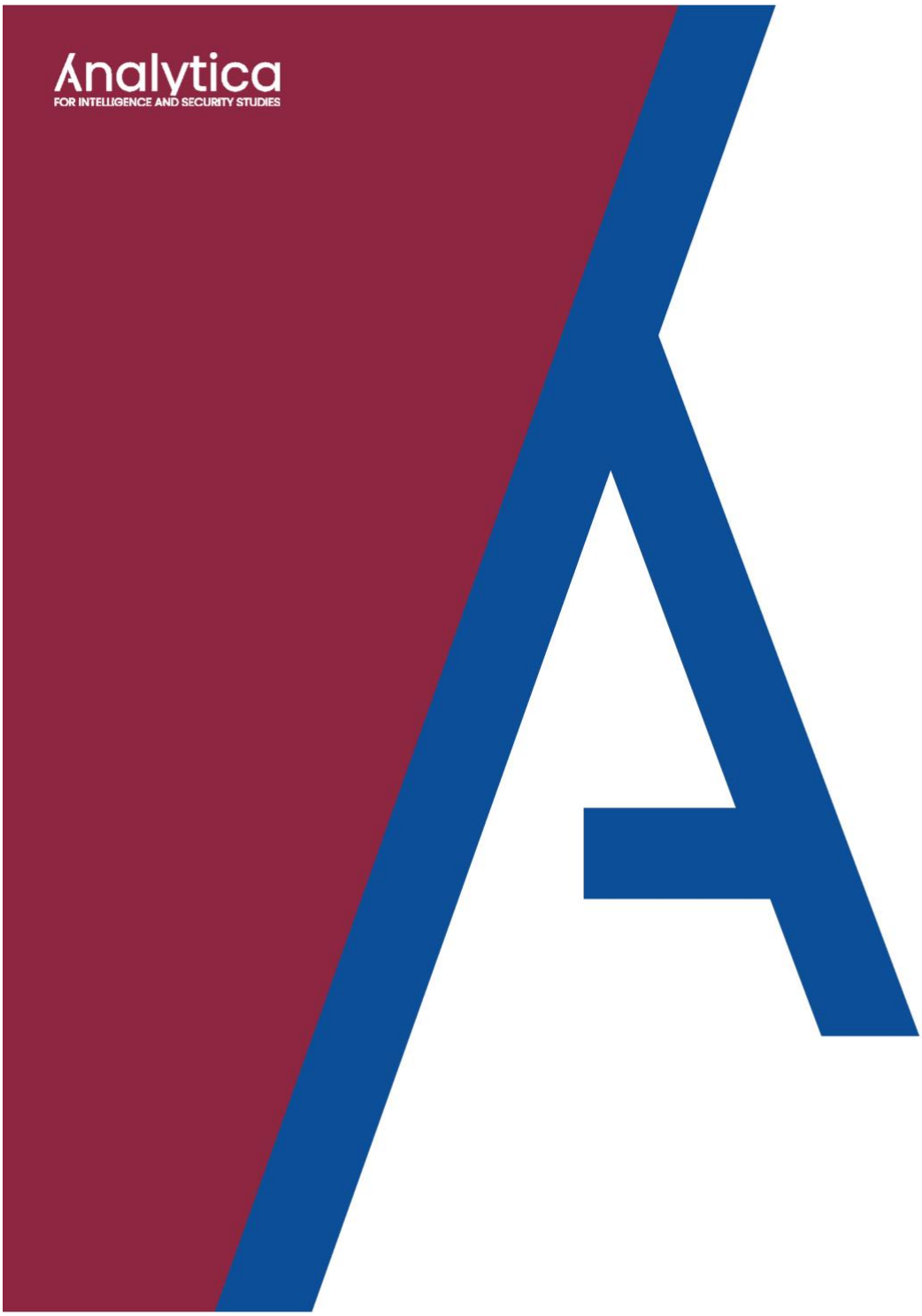

Covid-19: tra sorveglianza di massa e privacy

Giulia Molinari

Analytica for intelligence and security studies

Paper Cyber-Security

ISSN: 2784-8779

Covid-19:tra sorveglianza di massa e privacy

Giulia Molinari

Correzioni e revisioni a cura del Dottor SPELTA Maurizio

Direttore del Dipartimento Cyber - Security

Torino, luglio 2021

Introduzione

La fine del 2019 verrà ricordata per un evento che ha segnato in modo indelebile la storia mondiale: l'ufficio nazionale dell'Organizzazione Mondiale della Sanità nella Repubblica Popolare Cinese

riporta la notizia diffusa dai media di alcuni casi di "polmonite virale" a Wuhan. 10 giorni dopo, le autorità cinesi identificano la sequenza del nuovo coronavirus, o SARS-CoV-2. È solo l'inizio di ciò che poi nel giro di poche settimane evolverà in pandemia, interessando l'intera popolazione globale.

