è proposto di utilizzare l'occhio umano per visionare ed eventualmente rimuovere i contenuti non conformi alle regole. Quello che andremo ad analizzare in questo momento, è come questi operatori svolgono il loro lavoro e soprattutto qual è l'impatto psicologico a cui vanno incontro.

In uno studio effettuato su "The Guardian", sono state rese pubbliche delle interviste effettuate in maniera anonima a degli ex operatori,[20] con il fine di capire quali fossero le loro impressioni riguardo al proprio lavoro e quali fossero gli effetti psicologici derivanti. Quando lavoravano, erano obbligati a visionare questi contenuti estremisti, video pedopornografici, ed immagini molto forti che lasciavano dentro di loro delle "impronte". Infatti, secondo vari studi molti di loro sono stati influenzati da ciò che vedevano, e sono passati a partiti estremisti ad esempio, oppure sono rimasti scandalizzati. Per quest'ultimo caso abbiamo una testimonianza proveniente da un report di The Verge, che ci dice: "*Un ex moderatore ora dorme con una pistola al suo fianco*", rimasto impaurito da un video che aveva analizzato riguardo ad un accoltellamento.

Questo ci deve far ragionare molto perché questi, spesso sottopagati rispetto alle ore di lavoro e alle modalità in cui lo svolgono, prima ancora di essere dei lavoratori, sono delle persone. Anche loro hanno delle proprie idee, hanno i propri valori e le proprie idee politiche, e possono essere influenzati da ciò che vedono, possono tendere verso posizioni estremiste o possono avere paura di ciò che guardano. Inoltre, vi è tanta ignoranza su chi sono, che lavoro svolgono e che importanza ha per il mondo ciò che loro fanno. La maggior parte delle persone non è al corrente forse neanche della loro esistenza.

Oltre a visionare video e contenuti, hanno avuto l'incarico di leggere conversazioni private tra adulti e bambini a sfondo sessuale, dove queste persone chiedevano foto in cambio di soldi, ed è in questa occasione che hanno dichiarato di aver capito in che società viviamo e quale pericolo può portare l'utilizzo scorretto dei social networks, non solo per noi ma anche e in primo luogo per i bambini.

Molti degli intervistati sostengono di aver avuto in seguito problemi psicologici o addirittura paura a tornare la sera da soli nelle proprie abitazioni. I moderatori di Berlino hanno anche avuto la possibilità di andare da un consulente per esporre i propri problemi, ma chi si è dimostrato troppo vulnerabile è stato licenziato con il consiglio di trovare un giusto psicologo adeguato a quel tipo di problematiche. Vuol dire che

[20]The Guardian. (2019). *Revealed: catastrophic effects of working as a Facebook moderator*. Disponibile in: https://www.theguardian.com/technology/2019/sep/17/revealed-catastrophic-effects-working-facebook-moderator

ancora non c'è la giusta tutela ed il giusto rispetto di chi si occupa di questo, e soprattutto non si conoscono gli effetti psicologici che si hanno guardando questi contenuti.

Quello che bisogna dire è che questo lavoro è inevitabile ed è molto importante per il corretto funzionamento di qualsiasi piattaforma online e della protezione dei suoi utenti, perciò non può essere eliminato, ma una soluzione potrebbe essere quella di assumere più persone così da alleggerire il carico di lavoro di quelli già assunti.

Per quanto riguarda strettamente Facebook, alcuni suoi operatori sono stati accusati di aver preso il materiale illegale e di averlo salvato sui propri dispositivi, ma ciò è stato smentito in quanto è per gli operatori severamente vietato entrare nelle sale dove lavorano con i propri cellulari o apparecchi elettronici, e che il sistema è stato creato con l'impossibilità per loro di salvare qualsiasi tipo di contenuto.

Ciò che però ha creato scalpore è quello che è successo nel 2016, quando Facebook ha involontariamente divulgato informazioni personali dei moderatori, mettendo a rischio non solo loro ma anche le rispettive famiglie. Il problema è venuto alla luce quando questi operatori hanno ricevuto richieste di amicizia nei propri profili privati, di persone che controllavano a lavoro e che erano esponenti di movimenti estremisti e terroristici. Proprio per questo motivo è necessario che coloro che proteggono noi siano a loro volta protetti, è importante che la loro identità resti nascosta e che abbiano delle garanzie per quanto riguarda il rispetto dei loro diritti umani. Devono essere loro garantite ore giuste di lavoro ed un giusto salario, devono lavorare in libertà ma soprattutto in sicurezza, e devono essere tutelati dalle aziende in cui lavorano. Questo per permettere il corretto svolgimento del loro compito ma soprattutto per non metterli in pericolo a loro volta.

Secondo le ultime statistiche nel 2009 erano solo 12 gli operatori Facebook che si occupavano di questo problema, e ad oggi sono circa 35.000. Ai moderatori, chiamati con il termine di Community Operations, si affianca il settore della Content Policy, che crea le regole della comunità, e quello della Community Integrity che si occupa invece di creare la tecnologia avanzata per controllare i vari account.

Bisogna quindi riconoscere a Facebook il grande impegno che ha riposto in questo campo. Ciò che però noi cittadini ed utilizzatori di esso possiamo fare, è quello di comportarci nella maniera giusta e consigliata, soprattutto alla luce di quello che abbiamo precedentemente detto, ovvero il pericolo in cui incorrono tutti coloro che tentano di proteggere noi, la nostra privacy e la nostra vita. Certamente quello che fanno loro è un lavoro molto più intenso e complicato, a noi si richiede solo di essere dei bravi cittadini, di non cadere nelle trappole di coloro che utilizzano i social network per cattivi fini, e di rispettare tutte le regole.

È importante a questo scopo leggere sempre tutti i termini d'uso di tutte le applicazioni che utilizziamo, anche se spesso richiede del tempo, perché frequentemente accettiamo che vengano divulgate delle nostre informazioni senza saperlo, e agiamo in modo superficiale.

La domanda è la seguente: si può fondare l'utilizzo di Internet sulla speranza che gli utenti si comportino bene?

