UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di Diritto Pubblico, Internazionale e Comunitario

Corso di Laurea in Diritto e Tecnologia

Anno Accademico 2025/2026

Sorveglianza e diritti fondamentali tra Europa e Cina: un'analisi comparata

Relatore:
Prof. Giuseppe Bergonzini

Laureando: Edoardo Casagrande
matricola: 2069804

Sommario

1. INTRODUZIONE

Nel corso degli ultimi anni è tema ricorrente quello dell'intelligenza artificiale e delle implicazioni che essa comporta nella modernità. Questo particolarmente in merito a quelli che sono i diritti fondamentali dell'essere umano, con un attento focus su quelle che sono le possibili sfide e violazioni da una parte, e le successive opportunità e ampliamenti dall'altra. Una tematica ormai ricorrente è proprio quella dell'utilizzo di sistemi di sorveglianza biometrica da remoto in tempo reale, i quali si fregiano di una specifica regolamentazione *ad hoc* nel contesto normativo europeo data la loro pericolosità per la violazione di diritti fondamentali. Obbiettivo di questo elaborato è quello di analizzare le implicazioni dell'utilizzo di tali sistemi e ulteriori affini nell'attuale contesto normativo e sociale. Inizialmente viene presentata un'analisi dell'attuale quadro normativo europeo, quindi i suoi obbiettivi, le diverse regolamentazioni in materia, le prescrizioni condivise a livello internazionale, e i diritti e libertà tutelati dal modello. Successivamente si presenta un'analisi dettagliata dell'attuale modello della Repubblica Popolare cinese in materia di sorveglianza biometrica, strumenti affini e intelligenza artificiale. L'attenzione verrà rivolta principalmente agli obbiettivi del modello, con attenta descrizione delle diverse normative in materia, le implicazioni per Stato e cittadini e una finale presentazione descrittiva degli strumenti implementati nel suddetto Stato. Questo per presentare con chiarezza le differenze fra i due modelli e i rischi nel quale ci si può imbattere nell'utilizzo di questi sistemi. Un tema molto attuale, soprattutto nel contemporaneo contesto sociale ed economico nel quale l'utilizzo di detti sistemi di intelligenza artificiale è costantemente in espansione e presenta uno sviluppo innovativo esponenziale. È necessario tuttavia affiancare la diffusione di tali sistemi con un insieme di normative strutturate *ad hoc* in modo da poter assicurare nel loro utilizzo la tutela dei diritti fondamentali, tenendo conto sia dei diritti tradizionali che delle ultime novità e implicazioni giunte proprio con la nascita e diffusione di tali sistemi di I.A.

2. IL MODELLO EUROPEO

La storia del diritto europeo moderno e la struttura della società contemporanea hanno radici antiche. Iniziano coi primi sistemi giuridici complessi sviluppati in Mesopotamia ed Egitto, ampliate poi da un fondamentale passaggio successivo agli scritti di grandi pensatori della Grecia, tra cui Platone, Socrate e Aristotele. Questi e molti altri influenzeranno poi a loro volta il diritto romano, pilastro essenziale del diritto contemporaneo. È infine fondamentale menzionare, per completare il quadro storico del pensiero filosofico in campo giuridico, ulteriori autori come quelli associati alla scuola Giusnaturalista[1] e Giuspositivista, tra cui rispettivamente Ugo Grozio, Thomas Hobbes, John Locke, Jean-Jacques Rousseau, per poi concludere con le aggiunte di Hans Kelsen e Jeremy Bentham. Proprio quest'ultimo in particolare avrà un ruolo di rilievo negli argomenti che verranno di seguito esposti, sulla base della sua definizione di Panopticon[2] che si presenta come un'ottima descrizione del sistema di sorveglianza cinese. L'insieme di questi soggetti e le loro peculiari riflessioni hanno quindi plasmato le fondamenta per la creazione del concetto di diritti umani fondamentali, che nell'era moderna è universalmente riconosciuto all'interno del nostro continente. Il tutto è infatti stato poi concretizzato nel secondo dopoguerra, con la creazione dell'ONU e i vari patti internazionali, tra cui in primis la Dichiarazione Universale dei Diritti Umani, e successivamente la stesura e approvazione della Convenzione Europea per la Salvaguardia dei Diritti dell'Uomo, unita all'omonima Corte istituita con lo scopo di giudicare sulla giusta applicazione dei principi di quest'ultima. È necessario inoltre menzionare anche la Carta dei diritti fondamentali dell'Unione Europea, di cui si parlerà in seguito trattando del modello dell'omonima Unione sovranazionale. Queste riflessioni e successivi