Secondo i dati rilasciati dalle autorità cinesi riportati sul sito dell'OMS[1], i casi registrati[2] in Cina sarebbero 103.759 di cui 4.858 deceduti. Molti dubbi sono però sorti non appena il virus si è diffuso oltre i confini, facendo impennare la curva dei contagi soprattutto negli Stati Uniti, in Italia e in Spagna: in questi paesi, nonostante siano di dimensioni ben più ridotte rispetto alla Cina, si sono registrati molti più casi. Un articolo pubblicato da Bloomberg[3] ad aprile 2020 rivela infatti che l'Intelligence americana abbia le prove che Pechino intenzionalmente non sia stata trasparente nella comunicazione dei dati relativi ai contagi e ai decessi. Inoltre, le accuse mosse dalla CIA contro la Cina includono anche l'incompletezza delle informazioni relative al virus e al trattamento della malattia che avrebbero rallentato e reso meno efficace la risposta negli altri stati. L'allora Presidente degli USA Donald Trump sostenne proprio che la colpa delle difficoltà nella gestione dei contagi riscontrate dagli Stati Uniti fosse da attribuire all'opacità dei dati rilasciati da chi per primo aveva identificato il virus.

Nonostante l'incompletezza e la mancanza di trasparenza nei dati comunicati dalle autorità cinesi, è evidente che il governo di Pechino abbia gestito in modo molto diverso rispetto alle democrazie liberali il tracciamento dei contagi. Secondo Talha Burki[4], l'efficacia della risposta è dipesa largamente dal concetto di libertà civili della nazione poiché, come affermato da Gregory Poland, direttore del Vaccine Research Group alla Mayo Clinic di Rochester, Minnesota, il governo cinese ha potuto "implementare maggiori restrizioni alle libertà individuali che la maggior parte dei paesi occidentali non avrebbe considerato accettabili".

Efficacia e rapidità sono dunque i due aggettivi che meglio descrivono la gestione cinese dei contagi, ma quale prezzo ha pagato la popolazione? A quante libertà e diritti ha dovuto rinunciare per far sì che dopo soli 9 mesi dall'inizio dell'epidemia si potesse partecipare ad una festa a Wuhan?

---

[1] https://www.who.int/countries/chn/

[2] al 7 maggio 2021.

[3] https://www.bloomberg.com/news/articles/2020-04-01/china-concealed-extent-of-virus-outbreak-u-s-intelligence-says

[4] Talha Burki, China's successful control of COVID-19, The Lancet Infectious Diseases, November 2020.

Il presente paper vuole fornire una panoramica in merito all'impiego di sistemi di Intelligenza Artificiale (IA) per la sorveglianza di massa per il tracciamento dei contagi da Covid-19 e le lesioni di libertà individuali e privacy.

Prima verrà delineata l'attuale situazione relativa ai controlli implementati dal governo cinese e di come queste limitazioni si siano dimostrate efficaci per arginare la diffusione del virus. Successivamente, verrà portata alla luce l'altra faccia della medaglia, ossia gli effetti della pandemia sul controllo della popolazione da parte del governo di Pechino. Per concludere, infine, verrà proposto un confronto con l'approccio europeo al tracciamento dei contagi e i recenti sviluppi in merito alle norme per l'utilizzo dell'intelligenza artificiale.

1. Cina: digital authoritarianism

Il PCC, il Partito Comunista cinese, ha da tempo implementato nel proprio regime un sistema di autoritarismo digitale, ossia l'impiego di tecnologie digitali al fine di esercitare una forma di controllo e manipolazione sulla popolazione. La componente digitale di tale regime include tecnologie di ultima generazione come il machine learning[5] e la big data analytics[6] per aggregare ed elaborare i dati biometrici dei cittadini raccolti attraverso sistemi di riconoscimento facciale e sorveglianza di massa attuata attraverso una rete di più di 200 milioni di telecamere CCTV posizionate in luoghi pubblici. A fianco di questo controllo offline, il PCC esercita anche un'importante censura della vita online, definita "cyber sovereignty", ovvero la capacità di uno stato di controllare l'accesso a internet e ai social media all'interno dei propri confini nazionali. Il regime cinese di sorveglianza di massa viene esercitato con il dichiarato scopo di contrastare i 3 pericoli peggiori per la società, ossia separatismo, estremismo e terrorismo. Proprio in nome della lotta al terrorismo, inoltre, nella regione dello Xinjiang ci sono diversi centri di rieducazione dove milioni di musulmani (uiguri, kazaki, uzbeki, kirghisi) sono detenuti semplicemente per aver fatto crescere la barba o per aver frequentato troppo assiduamente la moschea.