Capitolo 3: Coronavirus: la nuova sfida digitale

3.1. Perché non è solo un problema sanitario?

Il nostro paese si è ritrovato di fronte ad una sfida senza precedenti, il Covid-19. È una malattia infettiva respiratoria partita dalla Cina, che presenta nella maggior parte dei casi sintomi ricollegabili a quelli influenzali ed è caratterizzato da una veloce e facile trasmissione. L'Italia in poche settimane si è vista costretta a "fermare" l'economia, obbligando i cittadini a circa due mesi di quarantena, bloccando tutte le attività non considerate di prima necessità, dai bar e ristoranti ai negozi, fino ad arrivare alle fabbriche e alle imprese, questo per permettere di contenere il contagio e di far respirare gli ospedali, soprattutto al nord. È proprio in questa situazione di emergenza che il nostro paese, come tutto il mondo, si è reso conto di quanto importante sia la tecnologia e quanto sia importante avere delle regole e delle norme per la cyber sicurezza. Infatti, le sfide sono state molteplici e in svariati campi, basti pensare alle scuole, alle università e al lavoro. Per poter garantire l'istruzione si è riusciti in poco tempo a creare programmi per lo svolgimento online e a distanza delle lezioni, per poter permettere a tutti gli studenti di non perdere l'anno e di seguire gli insegnanti da casa. Stessa cosa vale per i lavoratori, che hanno sperimentato il lavoro da casa il cosiddetto "smart working". Tutte queste possibilità sono importanti e necessarie ma devono essere accompagnate da un grande controllo per quanto riguarda la privacy e l'utilizzo di dati personali o pubblici, come quelli delle varie aziende interessate. Entrando ora nel particolare, i lavoratori si sono ritrovati ad adottare una modalità di lavoro completamente diversa da quella abituale, ed è quindi necessario che essi siano istruiti nel migliore dei modi e che siano soprattutto tutelati. Come abbiamo visto nei capitoli precedenti, gli attacchi informatici sono sempre più diffusi ed alcuni sono complicati da eliminare, con lo smart working cresce la possibilità che essi si verifichino, per questo è necessaria una vigilanza specifica e un maggiore coordinamento europeo. Dall'inizio della pandemia infatti, sono aumentati gli attacchi informatici anche nei confronti delle strutture sanitarie, per rubare i dati delle vittime e dei malati. A tal fine, si è dovuto trovare un meccanismo di difesa che permetta sia ai lavoratori che agli studenti di operare e studiare nella massima sicurezza e tranquillità. Facendo riferimento alla categoria dei lavoratori, essi sono sempre stati abituati nella maggior parte dei casi a ricorrere all'utilizzo di computer aziendali con determinati software per la protezione dei dati e per la protezione da eventuali attacchi. Lavorando da casa, spesso con dispositivi legati ai propri social network e ai propri dati, aumenta il pericolo. Infatti, come abbiamo visto in precedenza, basta collegarsi a determinate app con il proprio smartphone per condividere inconsapevolmente o meno le proprie informazioni e questo diventa anche un problema per i dati aziendali, perché si ha il pericolo di renderli accessibili a terzi senza volerlo.

Anche nel caso delle videoconferenze o delle video lezioni non si ha la piena certezza di essere protetti, infatti sarebbe necessario l'utilizzo di VPN (Virtual Private Network) per garantire la protezione del traffico in uscita e in entrata, oltre che dei software specifici antivirus.

Inoltre, è stato constatato attraverso una ricerca del Identity Theft Research Center[21] che sono aumentati in modo rilevante gli errori per quanto concerne la condivisione di informazioni sensibili a persone che non dovrebbero averle. Questo rende ancora più importante la sicurezza dei sistemi e delle piattaforme digitali, rendendolo evidente ai paesi e all'Unione Europea nel particolare, che si è mossa in questo campo da diversi anni per poter proteggere gli Stati membri. Nel nostro paese in realtà il ricorso allo smart working è arrivato con un forte ritardo e sono ancora moltissime le aziende che ancora non si sono servite di tali meccanismi. Essendo però consapevoli del cambiamento che ci sarà nella nostra società, in termini di distanziamento sociale, è evidente che ci dovrebbero essere degli sviluppi in questo ambito.

Infatti, non si ha la certezza che potremmo tornare tutti alla vita di prima, non si ha certezza di poter tornare tranquillamente nelle proprie aziende, e nelle proprie scuole e università, per cui la tecnologia dovrà essere accolta e utilizzata da tutti nel migliore dei modi e garantendo la tutela di chi la utilizzerà e la completa trasparenza dei servizi.

Mai come in questo stato emergenziale abbiamo capito la necessità di avere regole che tutelino il nostro diritto alla privacy, che ritroviamo nel GDPR (General Data Protection Regulation). Infatti, come detto in precedenza, anche i bambini e quindi i minori, si sono ritrovati ad utilizzare determinate piattaforme online per studiare e mai come oggi devono essere garantiti tutti i diritti del caso. È facile tramite queste applicazioni, risalire ad informazioni private e non si ha quindi la certezza assoluta di essere salvaguardati durante il loro utilizzo. Inoltre, tutti noi non potendo avere contatti reali e diretti con le persone abbiamo sperimentato l'utilizzo delle videochiamate. Anche in quest'ultimo caso spesso le app richiedono l'accesso tramite le credenziali di Facebook ed inconsapevolmente rischiamo di condividere le nostre informazioni con soggetti pericolosi, come successo ad esempio nel caso di Cambridge Analytica.

Non è inoltre un problema solo per i singoli cittadini, perché nell'ultimo periodo si sono visti attacchi informatici anche nei confronti degli ospedali, che impegnati a fronteggiare l'emergenza sanitaria si sono ritrovati ad avere ulteriori difficoltà, da chi sfrutta questa situazione per entrare nei loro computer e rubare dati relativi alla struttura ospedaliera, così da poterli utilizzare per truffare le persone. Negli ultimi giorni di marzo, l'ospedale Spallanzani di Roma, che si trova in prima linea per combattere il Covid-19 e per la ricerca di una possibile cura, è stato oggetto di un attacco informatico[22], che ha fatto emergere la necessità di una riunione straordinaria del Nucleo Sicurezza Cibernetica, collegato al Dipartimento delle Informazioni per la Sicurezza (DIS) che si occupa di far fronte ad eventuali problemi cibernetici e di prevenire gli attacchi informatici.

Si è reso evidente, attraverso questa riunione, il problema già esistente della protezione dei dati e sono state avvisate le strutture ospedaliere di tutto il paese per poter fronteggiare unilateralmente un fenomeno però che ha portata mondiale. Ci deve essere una risposta coordinata anche da parte dei cittadini, che sono stati

[21]Schiaffino, M. (2020) *Smart working: perché la prima preoccupazione dev'essere la cyber security*. Disponibile in: https://www.cybersecurity360.it/soluzioni-aziendali/smart-working-perche-la-prima-preoccupazione-devessere-la-cyber-security/

[22] Sol, P. (2020) *Coronavirus, attacco hacker allo Spallanzani di Roma. Indaga la procura.* Disponibile in: https://www.ilsole24ore.com/art/coronavirus-attacco-hacker-spallanzani-roma-indaga-procura-roma-ADtLHTH?refresh_ce=1

invitati dalle autorità europee e nazionali e dalla stessa polizia postale a mantenere alta l'attenzione, ad essere più scrupolosi. Ma come detto in precedenza non ci si può affidare al buon senso delle persone, e proprio per questi la rete dei CSIRT (Computer Security Incident Response Team) europei si è detto disponibile ad aumentare i controlli relativi alla sicurezza.

Gli stessi dati rubati dagli ospedali sono stati utilizzati per creare le cosiddette e-mail truffa, che utilizzando illegalmente il marchio dell'OMS (Organizzazione Mondiale della Sanità) rubano dati ai cittadini e a tutti coloro che aprono il link all'interno. Essa si presenta come un'e-mail normale, con su scritto nell'oggetto: "Coronavirus disease (COVID-19) Important Communication[23]" con un allegato che apparentemente sembrerebbe avere informazioni sul tema ma che in realtà è un malware per impossessarsi delle informazioni private.

A tal proposito il Consiglio Nazionale degli Ingegneri ha diffuso raccomandazioni generali[24] per aiutare gli utenti a proteggersi da questi attacchi. Prima di tutto consiglia di dotarsi di un antivirus, installandolo nel proprio computer e aggiornandolo ogni qual volta, servendosi della possibilità di effettuare ogni giorno il backup dei dati. Inoltre, consigliano di utilizzare password di difficile lettura e di munirsi di una diversa per ogni applicazione o account. E ancora, consiglia di utilizzare sistemi di crittografia dei messaggi di posta elettronica, soprattutto per chi non è pratico e rischierebbe di cadere facilmente nelle truffe online.

È bene però anche intraprendere una propaganda di sensibilizzazione non solo dei cittadini ma anche delle aziende, così da rendere chiare le norme e le regole al personale che si serve di queste nuove tecnologie.