[1] D. NERI, *Filosofia morale. Manuale introduttivo*, Milano, 2013, 146-160.
[2] B. HAN, *Perché oggi non è possibile una rivoluzione*, Milano, 2022, 42.

cambiamenti sono stati il risultato di sfide politiche, filosofiche e sociali che hanno caratterizzato il vivere dell'epoca, e che hanno spinto tali soggetti a mettere in gioco il loro sapere per il miglioramento delle condivise condizioni di vita. La stessa situazione è riscontrabile anche nell'epoca moderna, di fronte alle nuove numerose sfide del diritto riscontrabili in diversi settori, tra cui la bioetica, l'infosfera, la geopolitica internazionale, e soprattutto l'intelligenza artificiale. Quest'ultima in particolare si è rivelata come la sfida portante dell'ultimo decennio, con implicazioni in tutti i vari settori del diritto. E in merito a ciò, è obbiettivo di questo elaborato la presentazione dell'analisi dell'utilizzo dei seguenti sistemi di intelligenza artificiale, in relazione allo stato dell'arte del diritto finora sviluppato, le relative normative in materia e il rispetto dei diritti umani fondamentali. Il tutto con una particolare concentrazione critica sull'applicazione di una distinta e peculiare categoria di sistemi tecnologici, ovvero i sistemi di sorveglianza acuta e rilevazione biometrica a distanza in tempo reale. Negli ultimi anni le istituzioni europee si sono impegnate nel fissare obbiettivi e principi utili per la creazione di un diritto armonizzato atto alla regolamentazione di questi strumenti e delle nuove frontiere in campo tecnologico, con lo scopo di tutelare i soggetti all'interno dell'Unione. Nel seguente capitolo si vede nello specifico quali sono stati gli obbiettivi predisposti e ciò che è stato fatto finora in materia.

2.1 OBBIETTIVI E FINALITÀ DELL'UNIONE NELL'ARMONIZZAZIONE DEL DIRITTO EUROPEO DI FRONTE ALLE NUOVE SFIDE NORMATIVE

Come già discusso in precedenza, l'Europa è stata patria di una serie di grandi movimenti filosofici, sociali e politici che hanno plasmato l'evoluzione del diritto fino ai giorni nostri, il quale ruota intorno al concetto di diritti umani

fondamentali. L'Unione Europea a questo proposito ha sempre dimostrato di avere una posizione garantista in linea con i principi democratici, ed è proprio su questa posizione che essa ha basato anche lo sviluppo di recenti normative *ad hoc* con lo scopo di orientare l'imponente rivoluzione digitale rispetto ai principi di tutela della dignità[3] e della sicurezza umana, e dei diritti fondamentali. Tra queste risalta in particolare l'AI Act del 2024, volto alla regolamentazione del commercio dei sistemi di intelligenza artificiale all'interno dell'Unione, che verrà descritto in maniera più approfondita nei paragrafi successivi. Per quanto concerne gli obbiettivi dell'Unione a questo proposito, trattandosi della prima normativa in materia di intelligenza artificiale essa si è peculiarmente imposta come *standard-setter*[4] non solo per i paesi interni ad essa, ma anche come punto di riferimento per altri Paesi esterni alla stessa. In questo ruolo di standard-setter, l'Unione ha dovuto cimentarsi[5] in diverse sfide normative, tra cui in primis la difficoltà nel regolamentare un settore in continuo sviluppo esponenziale, ma soprattutto la necessità di imporre delle normative piuttosto severe atte a tutelare i propri cittadini e il rispetto dei valori europei, pur ricercando allo stesso tempo il rafforzamento del proprio ruolo nella competizione globale relativa alle qui citate tecnologie innovative. Da qui la necessità di implementare una regolamentazione armonizzata, atta inoltre a perseguire l'intento di assicurare il buon funzionamento del mercato comune[6], ed evitare la possibilità di un diritto frammentato dato da molteplici normative nazionali, che in presenza di un vuoto normativo comune impedirebbe la libera e corretta commercializzazione degli stessi sistemi, con l'aumento del rischio di possibili illeciti e violazioni dei diritti

[3] A. D'ALOIA, *Ripensare il diritto nel tempo dell'intelligenza artificiale*, in A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Bologna, 2022, 97.
[4] A. ADINOLFI, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione: considerazioni sulla (difficile) costruzione di un quadro normativo dell'Unione,* in A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Bologna, 2022, 161.
[5] A. ADINOLFI, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione: considerazioni sulla (difficile) costruzione di un quadro normativo dell'Unione, cit., 128.*
[6] A. ADINOLFI, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione: considerazioni sulla (difficile) costruzione di un quadro normativo dell'Unione*, cit., 137.