Per quanto riguarda invece la sempre più ampia diffusione degli strumenti di riconoscimento facciale, il PCC vuole creare un modello di smart city da esportare in tutto il mondo attraverso sistemi come "SkyNet" per la sorveglianza del traffico urbano e la crowd analysis[7], o "SharpEyes"

[5] In italiano "apprendimento automatico". Si tratta di "meccanismi che permettono a una macchina intelligente di migliorare le proprie capacità e prestazioni nel tempo". Fonte: https://www.intelligenzaartificiale.it/machine-learning/

[6] Si intende il "processo che include la raccolta e l'analisi dei big data [grandi quantità di dati] per ottenerne informazioni utili". Fonte: https://www.zerounoweb.it/analytics/big-data/come-fare-big-data-analysis-e-ottenere-valore-per-le-aziende/

[7] Si intende l'interpretazione dei dati relativi allo spostamento delle persone in gruppo. Si utilizza questo tipo di analisi per identificare dei pattern utili a prevedere i movimenti futuri.

per collegare apparecchi dell'Internet of Things (IoT)[8] della vita di tutti i giorni con le reti di sorveglianza pubblica. Attualmente la Cina vanta il più vasto apparato di sorveglianza del mondo e ambisce a diventare il leader globale nello sviluppo dell'IA e del riconoscimento facciale per la creazione di un sistema digitale di controllo sociale attraverso l'uso di algoritmi.

Il sistema di autoritarismo digitale cinese è stato definito da Ross Andersen[9] un "digital panopticon", ovvero un panottico digitale, nel quale ogni individuo è costretto a mantenere un comportamento corretto in ogni istante della quotidianità, condizionato dalla sensazione di un costante e ubiquo controllo da parte del regime. Uno strumento adottato dal PCC a partire dai primi anni 2000 e gradualmente migliorato grazie alla tecnologia è il Sistema di Credito Sociale (SCS). Ad oggi l'SCS consiste in un modello di machine learning che aggrega dati finanziari e non, come transazioni ed estratti conto, ma anche fedina penale, informazioni personali, dati biometrici e viaggi, per valutare ogni individuo con un punteggio che gli assegnerà sanzioni o ricompense. Con la diffusione sempre più ampia di telecamere e forme di controllo digitale, ogni cittadino sa ormai che ogni sua azione deve essere ragionata in funzione dell'esito che potrebbe avere sul proprio punteggio personale.

2.1 Impatto del coronavirus sul digital authoritarianism

La crisi portata dalla pandemia da coronavirus alla fine del 2019 ha richiesto una risposta immediata per arginare la diffusione dei contagi. Fin dai primi casi di infezione da Covid-19, si può riscontrare la censura severa del regime cinese contro quelle che vennero definite informazioni false che diffondevano il panico infondato. Il Dott. Li Wenliang pubblicò online il primo report della collega Dott.ssa Ai Fen che identificava il SARS-CoV-2 come causa delle numerose polmoniti virali che si stavano verificando a Wuhan, nella provincia di Hubei, a dicembre 2019. Il documento venne prima censurato da tutte le piattaforme online e successivamente il Dott. Li venne detenuto per aver scatenato inutilmente la paura. Ai medici di Wuhan venne perfino vietato l'uso di dispositivi di protezione personale come le mascherine per non allarmare la popolazione. Il Dott. Li morì il 7 febbraio 2020 proprio a causa del coronavirus che lui stesso aveva contratto. Fin dai primi casi di Covid-19, dunque, il regime cinese ha esercitato un forte controllo sulle informazioni relative al virus, tanto che perfino i dati relativi ai contagi e ai decessi rilasciati dal governo di Pechino suscitano non pochi dubbi in merito alla loro veridicità.

---

[8] Si tratta dell' "estensione alle cose dei benefici dell'uso di Internet finora limitati alle persone, permettendo agli oggetti di interagire con altri oggetti e quindi con le persone in modo sempre più digitale". Fonte: https://www.zerounoweb.it/analytics/big-data/internet-of-things-iot-come-funziona/

[9] https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/

La strategia del PCC si basa su due aspetti cardine, ossia censura e propaganda. Per quanto concerne la prima, Freedom House[10] denuncia un aumento della censura online durante la pandemia esercitata tramite la rimozione massiccia di post che ritraggono o trattano di persone che manifestano gravi sintomi dell'infezione da Covid, campagne di raccolta fondi, denunce della criticità della condizione degli ospedali o critiche alla gestione dell'emergenza. Non solo i social media ma anche i giornalisti sono sottoposti a uno stretto controllo, molti dei quali sono stati arrestati o obbligati a lunghi periodi di "quarantena" nonostante non fossero positivi al virus. Accanto alle limitazioni alla libertà di espressione, il governo di Pechino attua una potente strategia di propaganda televisiva e giornalistica che evidenzia l'efficacia delle misure adottate senza considerare le significative violazioni delle libertà individuali in atto. Inoltre, il PCC elabora delle campagne di disinformazione che Laura Rosenberg[11] definisce "information offensive", le quali non solo innalzano l'approccio cinese alla gestione dell'emergenza a modello da esportare in tutto il mondo, ma screditano anche le risposte che altri governi (in particolare quello USA) hanno messo in atto per contrastare l'epidemia. Un'altra strategia adottata da Pechino è quella della "mask diplomacy", ossia il tentativo di promuovere e rilanciare la propria immagine a livello globale aiutando alcuni paesi europei tramite l'invio di mascherine e altri dispositivi di protezione individuale durante le prime fasi della pandemia.