Coloro che effettuano tali azioni illegali fanno affidamento al periodo difficile che tutto il mondo sta affrontando, sia perché i cittadini sono sempre più "connessi" ed hanno più tempo libero per navigare su Internet, sia perché vi è un sentimento comune di paura e di sgomento. Proprio per quest'ultimo motivo è bene affrontare in questa circostanza l'argomento della disinformazione e delle fake news. I cittadini sono spaventati, leggono ogni giorno milioni e milioni di articoli per capire come fronteggiare il virus e per sentirsi più tranquilli. Il problema è: quali articoli sono pertinenti? Quali articoli informano nel modo giusto gli individui?

Da febbraio a questa parte, le persone sono state travolte da una miriade di notizie. La gente preoccupata digita sui motori di ricerca, come ad esempio Google: "sintomi del Coronavirus", prendendo per vero tutto ciò che leggono e creando a loro volta panico generale, condividendo tali informazioni. Potrebbe essere opportuno citare la notizia, ovviamente falsa e priva di fondamento scientifico, che circolava sul web all'inizio della pandemia, ovvero quella che gli animali domestici trasmettano ai padroni il Coronavirus. In pochi giorni, sono stati tantissimi gli animali che sono stati abbandonati o riportati al canile, questo per una

[23] Cyber Security 360. *Coronavirus, nuovo attacco spear phishing per rubare i dati personali: i dettagli*. (2020) Disponibile in: https://www.cybersecurity360.it/nuove-minacce/coronavirus-nuovo-attacco-spear-phishing-per-rubare-dati-personali-i-dettagli/

[24] Gennari, L. (2020) *Coronavirus, gli ingegneri contro gli attacchi informatici: 10 consigli.* Disponibile in: https://www.firstonline.info/coronavirus-gli-ingegneri-contro-gli-attacchi-informatici-10-consigli/

pura ed enorme ignoranza sul tema. Questo è solo un esempio dei tantissimi problemi che ha portato la cattiva informazione. Moltissime persone si sentono in dovere e si sentono competenti in materia, tanto da poter riportare su ogni sito qualsiasi cosa, pur di essere condivisi e di avere visualizzazioni.

Proprio per non far cadere la popolazione europea nel panico generale, l'UE si è messa al primo posto nella lotta alla disinformazione, invitando i cittadini a far riferimento solamente alle notizie ufficiali e di seguire i consigli delle sole autorità sanitarie pubbliche competenti e dei siti delle organizzazioni internazionali. Essa vuole anche in questo caso creare una risposta coordinata di tutti gli Stati membri, chiedendo loro di collaborare alla condivisione delle sole notizie autentiche, per tutelare quello che è un diritto fondamentale degli uomini: la libertà di espressione, di opinione e di condivisione.

La cattiva informazione crea dubbi nelle menti delle persone, che non sanno più cosa è giusto o sbagliato fare creando conseguenze gravi[25] : minacce alla sicurezza e perdita di fiducia nei governi e nei media. Per questo bisogna individuare i soggetti che commettono queste azioni ed aiutare i cittadini ad avere informazioni adatte.

Gli stessi social network, di cui abbiamo esplicato l'importanza precedentemente, si sono mossi per la protezione degli utenti dalle fake news. Primo tra tutti WhatsApp, un'applicazione di messaggistica istantanea creata nel 2009 e acquistata da Facebook nel 2014, che si è impegnata a controllare la diffusione di messaggi inoltrati con lo scopo di creare disinformazione, consentendo la condivisione di essi con altre persone solo per cinque volte. Stessa cosa è stata fatta da Facebook, che a sua volta collabora con altre organizzazioni per la lotta alla disinformazione nell'ambito del coronavirus e tramite esso sono state fatte numerose donazioni. Inoltre, una volta che una notizia sarà considerata falsa o errata, Facebook ha annunciato che ne eviterà la condivisione avvertendo tutti coloro che avranno interagito con tale informazione, mettendo like o commentando ad esempio. Non si hanno avuto ancora i risultati auspicabili, ma è sicuramente un punto di partenza

. Inoltre, negli Stati Uniti c'è stata l'introduzione di un centro informazioni Covid-19 chiamato "Get the Facts[26]" che contiene tutti gli articoli approvati e considerati veritieri, e che sarà presto utilizzato anche in Italia.

Importante è stato il contributo di un gruppo di attivisti digitali, il quale ha creato un progetto no profit il "Covid19Italia.help" per diffondere le corrette informazioni, per raccogliere i fondi necessari a quest'emergenza sanitaria ed economica e per unire i cittadini in questo momento difficile. Dalla sua attivazione, secondo le fonti citate sulla Repubblica[27], vi sono stati 80 volontari che hanno processato circa

[25] Commissione Europea. (2020) *Combattere la disinformazione.* Disponibile in: https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/fighting-disinformation_it

[26] La Stampa. (2020) *Sorpresa la disinformazione su Facebook si può combattere*. Disponibile in: https://www.lastampa.it/tecnologia/idee/2020/04/16/news/sorpresa-la-disinformazione-su-facebook-si-puo-combattere-1.38725713

[27] Repubblica. (2020) *Nasce Covid19Italia.help: un sito non profit per combattere fake news e disinformazione.2020*. Disponibile in: https://www.repubblica.it/cronaca/2020/03/22/news/nasce_covid19italia_help_un_sito_non_profit_per_combattere_fake_news_e_disinformazione-251981708/

700 segnalazioni che riguardano servizi di consegna a domicilio, attività ricreative per i bambini, raccolte fondi, supporto psicologico agli utenti, e informazioni utili. È un'iniziativa importante, che da voce personalmente ai cittadini i quali possono aiutarsi a vicenda, sostenersi e scambiarsi esperienze vere in un momento in cui la solidarietà sembra essere la prima cosa necessaria. Questo può essere considerato il potere della condivisione, che aiuta tutti noi ad essere vicini in un momento mai vissuto prima, e tramite questo progetto i cittadini vengono istruiti ad affidarsi alle fonti di informazione ufficiali riducendo il rischio di truffe, inganni e comportamenti illeciti.

L'ultima innovativa iniziativa è stata la creazione dell'e-book "Covid-19 il virus della paura"[28], presentato all'AGI da Massimo Tortorella e scritto dall'infettivologo Massimo Andreoni, primario del reparto di malattie infettive al policlinico Tor Vergata di Roma e da Giorgio Nardoni esperto di disturbi fobico-ossessivi, creato principalmente con lo scopo di fornire una giusta informazione e di combattere la cosiddetta "infodemia", ovvero la diffusione di innumerevoli notizie provenienti da molteplici fonti di cui non sempre è verificata la fondatezza e correttezza. Ciò ha creato, come detto in precedenza, un sentimento di sfiducia nell'anima delle persone, le quali non sanno più a chi credere e a chi affidarsi, e che cadono in una condizione di ansia e di paranoia. La popolazione vuole sapere, vuole capire come deve comportarsi e proprio per questo motivo sono stati innumerevoli gli interventi di esperti in ospitate televisive e sugli stessi social media per informare i cittadini nella maniera corretta. È un periodo complicato per tutti, infatti sono aumentati anche i casi di psichiatria e i tentativi di suicidio, proprio per l'impossibilità di capire quali notizie seguire e quali invece eliminare, ed è proprio la paura che ci fa tendere a credere a qualsiasi cosa, nonostante la notizia non provenga da fonti certe o dagli stessi medici.

Le iniziative sono state innumerevoli, le istituzioni si affidano ai cittadini ed essi a loro volta si affidiamo a tutte le norme che regolano la cyber security, affidandosi a tutte le leggi che regolano la protezione dei dati e a tutti gli interventi per garantire la corretta circolazione delle informazioni.