La pandemia è stata capro espiatorio anche per una serie di ulteriori misure di limitazione alle libertà individuali e privacy implementate in nome del bene comune per arginare i contagi da Covid. La situazione di emergenza ha permesso l'espansione del controllo da parte del regime sulla popolazione mediante diversi sistemi. In primis, come in molti altri paesi del mondo, anche in Cina è stata creata un'applicazione per smartphone per il digital tracking dei contagi. A differenza di altre app, come l'italiana "Immuni", il download della cinese "Health Code" è stato reso obbligatorio mediante nuove norme di accesso ai trasporti pubblici, agli uffici, ai supermercati e perfino ai luoghi di svago e cultura come cinema e teatri, ai quali l'ingresso è limitato solo a chi possiede un codice verde. L'applicazione, infatti, funziona con un algoritmo che valuta ogni persona con un codice (verde, giallo o rosso) in base a criteri come età, stato di salute, movimento, alimentazione e geo-localizzazione. Le critiche mosse verso Health Code si riferiscono alla mancanza del requisito di trasparenza, ossia dell'impossibilità di capire come l'algoritmo elabori le valutazioni ed assegni i codici. Le persone, dunque, faticano a comprendere quali comportamenti possano portare all'attribuzione di un codice giallo o rosso (e quindi alla limitazione della libertà). Il sistema di

[10] https://freedomhouse.org/report/china-media-bulletin/2020/china-media-bulletin-coronavirus-era-repression-propaganda

[11] https://www.foreignaffairs.com/articles/china/2020-04-22/chinas-coronavirus-information-offensive

behavior management[12] attuato dal regime di Pechino attraverso il Sistema di Credito Sociale include ora anche un personal health index ricavato dall'applicazione Health Code, per cui anche lo stato di salute, l'abuso di fumo o alcol e l'attività fisica contribuiscono al SCS.

Inoltre, anche le misure di sorveglianza già esistenti sono diventate più invasive, arrivando perfino all'istallazione di telecamere davanti agli ingressi delle abitazioni per controllare che nessuno infrangesse le regole del lockdown. Anche dal punto di vista tecnologico ci sono state delle importanti evoluzioni, come ad esempio lo sviluppo di sistemi di riconoscimento facciale in grado di operare con un certo grado di precisione anche sui volti semi coperti dalle mascherine.

È importante sottolineare un importante vantaggio di natura psicologica portato dalla pandemia al modello cinese di sorveglianza onnipresente. L'epidemia ha infatti fornito al mondo quello che in inglese viene definito proof of concept (PoC)[13], ossia l'opportunità di dimostrare l'efficacia e l'utilità delle misure di controllo della popolazione (in questo caso per il contenimento dei contagi). Inoltre, l'emergenza ha portato la necessità di forme di limitazione delle libertà individuali anche in paesi democratici, riducendo di fatto lo "stigma" del controllo e elevando le misure cinesi a "modello" da poter applicare nel resto del mondo per uscire in tempi brevi dalla pandemia.

È largamente sostenuto che sia molto alta la probabilità che con la fine dell'emergenza da Covid-19 non scompariranno tutte queste nuove modalità di controllo e sorveglianza. Così come è avvenuto in Cina dopo le Olimpiadi di Pechino 2008 e a livello globale dopo gli attentati del 9 settembre 2001, è molto probabile che anche questa emergenza lascerà dietro di sé un aumento delle limitazioni più o meno invasive delle libertà individuali.

3. Intelligenza Artificiale nell'Unione Europea

Al momento della diffusione della pandemia da Covid-19 a cavallo tra il 2019 e il 2020, l'Unione Europea aveva già mosso i primi passi verso una regolamentazione dell'intelligenza artificiale a livello comunitario. Risale infatti ad aprile 2018 la pubblicazione della Dichiarazione sulla cooperazione in materia di intelligenza artificiale[14] e la Comunicazione: L'intelligenza artificiale per l'Europa[15], le quali propongono le prime linee guida per uno sviluppo controllato dell'IA nell'UE. Come esplicitato nella Dichiarazione, la necessità di muoversi verso una regolamentazione

[12] Con il termine "behavior management" si intende la gestione del comportamento della popolazione per il mantenimento dell'ordine.
[13] https://www.lowyinstitute.org/publications/digital-authoritarianism-china-and-covid#
[14] Bruxelles, 10 aprile 2018.
[15] COM (2018) 237 final.

a livello europeo è dettata dal fatto che "Il modo in cui ci relazioniamo all'IA determinerà il mondo in cui viviamo".

Due anni dopo, a febbraio 2020, è stato pubblicato il Libro Bianco[16] (in inglese White Paper) sull'Intelligenza Artificiale. Lo scopo principale di questo documento era di definire un approccio comune a tutti gli Stati Membri per evitare la frammentazione del mercato unico, affiancato dall'imperativo di sviluppare un'IA al servizio dell'uomo e nel rispetto dei valori etici e dei diritti umani fondamentali. Due aspetti cruciali vengono delineati, ossia la creazione di un "ecosistema di eccellenza" e di un "ecosistema di fiducia". Mentre il primo si occupa di innovazione, sottolineando l'importanza di un programma di finanziamento e della collaborazione tra i centri di ricerca in Europa, il secondo si concentra sui requisiti che le applicazioni dell'IA devono imprescindibilmente possedere, come ad esempio trasparenza, governance dei dati, equità, non discriminazione e sorveglianza da parte dell'uomo.

Questi tre documenti dell'Unione Europea sono accomunati da tre obiettivi: promuovere la ricerca, l'innovazione e l'utilizzo dell'IA; prevedere i cambiamenti socioeconomici; delineare un framework etico e giuridico.

Inoltre, il Libro Bianco del 2018 sancisce che "l'uso delle applicazioni di IA a fini di identificazione biometrica remota e l'impiego di altre tecnologie di sorveglianza intrusive sarebbero sempre considerati "ad alto rischio"" e pertanto stabilisce delle prescrizioni chiare e rigide da rispettare per il loro utilizzo. Con il termine "identificazione biometrica remota" si intendono quei sistemi di IA volti "a determinare l'identità di più persone utilizzando identificatori biometrici (impronte digitali, immagine del volto, iride, schema delle vene, ecc.) a distanza, in uno spazio pubblico e in modo continuo o permanente confrontandoli con i dati contenuti in una banca dati"[17], ossia quella che comunemente viene chiamata sorveglianza di massa. Tale applicazione dell'intelligenza artificiale, tuttavia, si scontra con i diritti umani fondamentali, come il diritto alla privacy (tutelato in UE dal GDPR[18]). Diversi gruppi[19] che si battono a sostegno della privacy considerano che la raccolta di dati da parte di Paesi come Francia, Belgio e Regno Unito per scopi di sicurezza nazionale abbia superato il limite di tutela della libertà individuale dei cittadini. In particolare, le critiche avanzate si

[16] COM(2020) 65 final.

[17] definizione fornita dal Libro Bianco sull'Intelligenza Artificiale, COM(2020) 65 final.

[18] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[19] https://techcrunch.com/2020/01/15/mass-surveillance-for-national-security-does-conflict-with-eu-privacy-rights-court-advisor-suggests/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAAS9hfO-m4Ze5okANJEIx6v8QkNG90iosJzgUGYtColDHy0AFXCEDUcCleFDDPmFTrSZJ9R8Y8BAmIxcLMIHq0MtA7inXoqLzW0FFdYfyb6qqj5vhAxazcvqcZKbTbBWlfqFsaijvqSEux9quRHu__eQuO6yaj8kZDGC2TwJy7j4

basano sul fatto che tali rilevazioni biometriche vengano condotte in modo generico e indiscriminato e, pertanto, non possono essere giustificate da uno scopo come la lotta al terrorismo. Tali gruppi richiedono invece che le misure di sorveglianza per la sicurezza nazionale avvengano in modo limitato e discriminato, vale a dire solo nei confronti di individui che rappresentano una minaccia reale e concreta.

Con la pubblicazione del Libro Bianco nel febbraio 2020, è stata avviata una consultazione pubblica per raccogliere proposte dalla società, dall'industria e dal mondo accademico per lo sviluppo di un approccio europeo all'IA. Il risultato del dialogo tra i portatori di interesse è stato pubblicato nel "Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe"[20] del 21 aprile scorso. Nello stesso giorno, la Commissione Europea ha anche reso pubblica la proposta di regolamento sull'approccio europeo all'Intelligenza Artificiale per lo sviluppo del primo quadro giuridico comunitario sull'IA. La comunicazione si inserisce nel progetto più ampio di Digital Strategy e in particolare nella Digital Decade, ovvero la prospettiva di una trasformazione digitale dell'UE entro il 2030. Una regolamentazione dell'IA a livello comunitario è necessaria per assicurare la sicurezza delle sue applicazioni e il rispetto dei diritti umani fondamentali, come il diritto all'autodeterminazione e il diritto alla protezione dei dati personali. Inoltre, una buona base legale è fondamentale per favorire gli investimenti e l'innovazione del settore e per la creazione di un mercato unico. Nel contesto globale di sviluppo dell'Intelligenza Artificiale, l'Unione Europea vuole distinguersi dagli approcci di Washington e Pechino per la sua attenzione all'etica e ai diritti umani. Lo scopo di questa proposta di regolamento è quello di guidare l'IA verso uno sviluppo sicuro, affidabile e antropocentrico. Attraverso un approccio proporzionato e basato sul rischio, la proposta di regolamento classifica gli utilizzi dell'IA in quattro categorie, cosicché maggiore è il rischio, più severe saranno le regole.