Esso, purtroppo, è un problema che continuerà ad esserci, soprattutto nelle società che ad oggi richiedono un'alta digitalizzazione.

[28]Arcovio, A. (2020) AGI. *Contro lefakenews sul coronavirus arriva un e-book.* 2020. Disponbile in: https://www.agi.it/scienza/news/2020-04-28/coronavirus-covid-19-fake-news-ebook-virus-della-paura-8462004/

3.2. App per il tracciamento del contagio: "IMMUNI" – pro e contro

Dal 4 maggio 2020 l'Italia entrerà nella cosiddetta "fase 2", l'economia inizierà a ripartire e in base al rispetto delle norme riapriranno anche tutte le attività. Ciò che è importante sottolineare, è che la popolazione sarà costretta a convivere con il virus, perciò a mantenere il distanziamento sociale, evitare assembramenti e indossare guanti e mascherine nei luoghi chiusi come per esempio nei supermercati. La nostra vita non tornerà ancora come lo era prima, e proprio per questo sono state proposte delle iniziative per tracciare il contagio e per permettere sia alle istituzioni che ai cittadini la corretta informazione.

È opportuno fare una differenziazione tra le misure prese nel nostro paese e quelle prese dalla Cina[29]. Quest'ultima è stato il primo paese ad affrontare la pandemia ed il conseguente lockdown, sappiamo inoltre quanto la tecnologia sia utilizzata dai suoi cittadini e come questa ha permesso di aiutare il contenimento del contagio, applicandola al campo medico, della sicurezza e della sorveglianza. I cittadini erano tenuti al rientro in casa o all'ingresso a lavoro obbligatoriamente a scansionare il proprio QR code (quick response, che permette la decodifica delle informazioni contenute al suo interno) personale, procedendo alla compilazione di un'autodichiarazione dove venivano indicati i sintomi e tutti i movimenti effettuati fino a quel momento, il tutto ovviamente monitorato dalle autorità competenti. Bisogna prendere in considerazione il fatto che sia un paese dove i cittadini sono abituati al controllo massiccio che il governo attua nei loro confronti, sono abituati a condividere le proprie informazioni personali, i propri spostamenti, perciò quello che l'epidemia ha causato non è qualcosa di nuovo per essi. Un altro aspetto determinante da citare è il fatto che nel momento in cui arrivavano a lavoro essi erano tenuti, nel caso in cui gli fosse richiesto, a fornire tutti gli spostamenti tramite il GPS e la compagnia telefonica di riferimento. Non vi è come in Italia, il problema della privacy del singolo individuo, in Cina viene messo prima di qualsiasi cosa l'interesse nazionale.

Per controllare che effettivamente le persone rimanessero in casa, sono stati attivati droni, megafoni e videocamere ad alta definizione, che controllavano il rispetto di tutte le regole da parte dei cittadini. Gli stessi droni erano in grado di misurare la temperatura degli individui, avvisando chi di dovere in caso di febbre.

In Italia c'è il fenomeno dell'autocertificazione, che qualsiasi cittadino deve portare con sé in caso di spostamenti necessari, e successivamente le autorità devono controllare la validità e veridicità di questi movimenti. In Cina, al contrario, i cittadini hanno un pochissimo se non inesistente contatto con le forze dell'ordine, per evitare che siano anche essi contagiati.

Inoltre, è stata fondamentale l'adozione di un'app specifica per il tracciamento del contagio chiamata "Health Code" di Aplipay, che assegna un colore diverso ad ogni utente, in base alle proprie condizioni sanitarie, che cambia quando il soggetto è stato a contatto con persone che invece hanno un colore che indica

[29]Berti,R. Network Digital 360. (2020) *Coronavirus, come la Cina lo ha fermato con la tecnologia e cosa può imparare l'Italia*. Disponibile in: https://www.agendadigitale.eu/cultura-digitale/coronavirus-come-la-cina-lo-ha-fermato-con-la-tecnologia-e-cosa-puo-imparare-litalia/

il pericolo, ovvero qualcuno che ha contratto il virus. Questo ha fatto in modo che il governo potesse controllare ogni spostamento e che si riducesse la possibilità di creare nuovi focolai di contagio. Questo meccanismo è stato poi adottato nel governo con l'utilizzo di un altro strumento chiamato "close contact detector" che avvisava in tempo reale ogni cittadino che risultasse essere stato a contatto con una persona contagiata.

E ancora, un ulteriore modo per evitare assembramenti è stato trovato in Baidu (uno dei principali motori di ricerca in Cina), che forniva informazioni su quante persone effettivamente si trovavano in un determinato luogo, per evitare che i cittadini si ritrovassero in situazioni ad alto rischio di contagio.

Inoltre, per monitorare tutti coloro che viaggiavano è stata creata la China Eletronics Technology Group Corporation, ovvero un programma online che richiede ai viaggiatori (sia sugli aerei e treni che sui mezzi pubblici) di condividere i propri dati personali e i propri spostamenti per consentirgli di capire se hanno viaggiato con persone malate.

Sono innumerevoli le misure tecnologie attuate, perché il governo cinese ha la necessità di mantenere alto il controllo politico e sociale sulla popolazione, specialmente in un momento d'emergenza come quello che stiamo vivendo.

Anche nei confronti delle fake news si sono delineate delle differenze importanti con l'Italia. In Cina non si vogliono assolutamente accettare critiche al governo, al modo in cui è stato fronteggiato il virus ed al sistema sanitario, quindi non è tanto una lotta la loro quanto una repressione a priori delle notizie considerate dannose dalle autorità. Infatti, vi sono minacce di reclusione per la diffusione di voci infondate, seguite dalla sparizione di moltissime notizie che circolavano sul web e sui principali social media. C'è quindi la volontà di non creare problemi al governo che non ha intenzione di essere giudicato sul proprio operato, tramite il controllo della China cyber security su tutti i mezzi di comunicazione.

È impensabile che queste misure di controllo coercitivo della popolazione da parte del governo, siano possibili da applicare anche in un paese democratico come il nostro. Innanzitutto, perché si è sempre difesa la privacy di tutti i cittadini, ed è impossibile che essi si ritrovino a diventare "sudditi" del governo, delle istituzioni, dei datori di lavoro. Non è possibile monitorare la vita umana tramite i droni che entrano nelle proprie case, non è possibile utilizzare videocamere per il tracciamento dei contagiati. Si può però utilizzare l'esempio della Cina per creare un sistema di controllo conforme ai diritti esplicati e difesi dalla nostra costituzione.

In Europa, così come in Italia si è iniziato a parlare della possibilità di adottare un'app per il tracciamento dei contagi chiamata Immuni, il che ha creato due schieramenti: coloro che sono favorevoli a tale iniziativa e coloro che invece sono totalmente contrari.

Innanzitutto, anche in questo caso l'Unione Europea ha dichiarato la volontà di adottare misure coordinate tra tutti gli Stati membri. Infatti, la Commissione Europea e l'EDPB (European Data Protection Board) si sono accordati per la creazione di un'applicazione per il tracciamento del contagio, che rispetti e

tuteli l'individuo[30]. È importante citare in particolare un importante articolo della Dichiarazione Universale dei Diritti Umani, l'art 7 che esplica che: "*nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua abitazione, nella sua corrispondenza, né a lesione del suo onore della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge, contro tali interferenze o lesioni"*.

La nostra Costituzione invece nell'art 32 esplica che: *"la Repubblica tutela la salute come fondamentale diritto dell'individuo e interesse della collettività…"*. Adesso la domanda è: come si possono coordinare questi due articoli? È bene che si trovi una modalità di tracciamento del contagio per garantire ad ogni individuo il diritto alla salute senza però andare ad intaccare il diritto alla privacy.