Alla base della piramide ci sono le applicazioni più comuni e diffuse che rappresentano un rischio da basso a nullo e per le quali è necessaria solamente la garanzia di conformità alle norme generiche di protezione del consumatore. Uno scalino sopra si trovano le applicazioni a rischio limitato, per cui è importante che sia rispettato il principio di trasparenza e che sia chiaro all'utente di stare interagendo con un algoritmo. I sistemi di machine learning che riguardano aspetti materiali della vita dell'uomo, come quelli utilizzati per la guida autonoma, per gli strumenti medici o per lo screening dei candidati ad un posto di lavoro, sono classificati ad alto rischio e pertanto il rispetto dei seguenti cinque obblighi è imprescindibile per il loro sviluppo, commercio e uso: dati di ottima qualità devono essere utilizzati per l'allenamento per evitare che si producano risultati

[20] https://op.europa.eu/it/publication-detail/-/publication/55538b70-a638-11eb-9585-01aa75ed71a1

pregiudizievoli; lo sviluppo e utilizzo devono sempre avvenire sotto supervisione dall'uomo; il requisito di trasparenza deve essere garantito, permettendo così la comprensione del funzionamento dell'algoritmo; l'utente deve essere consapevole di stare comunicando con un sistema di IA; è obbligatoria la registrazione nel database europeo delle applicazioni di IA che garantisce il rispetto degli standard di cybersicurezza. Al vertice della piramide ci sono le applicazioni vietate poiché considerate inaccettabili, come gli algoritmi per calcolare il credito sociale, che possono in qualunque modo arrecare danni fisici o psicologici all'uomo, o che manipolano il comportamento delle persone. All'interno di questa categoria si trovano i sistemi di identificazione biometrica in tempo reale, ossia quelli volti all'identificazione di persone a distanza attraverso il confronto con dati biometrici contenuti in un database. È importante distinguere tra i sistemi che operano in tempo reale, ovvero quando la registrazione, il confronto e l'identificazione avvengono simultaneamente, da quelli in differita, cioè quando vengono usate immagini registrate da telecamere private o a circuito chiuso. Mentre le seconde, sebbene classificate tra le applicazioni ad alto rischio, sono autorizzate, le prime sono invece vietate poiché sottopongono tutti gli individui all'analisi in modo indiscriminato.

Una controversa eccezione viene fatta se sono le forze di polizia ad utilizzare dei sistemi di identificazione biometrica, ad esempio, nei controlli di frontiera o per la ricerca di criminali: in questo caso si collocano tra gli algoritmi ad alto rischio e non tra quelli vietati. Tuttavia, anche per le forze dell'ordine non è consentito l'impiego di sistemi di sorveglianza di massa in luoghi pubblici come piazze o stazioni. Le prime critiche mosse verso la proposta di regolamento riguardano proprio questa eccezione poiché verrebbe lasciato eccessivo spazio per lo sviluppo e l'utilizzo di sistemi di sorveglianza di massa e riconoscimento facciale. Molta preoccupazione è stata anche generata dall'assenza di divieti per l'identificazione del genere e dell'orientamento sessuale, così come dell'etnia. Studi sui sistemi di riconoscimento facciale attualmente in uso da parte degli organi di polizia dimostrano che i risultati sono più precisi su individui di sesso maschile e pelle bianca, mentre le percentuali più alte di errore riguardano il genere femminile e la pelle nera. Un'altra critica è stata avanzata da Daniel Leufer[21] in merito ai termini utilizzati, che sarebbero troppo vaghi e lascerebbero spazio a scappatoie per eludere le norme.

In questa prima fase, la proposta rappresenta solo una prima bozza per la creazione di un quadro giuridico per regolare l'intelligenza artificiale a livello UE e pertanto verrà sottoposta a revisioni dopo i riscontri dei membri del Parlamento Europeo.

[21] https://www.theverge.com/2021/4/14/22383301/eu-ai-regulation-draft-leak-surveillance-social-credit

3.1 Misure in risposta alla pandemia da Covid-19

Per la pandemia da Covid-19, così come per il terrorismo, sono state necessarie delle nuove misure di controllo della popolazione con l'obiettivo di contenere i contagi e limitare la diffusione dell'epidemia. Ogni Stato è legittimato a limitare i diritti umani fondamentali dei cittadini per ragioni di salute pubblica o emergenza nazionale secondo i Principi di Siracusa, adottati dal Consiglio Economico e Sociale delle Nazioni Unite nel 1984. Si tratta di uno strumento di soft law[22], ovvero privo di vincolo giuridico, ma non per questo meno rilevante a livello internazionale. I Principi di Siracusa, infatti, forniscono delle linee guida in merito alle possibili limitazioni e deroghe dei diritti sanciti dalla Convenzione Internazionale sui diritti civili e politici[23] dell'ONU in vigore dal 1976. Tali restrizioni devono imprescindibilmente essere dirette verso un obiettivo legittimo di interesse comune, strettamente necessarie, il meno invasive possibile, basate su evidenza scientifica, non arbitrarie o discriminatorie, di durata limitata, nel rispetto della dignità umana, e soggette a revisione. Di estrema importanza è dunque che le misure limitative delle libertà personali siano temporanee, proporzionate ed eccezionali, e, pertanto, che non si prolunghino oltre la durata dell'emergenza. Anche la Presidente della sottocommissione per i diritti dell'uomo al Parlamento Europeo, Marie Arena, si è espressa in merito al rischio concreto che alcune limitazioni possano restare in vigore anche in assenza di uno stato di emergenza[24].

Per quanto concerne le applicazioni di tracciamento dei contagi, la Commissione Europea[25] ha proposto fin da subito un approccio unico comunitario con il fine non solo di uniformare tali strumenti per facilitare lo scambio transfrontaliero dei dati, ma anche per garantire un maggiore controllo dell'utilizzo dei dati sensibili. Il Parlamento Europeo ha espresso la necessità che le app di tracciamento rispettino la privacy individuale e siano conformi alle normative di protezione dei dati sensibili. Inoltre, questo strumento non deve mai essere diventare un requisito per poter esercitare il diritto alla libertà di movimento (come invece è avvenuto in Cina, dove l'applicazione Health Code è necessaria per accedere ad uffici, cinema e altri luoghi pubblici). Questa misura deve anche mantenere il suo carattere eccezionale e, pertanto, la sua implementazione deve essere provvista di una sunset clause (letteralmente "clausola del tramonto"), ossia la chiara specificazione che tale strumento cesserà di essere utilizzato quando la pandemia sarà terminata. Un altro requisito

[22] Con il termine "soft law" si intendono "modelli di norma giuridica, la cui traduzione in regola effettiva può avvenire mediante un recepimento a opera di legislatori, giudici o privati.". Fonte: https://www.treccani.it/enciclopedia/soft-law_%28Lessico-del-XXI-Secolo%29/

[23] https://www.ohchr.org/Documents/ProfessionalInterest/ccpr.pdf

[24] https://www.europarl.europa.eu/news/en/headlines/priorities/eu-response-to-coronavirus/20200618STO81514/covid-19-digital-surveillance-borders-and-human-rights

[25] https://www.europarl.europa.eu/news/en/headlines/priorities/eu-response-to-coronavirus/20200429STO78174/covid-19-tracing-apps-ensuring-privacy-and-use-across-borders

importante è la trasparenza riguardo il funzionamento di queste app e la gestione dei dati sensibili nel rispetto della normativa GDPR, i quali devono essere anonimizzati e non conservati in database centralizzati.

È bene inoltre chiarire la differenza tra le applicazioni di "contact tracing" e quelle di "contact tracking". Sebbene in italiano siano entrambe tradotte come applicazioni di tracciamento dei contatti, si tratta di due modalità totalmente differenti anche in relazione ai diritti umani. Con il termine "contact tracing" si intendono quelle applicazioni che sfruttano la tecnologia Bluetooth (Bluetooth Low Energy – BLE) per rilevare la presenza tra diversi dispositivi all'interno di una determinata area, senza registrare gli spostamenti di ogni soggetto, segnalando l'eventuale vicinanza con un individuo positivo senza specificare il luogo o l'orario. Al contrario, le applicazioni di "contact tracking" si basano sulla geo-localizzazione (GPS): queste ultime raccolgono i dati sulla posizione geografica dei dispositivi e sui movimenti, inviando una notifica in tempo reale. La Commissione Europea ha espresso la preferenza verso le prime, le applicazioni di "contact tracing", poiché il rischio di violazione di diritti umani sarebbe minore rispetto alle seconde. Inoltre, queste applicazioni collaborano tra loro a livello europeo per garantire il funzionamento in gran parte dell'Unione. Sul sito ufficiale dell'applicazione italiana Immuni è fornita una mappa dei quattordici Paesi dell'UE che partecipano insieme all'Italia alla rete di interoperabilità, tra i quali Francia, Paesi Bassi, Slovenia, Norvegia, e Austria.

Il 17 marzo scorso è stata avanzata dalla Commissione Europea la proposta per l'introduzione di una nuova misura comunitaria che dovrebbe permettere il ripristino della libertà di movimento all'interno dell'area Schengen: il Digital Green Certificate (DGC) o Green Pass. Questo documento viene rilasciato secondo tre criteri: vaccinazione contro il Covid-19, anticorpi sviluppati contraendo l'infezione fino a 6 mesi prima, o tampone negativo effettuato nelle 48 ore precedenti. Per garantire il rispetto delle libertà fondamentali e della privacy individuale, il Pass dovrà essere gratuito, accessibile a tutti, sicuro e non discriminatorio. Inoltre, come tutte le altre misure implementate in risposta alla pandemia, deve avere carattere temporaneo e il suo utilizzo dovrà pertanto cessare al termine dell'emergenza. Nonostante la proposta avanzata dalla Commissione delinei dei requisiti necessari per garantire il rispetto della normativa GDPR, non pochi dubbi sono sorti in merito a questa nuova misura. Come evidenziato da Euobserver[26], la vaccinazione contro il Coronavirus non garantisce la totale immunità e pertanto c'è la possibilità che un individuo vaccinato possa contrarre l'infezione, magari anche in forma asintomatica e quindi di più difficile individuazione. Inoltre, sembrerebbero mancare le basi legali per imporre dei controlli frontalieri nel codice frontiere