È di questo che si stanno occupando le autorità europee e nazionali, che stanno prendendo in considerazione tutte le valutazioni di impatto del caso prima di rendere possibile quest'applicazione, con l'intento di realizzare politiche pubbliche di salute necessarie senza andare ad intaccare la privacy e la vita privata dei cittadini. Quella che ha proposto l'EDPB è un'applicazione di contact tracing che si basa innanzitutto sull'utilizzo di codici anonimi monouso, nessun cittadino qualora decidesse di utilizzarla volontariamente deve essere esposto ad alcun rischio, ed in nessun modo si deve rilevare la sua identità. Infatti, non deve essere utilizzata come mezzo di esclusione o di diffusione di paura e di panico. Al termine di questa fase emergenziale i dati sono e devono essere eliminati in via definitiva.

L'eHealth (sanità elettronica, termine che indica misure informatiche applicate al campo della sanità) Network, agendo in collaborazione con la Commissione, ha pubblicato il 15 aprile 2020 la prima versione del "Toolbox", ovvero dei consigli pratici su come sviluppare correttamente questa tipologia di applicazioni, elaborata secondo tutti i requisiti voluti da ENISA, che sono i seguenti:

- Natura volontaria
- Approvazione dell'autorità sanitaria nazionale
- Tutela della privacy e della sicurezza dei dati
- Interoperabilità dei sistemi a livello transazionale
- Dimissione dei sistemi nel momento in cui il trattamento non sia più necessario.

Inoltre, per avere risultati attendibili riguardanti la curva di crescita dei contagi, l'applicazione dovrebbe essere utilizzata dal 50% della popolazione.

Andiamo a vedere adesso le regole principali richieste dal Toolbox nello specifico:

- Vi è l'obbligo di rispetto dei protocolli di identificazione dei possibili contagi, aggiornandone i contenuti soltanto in termini di vicinanza, distanza, tipo di contatto.

[30] Carbone, M.R. Cybersecurity360. (2020) *Covid-19 e app di contact tracing: le linee guida della commissione UE.* Disponibile in: https://www.cybersecurity360.it/legal/privacy-dati-personali/covid-19-e-app-di-contact-tracing-le-linee-guida-della-commissione-ue/

- L’accesso ai dati è consentito alle sole autorità pubbliche sanitarie e agli istituti che si occupano di tali controlli. L’autorità pubblica sanitaria dovrebbe, in caso di positività, autorizzare l’app a notificare il contagio, in base al rischio e alla vicinanza del contatto, senza rilevare l’identità della persona divenuta positiva al virus.
- L’applicazione deve garantire il rispetto della privacy, eliminando tutti i dati definitivamente in seguito alla conclusione dell’epidemia.
- Gli ID registrati dovranno essere anonimi e randomici e cambiare ogni volta.
- I protocolli dovranno essere comuni in tutti gli Stati membri, per rendere possibile alle Autorità nazionali un’azione coordinata per sconfiggere il virus.
- Si dovranno rispettare tutte le misure di sicurezza indicate da ENISA, e spiegate nei capitoli precedenti, specialmente per quanto riguarda la trasparenza da parte delle autorità nei confronti dei cittadini.
- L’applicazione dovrà essere volontaria e temporanea e nessun cittadino potrà incorrere in sanzioni o limitazioni nel caso in cui decidesse di non utilizzarla.
- Si dovranno trovare delle soluzioni per la cosiddetta categoria degli “esclusi digitali”, nella quale rientrano bambini, anziani e lo stesso personale sanitario (che non usa il cellulare durante l’orario di lavoro). Si è pensato a tal proposito a dispositivi indossabili senza l’utilizzo del proprio cellulare.

In sintesi, ciascun cittadino potrà decidere se scaricare o meno l’applicazione, e nel caso in cui risultasse positivo egli potrà decidere di condividere i propri dati con essa, rendendo possibile alle autorità competenti la ricostruzione dei contatti che ha avuto nell’ultimo periodo e il livello di pericolosità di essi. Il cittadino avvertirà le autorità che a loro volta forniranno un “codice di sblocco” per avvertire tutte le persone con cui ha avuto recentemente dei contatti.

Successivamente, verranno avvertite tutte le persone con cui questa persona ha avuto dei contatti, che saranno tenute obbligatoriamente a rispettare l’isolamento nella propria abitazione, e non potranno così in nessun modo uscire senza incorrere in una sanzione.

Come avviene però il tracciamento? Una volta scaricata l’applicazione, essa genererà un codice temporaneo, che verrà scambiato attraverso la modalità del Bluetooth con i codici degli altri, nel caso in cui non sia rispettata una distanza consona ad evitare il possibile contagio.

Inoltre, IMMUNI ha anche un’altra caratteristica che è quella di costituire una sorta di “diario clinico”, dove ciascuna persona potrà inserire patologie pregresse o sintomi legati al COVID-19. Queste informazioni per il momento sembrerebbero essere salvate solo sul cellulare della persona interessata e non condivisa con le autorità.

Nonostante ci si avvicini all’attivazione di quest’applicazione sono ancora tantissimi i dubbi inerenti alle sue funzionalità, ad esempio non è ancora chiaro come funzionerà il codice di sblocco. Sono molte le domande che i cittadini si pongono, come ad esempio: una volta che si è venuti a conoscenza di essere stati a

contatto con una persona risultata positiva, si ha diritto al tampone? E soprattutto come avverrà la comunicazione alle autorità sanitarie?

Inoltre, si hanno dubbi sulla tempestività delle comunicazioni, che è sicuramente un fattore importante inerente alla guarigione del soggetto interessato.

Ma ciò che ci interessa maggiormente in questo ambito è chiarire se effettivamente verranno rispettati tutti i requisiti della privacy, quindi se i codici saranno effettivamente anonimi con nessuna possibilità di risalire all'identità degli utenti, se queste informazioni saranno protette limitando l'accesso alle sole persone competenti e infine ci si chiede se alla fine dell'emergenza queste informazioni verranno veramente eliminate dal principio.

Abbiamo visto nei capitoli precedenti che, nonostante tutte le misure adottate, la possibilità di ricevere attacchi informatici rimane molto alta e non ci deve essere quindi il rischio di mettere in pericolo le persone che decideranno di usufruire di questo meccanismo.

Il governo dovrà fare chiarezza su tutti questi aspetti ed i cittadini dovranno sentirsi liberi e sicuri di utilizzare questa nuova modalità di tracciamento del contagio, soprattutto perché essa non deve essere il motore di comportamenti illeciti ed illegali e non deve essere l'origine di comportamenti discriminatori verso tutti coloro che purtroppo contrarranno il virus.

Conclusioni

Questo studio voleva dimostrare l'importanza che la sicurezza informatica ha acquisito nel tempo e nelle nostre società, partendo dall'analisi dei meccanismi di funzionamento e di difesa a livello europeo e nazionale.

È necessario infatti che i diritti fondamentali di tutti gli esseri umani siano difesi e tutelati anche nell'utilizzo delle piattaforme online, per far si che esse non diventino mezzi di diffusione di odio, razzismo e bullismo. Infatti, abbiamo visto che nella vita di tutti i giorni gli individui si trovano ad utilizzarle per qualsiasi motivo, che può essere un'e-mail o la condivisione di fotografie e video sui social network. In tutti questi aspetti, loro devono sentirsi sicuri e i dati devono rimanere personali e protetti.