[26] https://euobserver.com/opinion/151678

Schengen[27]: la reintroduzione di controlli sulle persone che attraversano un confine sarebbe infatti permessa solo in caso di "grave minaccia per l'ordine pubblico o la sicurezza interna" - non viene appunto citato il caso di un'emergenza sanitaria. È stata anche sollevata una preoccupazione in merito alla temporaneità della misura poiché la Commissione ha proposto che fosse l'OMS (Organizzazione Mondiale della Sanità) a decidere quando sospenderla e pertanto l'Unione Europea non avrebbe il potere di porre fine al suo utilizzo. Con l'utilizzo del termine "suspend", la Commissione si riserva la possibilità di reintrodurre questo strumento nel caso l'OMS dichiari una nuova pandemia. La definizione di "pandemia" dell'Organizzazione Mondiale della Sanità si basa però sull'aumento di casi di contagio da un virus e non sul numero dei decessi. Nel futuro prossimo si prospetta la possibilità che altre pandemie si verifichino con più frequenza rispetto al passato, sebbene non tutte saranno particolarmente letali. Pertanto, questo significa che il DGC potrebbe essere destinato a restare in vigore più a lungo di quanto si immagini, portando con sé il ripristino dei controlli frontalieri e un implicito obbligo di vaccinazione.

4. Conclusione

In luce di quanto illustrato in merito al panorama cinese così come a quello europeo, è evidente che la pandemia da coronavirus abbia portato i governi di tutto il mondo ad adottare misure restrittive delle libertà individuali per rispondere all'emergenza. La sostanziale differenza che si può notare è che laddove un governo esercitava già delle forme di controllo della popolazione, come in Cina, il Covid-19 ha rappresentato un capro espiatorio per l'introduzione di misure ancora più invasive, specialmente attraverso l'utilizzo dell'intelligenza artificiale. Nell'Unione Europea, al contra**rio, i diritti umani fondamentali[28] e i dati personali[29] sono soggetti a maggiore tutela poiché l'UE trova nello Stato di diritto uno dei suoi valori fondamentali.** L'Articolo 2 del Trattato sull'Unione Europea[30] (TUE) elenca tra i principi basilari dell'Unione l'uguaglianza, la democrazia e, appunto, lo Stato di diritto. Sebbene nel TUE non venga fornita una vera e propria definizione, con il concetto di Stato di diritto si intende uno Stato liberale, nel quale sono garantite le libertà individuali e il diritto all'autodeterminazione, la certezza del diritto e la subordinazione del potere alla legge. Il 30 settembre dello scorso anno, la Commissione Europea ha pubblicato la prima

[27] https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0399&from=EN
[28] https://www.echr.coe.int/documents/convention_eng.pdf
[29] Vedi nota 14.
[30] C 326/13 - https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0017.02/DOC_1&format=PDF

Relazione sullo Stato di diritto 2020 - La situazione dello Stato di diritto nell'Unione europea[31] nella quale sono stati analizzati diversi ambiti, in particolare i sistemi giudiziari, il quadro anticorruzione, il pluralismo e la libertà dei media, e il bilanciamento dei poteri. Particolare attenzione è stata anche prestata alle conseguenze delle misure restrittive in risposta alla pandemia da coronavirus e al possesso dei requisiti di temporaneità, necessità e proporzionalità previsti dalla legge. Data la rilevanza che l'Intelligenza Artificiale sta acquistando recentemente, è probabile le prossime Relazioni annuali della Commissione comprendano anche l'impatto che lo sviluppo di nuove tecnologie di IA ha sullo Stato di diritto.

Diversi studi, come quello di Lydia Khalil pubblicato da Lowy Institute[32], sostengono che una delle eredità del coronavirus comune a tutti i Paesi sarà l'ampia diffusione di nuove forme di controllo della popolazione da parte degli Stati e la normalizzazione di tali restrizioni anche nelle democrazie occidentali. Le sfide che dovremo affrontare in un futuro non troppo lontano riguarderanno quindi l'elaborazione di politiche per la sicurezza efficaci nel totale rispetto dei diritti umani fondamentali, così come dei piani d'azione per rispondere a future emergenze sanitarie e un valido quadro normativo per lo sviluppo, il commercio e l'utilizzo dei sistemi di intelligenza artificiale.

[31] COM(2020) 580 final - https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020DC0580&from=EN

[32] https://www.lowyinstitute.org/publications/digital-authoritarianism-china-and-covid#