Il caso di Facebook è stato fondamentale per spiegare come attraverso poche e semplici mosse gli individui leghino i propri dati all'utilizzo di quest'applicazione. Infatti, molte volte gli utenti scaricano applicazioni collegate a Facebook accettando di condividere inconsapevolmente i propri dati. Anche per quanto riguarda le inserzioni pubblicitarie che appaiono sulla home, esse sono legate alle ricerche effettuate dagli utenti su altri motori di ricerca o da ciò che lo smartphone sente durante il giorno. Questo è spaventoso e pericoloso, soprattutto per chi intende utilizzare queste informazioni non a scopo pubblicitario ma per commettere azioni illecite ed illegali.

Nell'ultimo capitolo ho poi parlato delle conseguenze sanitarie, economiche e sociali del Coronavirus. In un periodo dove non era possibile vedersi ed uscire, la tecnologia ha aiutato tutti a rimanere in contatto e a sentirsi meno soli, con videochiamate e messaggi ad esempio. La mia attenzione è ricaduta principalmente sulla nuova sfida digitale che questo virus ha causato: gli adulti si sono ritrovati a lavorare da casa in modalità smart working e tutti gli studenti invece si sono visti costretti a seguire le lezioni online ed a sostenere gli esami da casa. I pericoli che nascono da queste nuove attività riguardano specificamente la protezione dei dati personali e aziendali. Infatti, sono cresciuti gli attacchi informatici ad aziende, utenti e ad ospedali, per rubare dati ed informazioni.

Inoltre, essendo un virus estremamente contagioso le autorità hanno pensato a come contenere il contagio con la creazione dell'applicazione Immuni. Essa ha creato non poche polemiche, tante infatti sono state le domande dei cittadini: è sicura? Protegge i dati? Rispetta la privacy e i principi democratici? Secondo l'opinione di molti infatti, si dovrebbe trovare un modo per proteggere contemporaneamente il diritto alla salute ed il diritto alla privacy.

Per concludere il mio elaborato posso dire con estrema consapevolezza che il percorso per una maggiore sicurezza informatica è iniziato da diversi anni ma richiede ancora numerosi e dettagliati interventi per far si che anche il campo dell'informatica sia sicuro e tutelato dalla legge.

Sitografia

Agenzia Europea per la sicurezza delle reti e dell'informazioni. (2004) Disponibile in: https://www.agendadigitale.eu/sicurezza/cybersecurity-act-ecco-cosa-ci-aspetta-dopo-la-direttiva-nis/

Arcovio, A. (2020) AGI. *Contro le fake news sul coronavirus arriva un e-book.* 2020. Disponbile in: https://www.agi.it/scienza/news/2020-04-28/coronavirus-covid-19-fake-news-ebook-virus-della-paura-8462004/

Baldoni, R., De Nicola, R. e Prinetto, P (2018) *Il futuro della cyber security in Italia: Ambiti Progettuali Strategici.* Roma. Cyber security National Lab. Disponibile in: http://doc989.consiglioveneto.it/oscc/resources/Libro-Bianco-2018.pdf

Berti,R. Network Digital 360. (2020) *Coronavirus, come la Cina lo ha fermato con la tecnologia e cosa può imparare l'Italia*. Disponibile in: https://www.agendadigitale.eu/cultura-digitale/coronavirus-come-la-cina-lo-ha-fermato-con-la-tecnologia-e-cosa-puo-imparare-litalia/

Bulger, M., Davison, P. (2018) *The Promises, Challenges, and Futures of Media Literacy.* Disponibile in: https://digital.fundacionceibal.edu.uy/jspui/bitstream/123456789/227/1/DataAndSociety_Media_Literacy_2018.pdf

Carbone, M.R. Cybersecurity360. (2020) *Covid-19 e app di contact tracing: le linee guida della commissione UE.* Disponibile in: https://www.cybersecurity360.it/legal/privacy-dati-personali/covid-19-e-app-di-contact-tracing-le-linee-guida-della-commissione-ue/

Commissione Europea. (2020) *Combattere la disinformazione.* Disponibile in: https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/fighting-disinformation_it

Comunicazione congiunta al Parlamento Europeo e al Consiglio. (2016) *Quadro congiunto per contrastare le minacce ibride: La risposta dell'Unione Europea.* Bruxelles. Disponibile in: *https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52016JC0018&from=en*

Cyber security act, adopted by the European Commission. (2017) Disponibile in: https://ec.europa.eu/digital-single-market/en/news/cybersecurity-commission-scales-its-response-cyber-attacks

Cyber Security 360. *Coronavirus, nuovo attacco spear phishing per rubare i dati personali: i dettagli*. (2020) Disponibile in: https://www.cybersecurity360.it/nuove-minacce/coronavirus-nuovo-attacco-spear-phishing-per-rubare-dati-personali-i-dettagli/

Cyber security Technology & Capacity Building. (2020) *Cyber Security.* Disponibile in: https://ec.europa.eu/digital-single-market/en/cyber-security

Decreto del presidente del Consiglio Gentiloni. (2017) Disponibile in: https://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/dpcm-17-febbraio-2017.html

Dipartimento per le politiche europee. (2018) *Disinformazione online, codice di condotta per le piattaforme digitali*. Disponibile in: http://www.politicheeuropee.gov.it/it/comunicazione/notizie/disinformazione-online-codice-di-condotta-per-le-piattaforme-digitali/

Direttiva (UE), 2000/31 del Parlamento europeo e del Consiglio. Disponibile in: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32000L0031&from=EN

European Union's Horizon 2020. (2020). *Dialogue About Radicalisation and Equality.* Disponibile in: *http://www.dare-h2020.org*

Gennari, L. (2020) *Coronavirus, gli ingegneri contro gli attacchi informatici: 10 consigli.* Disponibile in: https://www.firstonline.info/coronavirus-gli-ingegneri-contro-gli-attacchi-informatici-10-consigli/

La Stampa. (2020) *Sorpresa la disinformazione su Facebook si può combattere*. Disponibile in: https://www.lastampa.it/tecnologia/idee/2020/04/16/news/sorpresa-la-disinformazione-su-facebook-si-puo-combattere-1.38725713

Liang, Q., Xiangsui, W. (1999). *Unrestricted Warfare.* Pechino. PLA Lettere ed Arti Casa Editrice

*Lotta alla disinformazione online: proposta della Commissione di un codice di buone pratiche dell'UE. (*2018). Bruxelles. Disponibile in: https://ec.europa.eu/commission/presscorner/detail/it/IP_18_3370

Manietti, E. (2018) *Il caso Cambridge Analytica, spiegato bene.* Disponibile in: https://www.ilpost.it/2018/03/19/facebook-cambridge-analytica/

Perché Facebook sta perdendo la battaglia contro l'Isis e il terrorismo online. (2019). Disponibile in: https://www.wired.it/internet/social-network/2019/05/14/facebook-isis-terrorismo/

Raccomandazione (UE), 2018/334 della Commissione Europea sulle misure per contrastare efficacemente i contenuti illegali online. Disponibile in: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32018H0334&from=FR

Repubblica. (2020) *Nasce Covid19Italia.help: un sito non profit per combattere fake news e disinformazione.2020.* Disponibile in: https://www.repubblica.it/cronaca/2020/03/22/news/nasce_covid19italia_help_un_sito_non_profit_per_combattere_fake_news_e_disinformazione-251981708/

Russo, F. (2020) *Social Media in Italia: ecco alcuni dati per il 2020.* Disponibile in: https://www.franzrusso.it/condividere-comunicare/social-media-italia-dati-2020/

Schiaffino, M. (2020) *Smart working: perché la prima preoccupazione dev'essere la cyber security*. Disponibile in: https://www.cybersecurity360.it/soluzioni-aziendali/smart-working-perche-la-prima-preoccupazione-devessere-la-cyber-security/

Sol, P. (2020) *Coronavirus, attacco hacker allo Spallanzani di Roma. Indaga la procura.* Disponibile in: https://www.ilsole24ore.com/art/coronavirus-attacco-hacker-spallanzani-roma-indaga-procura-roma-ADtLHTH?refresh_ce=1

Statistiche e fatti di Facebook. (2020). Disponibile in: https://www.websitehostingrating.com/it/facebook-statistics/ ; https://investor.fb.com/investor-events/default.aspx

The Directive on security of network and information systems (NIS Directive) adopted by the European Parliament. (2016). Disponibile in: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

The Guardian. (2019). *Revealed: catastrophic effects of working as a Facebook moderator.* Disponibile in: https://www.theguardian.com/technology/2019/sep/17/revealed-catastrophic-effects-working-facebook-moderator

Unesco, *Media and information literacy curriculum fot teachers.* Disponibile in: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/media_and_information_literacy_curriculum_for_teachers_en.pdf

Abstract

"CYBER SECURITY IN EUROPE AND THE COOPERATION BETWEEN PUBLIC AND PRIVATE SECTORS"

Index

Introduction…….....p.2

Chapter 1: "The European legal framework on cyber security"

1.1.Why the phenomenon is relevant at the European level……..…..…..p.3
1.2 Directive NIS (2016)……...p.4
1.3 ENISA…….....p.5
1.4 Illegal content on online platforms, communication from the European commission…….....p.7
1.5 Fake news phenomenon…….....p.8
1.6 Italian Legislation…….....p.12

Chapter 2: **"Study case on Facebook"**

2.1. Rules for the use of Facebook and its control mechanisms…….....p.15
2.2. Statistics, videos, offices…….....p.17
2.3. Facebook criticism…….....p.17
2.4. Extremism in Europe…….....p.19
2.5. Psychological impact on operators…….....p.21

Chapter 3: "Coronavirus: the new digital challenge"

3.1. Coronavirus: why it is not just a health problem……..…..…..p.23
3.2. App for the contagion tracking: "IMMUNI" in Italy, pros and cons…….….p.28

Conclusions…….....p.33
Sitography…….....p.34
Abastract…….....p.37
Thanks…….....p.43

Introduction

This thesis intends to clarify the characteristics, functions and mechanisms of cyber security, i.e. the defense of all electronic devices, servers, networks, online sites and data of any kind. It is an important topic in the political-cultural context of our societies, where technologies bring great benefits such as greater communication between the various countries and the exchange of information, but which can carry risks such as that of cyber-attacks.

In particular, the interventions, directives and regulations of the European Union and Italy will be analyzed, considering Facebook as a case study, and all possible risks that individuals face, from sharing illegal content to the spread of fake news.

The goal of this work is to demonstrate the importance of this discipline, of protecting the data of users, citizens and countries in an increasingly digitalized world. I decided to talk about this topic because I think individuals must know the subject and that there must be good information; I believe that the protection of fundamental rights must also be recognized on these platforms, such as the right to privacy and the freedom of expression and opinion.

In the first chapter I talk about the 2016 NIS (Network and Information Security) directive which requires all EU Member States to adopt common measures to contrast cyber-attacks, and the role of ENISA (European Network and Information Security Agency), the European agency created with the aim of making European telecommunication networks more secure.

In the second chapter I analyze the Facebook case study, explaining its operation and the mechanism of user data protection.

In the third chapter I deal with the issue of Covid-19, a virus that started off in China and spread quite quickly all around the world, causing enormous health, economic and social consequences underlining the need to strengthen the online security. A perfect example of this conflict of interests (health on one side and privacy on the other) is the bran new “Immuni App” created to keep the contagion under control and prevent the spread of the virus by facilitating the social distancing. At the same time though, this App clashes with the other very important interest such as the one of the right to privacy.

Chapter 1: “The European legal framework on cyber security”

This chapter describes the European legal framework on cyber security. In fact, while it has brought us many advantages, such as greater communication between countries and an unlimited exchange of information, it has also highlighted quite few risks, such as cyber-attacks that fall within the category of "hybrid threats".

To deal with all this, the European Union has issued the joint communication to the Parliament and the 2016 European Council, which lists the responses to counter these threats, such as the creation of an EU cell aimed at studying strategies for the repression of cyber-attacks.

In this regard, it is important to mention the 2016 NIS directive which represents the first European regulation in the field of IT security. It aims to strengthen the role and mandate of ENISA (European Network and Information Security Agency) and to create a common framework for IT security certification of ICT products and digital services, proposing schemes that however are not directly operational but must first be programmed by ENISA and the European Commission with executive acts.

Furthermore, the European Commission in 2017 has adopted an IT security package, which contains an important regulation: the Cyber Security Act, that includes important rules governing European certification schemes.

As for ENISA, established in 2005, it initially had a temporary mandate and had the role of technical consultancy for states and institutions. In 2016, it received a permanent mandate with the important role of supporting the management of IT incidents, accompanied by the CSIRT, the national team network that acts as a site where users write opinions and experiences.

Another important topic is the battle against illegal material posted on the online platforms. Being able to be used by anyone, they can become a vehicle for the spread of bullying, racism and violence and therefore become very dangerous. Until 2017, EU Directive 31 of 2000 was in force, which did not give providers the obligation to monitor content. Subsequently, in 2018, a recommendation was made by the European Commission with which the providers were made responsible for what was published by third parties.

The European Union has decided to act also in the field of disinformation and fake news, which can become dangerous for the stability of the countries themselves, by approving a Code of Conduct with the aim of self-regulating, through a voluntary signature by the Member States, the use of platforms and social networks. The goal is to make websites more transparent by eliminating fake accounts and controlling advertising and privacy.

However, citizens are also required to collaborate; they must be aware of the risks they face when using the Internet, especially the categories of the elderly and children. For this reason, the European Union has introduced the "European media literacy week", to ensure that all those who use the platforms are aware of its operating mechanisms, the dangers and the benefits and have therefore the knowledge to contrast the disinformation.

Human rights, such as freedom of expression and opinion, must also be protected online and it is for this reason that UNESCO supports Media Literacy and Information (MIL), which promotes the individuals' right to communicate freely their own ideas on platforms but this right must be accompanied by an exhaustive knowledge of online platforms.

This process is organized around five main themes: youth participation, teacher training, parent support, policy initiatives and evidence building.

Our country has adopted the European NIS directive in 2013 with the creation of five ministries: health, environment, economy, infrastructure & transportation and economic development. In 2017, with the DPCM Gentiloni, even more importance was given to the matter. In fact, an important role was given to the DIS (Department of Security Information) which, linked to the EU and the Member States, coordinates the various activities and develops strategies.

Two other important initiatives of this decree are the creation of the Cyber Security Unit and the national evaluation and certification center for the control of products and devices.

With specific regard to the right of privacy, with this decree the GDPR legislation of 2018 was approved, i.e. the General Regulation on data protection, in which the principle of "data protection by design" applies meaning that data protection must be taken into consideration since the very first creation of the various systems.

Chapter 2: “Study case on Facebook”

I have analyzed the case of Facebook to investigate its use and its characteristics, being one of the most important digital platforms in the world. In fact, it has 29 million users registered in our country and is used every day by the majority of the population to stay in touch with the rest of the world by sharing photographs, thoughts and opinions; for this reason it is necessary that all the measures I have mentioned in chapter 1 are respected and applied.

Facebook does not receive money for user registration, but rather receives compensation from the companies with which it agrees for the insertion of their advertisements that are then included in the Home page based on the study that is done on users and their interests.

The user has the obligation to use his / her name and surname when registering into Facebook, but despite numerous checks, there are still fake accounts, used for the purpose of divulging illegal material, committing scams online or stealing personal information. In this regard, the platform declares to collect information from people's private profiles to improve their products and not to abuse private content.

The scandal that hit Facebook in 2018 was the so-called case of “Cambridge Analytica”, an online marketing consulting company that deals with analyzing consumers data, adapting it to behavioral science and creating highly personalized advertisements for each individual through algorithms. It examines how many likes a particular user puts to which contents and from where. Through the use of online platforms, each of us leaves information on them, and it is in fact very easy to trace, for example, the position from which we share a post, thus causing significant dangers. The accusation against Facebook started from an application called "this is your digital life", created by a Cambridge researcher, Aleksandr Kogan. Users could access it through the Facebook login, agreeing to share data with it such as e-mail address, age and gender. But along with the user’s information, also the information of the subscribers’ friends were taken (stolen) without their approval.

This application decided to share the stolen information with Cambridge Analytica, and much of the data was used for Donald Trump's election propaganda in the US, spreading fake news against Hilary Clinton. Same thing was done for Brexit.

This experience has made evident the extreme easiness with which Facebook users are stolen personal data and the incredible diffusion of fake news through it. As regards the latter area, the European Commission has undertaken to create a code of good practices on disinformation, an independent European network of fact-checkers, a secure online EU platform on disinformation, promoting media literacy and awareness raising activities to counter this phenomenon.

Another problem is the diffusion on this platform of material aimed at the dissemination of extremist movements, used to recruit young people or easily influenced people. Social networks are channels through which extremism is trying to spread in Europe. Its content is often eye catching such as videos, cartoons, articles of satire. For this reason, the European Union has decided to support, within the "Horizon 2020 framework", the DARE (Dialogue about Radicalization and Equality) project which includes 17 partners in 13 European countries. The goal is to analyze the behavior and choices of young people, examining the channels where they express their messages and make a psychological study to understand why they tend to extremism.

In recent years Facebook has committed itself to contrasting these phenomena with the intervention of human supervision and for this reason I have analyzed the impact that these contents have on staff. In a study done by "The Guardian", many workers said they were shocked and frightened by everything they were forced to watch all day. These people have their own interests, political ideas and they too can be influenced by what they see or read, such as conversations between adults and sexually motivated children. In fact, many workers later had psychological problems, fear of returning home. For this reason, they must be protected, because they do an important job that can become quite dangerous.

In 2016 Facebook unintentionally disclosed personal information about these people, who started receiving messages and requests for friendship on their profiles, creating a danger for their families too. We must recognize the attention that Facebook has had for all these issues but it must also be said that the right protection of users and workers has not yet been reached.

Chapter 3: “Coronavirus: the new digital challenge”

Our country has found itself facing an unprecedented challenge: covid-19, an infectious respiratory disease that started off in China and has caused important health, economic and social consequences. Italy has been forced to stop the economy and shut citizens at home with a very severe lockdown policy; it is in this emergency situation that cyber security has acquired even more importance. The students had to take lessons and exams online and the employees started smart-working from home. This has brought privacy issues to the surface, both with regard to personal data and company data. Since the beginning of the pandemic, cyber-

attacks have also increased against healthcare facilities, also due to the fact that by working from home each individual used the same device both to work and to use applications, such as social networks.

Even in the case of videoconferencing and video lessons, there is no complete certainty of being protected. For this reason, the GDPR today has acquired even more relevance and has also required a coordinated response from citizens, who have been invited by the authorities to maintain high attention.

For example, data stolen from hospitals was used both to create scam emails and to scare citizens by spreading fake news and creating general panic. In fact, the government was forced to ask to the population to listen only to the official news coming out from the official channels, and in this regard, the "Covid19italia.help" was created to disseminate the correct information, to raise the necessary funds for this emergency and to unite citizens in this difficult moment. Subsequently, the e-book "Covid-19 the virus of fear" was written by the infectious disease specialist Massimo Andreoni together with psychologist Giorgio Nardone was presented to the AGI by Massimo Tortorella; the book has been written with the aim of counteracting the so-called "infodemic", i.e. the dissemination of information from multiple sources whose reliability is not always verified.

The institutions rely on citizens and citizens rely on the rules that regulate cyber security.

Another central topic of this last period is the creation of applications aimed at tracing the contagions of the Coronavirus. They were first adopted by China, which we know is a country that has always controlled citizens through technology, and which on this occasion simply had to strengthen the mechanisms. In fact, it forced citizens to scan their QR code when entering to work and to provide all private travel via GPS if necessary. In addition, to check that people were really at home, they used drones that entered private homes or high definition cameras. Finally, it was created the "Health Code" application that assigns a color to each user based on their health conditions; the color changes when the subject comes into contact with people who instead have a color that indicates danger, i.e. an infected person.

The Chinese government therefore has full political and social control over the population, and this also concerns the spread of fake news. In fact, it does not accept criticism of any kind and threatens imprisonment for all those who spread unfounded news.All these measures, however, are not compatible with European and democratic countries like ours.

For this reason, our government thought of creating an application, called "Immuni" which respects the fundamental human rights. Each citizen will be able to decide whether to download it or not, and if it proves that the given individual is positive, he/she can decide whether to declare it, making it possible for the competent authorities to reconstruct the contacts he/she has had in the last period. This application is anonymous and does not take personal information, such as the position via GPS and, at the end of this health emergency, the application will be deleted and with it all the data within it.

So how does the tracking take place? Once the application has been downloaded, it will generate a temporary code, which will be exchanged via Bluetooth with the codes of the others, if the safety distance is not respected.

There are many doubts about this application. For example: once we are warned that we have been in contact with a positive person, are we entitled to a swab? And, above all, how will communication to health authorities take place? Will the codes remain anonymous?

The government will have to clarify all these aspects and citizens will have to feel free to download it and communicate a possible positivity to the virus without fear of discriminatory attitudes.

Conclusions

This study wanted to demonstrate the importance that IT security has acquired over time in our societies, starting from the European and Italian frameworks.

Fundamental human rights must be protected also on online platforms. All individuals must feel safe and free to publish photographs, videos and content, and the Internet must not be used as a channel for spreading hatred, violence, racism and extremism.

The Facebook case has highlighted the problems related to the use of social networks with regards to privacy and personal information, explaining how easy it is to trace the interests of each individual with the creation of specific advertisements, while the chapter on Covid- 19 revealed how important technology is today and with it cyber security.

I can therefore say with extreme awareness that the path to greater safety in this field has started several years ago but still requires numerous interventions to ensure that this field is also protected by law.

Ringraziamenti

In quest'ultima pagina vorrei ringraziare tutte le persone che mi sono state vicine e che hanno contribuito alla mia crescita professionale e personale.
Ringrazio il professor Michele Sorice per avermi guidata e supportata in ogni momento per tutta la stesura della tesi.
Un grazie immenso alla mia famiglia che mi ha permesso di studiare e mi ha sostenuta ed incoraggiata a fare sempre meglio.
Alle mie amiche, compagne di studio, di ansia ma soprattutto di vita: Arianna, Benedetta, Giuliana, Marisa e Martina. Grazie per avermi accompagnata in questo percorso difficile ma indimenticabile.

Infine, dedico questo traguardo alle mie nonne che oggi sarebbero state sicuramente fiere di me.

Francesca Uricchio