fondamentali. La stessa cosa è riscontrabile non solo riguardo i sistemi intelligenti, ma anche la protezione dei dati e la privacy dei soggetti interni all'unione. Sono infatti state approvate ulteriori normative in materia, in particolare il Regolamento (UE) n. 2016/679, anche detto GDPR, e il Digital Service Act, approvato nel 2022. L'obbiettivo di queste due regolamentazioni è rispettivamente garantire potere di decisione e tutela ai cittadini nell'adattamento all'era dei Big Data, oltre alla tutela dei diritti fondamentali con riguardo alla limitazione di contenuti illegali, il contrasto alla disinformazione e l'imposizione di obblighi e limitazioni di responsabili per intermediari e piattaforme online. Un tema peculiare legato al sempre crescente utilizzo della cosiddetta infosfera, e della diffusione del concetto di sistemi di identificazione digitale, tematica che verrà maggiormente approfondita nelle varie implicazioni attribuite alle politiche statali della Repubblica Popolare Cinese.

2.2 LE NUOVE NORMATIVE EUROPEE NELLA GESTIONE DELLE ULTIME NOVITÀ DI DATIFICAZIONE E AUTOMAZIONE

Lo sviluppo tecnologico degli ultimi anni ha seriamente messo a dura prova il legislatore europeo, il quale ha dovuto mettersi a confronto con innumerevoli nuove fattispecie di illecito senza precedenti. L'avvento della rete internet poi evoluta nel cyberspace ha prima portato delle incertezze riguardo nuove tipologie di illecito da tipizzare; e successivamente l'evoluzione dei nuovi sistemi d'intelligenza artificiale si è confermato come nuovo portatore di incertezze in un quadro normativo già decisamente complesso, che ha richiesto un veloce adattamento atto alla tutela dei diritti e delle libertà garantiti ai cittadini all'interno dell'Unione. Su questa direzione sono state emanate nuove innovative regolamentazioni che verranno presentate qui di seguito, ovvero l'AI

Act, caposaldo del seguente paragrafo, seguito dall'antecedente Regolamento (UE) n. 2016/679, anche detto GDPR, e il Digital Service Act, approvato nel 2022.

2.2.1 IL REGOLAMENTO SULL'INTELLIGENZA ARTIFICIALE, I PRINCIPI E LE RELATIVE IMPLICAZIONI

Cominciando dall'AI Act, esso è una nuova forma di regolamentazione entrata in vigore nel 2024 con lo scopo di armonizzare la gestione dei sistemi di intelligenza artificiale all'interno dell'Unione Europea. Composto da 113 articoli suddivisi in capi, di questi si evidenzia l'art. 1[7] che ne presenta gli obbiettivi fondanti, ovvero "migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione, e promuovendo l'innovazione". Già da questo primo passaggio è possibile notare l'interesse dell'Unione nello sviluppare la normativa sul bilanciamento tra sicurezza e protezione di cittadini e istituzioni e lo sviluppo del mercato comune e dell'innovazione con un ruolo di guida a livello mondiale. Il Regolamento prevede infatti, come già applicato precedentemente nel Regolamento (UE) n. 2016/679, un approccio basato sul rischio; il quale tuttavia si differenzia per le modalità con cui esso viene declinato e imputato ai vari prestatori di servizi. Nell'AI Act vi è la suddivisione in quattro livelli di rischio, ovvero:

1- **Sistemi a rischio inaccettabile**, ovvero sistemi[8] vietati con un elevato

[7] F. MOLLO, *Il trattamento dei dati biometrici nell'IA Act: intersezioni tra la normativa di protezione dei dati e la nuova disciplina europea dell'intelligenza artificiale*, in *federalismi.it*, 11/2024, 7.
[8] F.M. MANCIOPPI, *La regolamentazione dell'intelligenza artificiale come opzione per la salvaguardia dei valori fondamentali dell'UE*, in *federalismi.it,* 03/2024, 14.

potenziale di manipolazione degli individui o che provocano un danno psicologico o fisico a particolari gruppi identificabili come vulnerabili, approfittandosi della loro fragilità e inducendoli ad adottare un determinato comportamento. Tra questi vi sono in otto pratiche vietate:

a. Pratiche di manipolazione e inganno che possano arrecare danno a un soggetto;
b. Sfruttamento dannoso delle vulnerabilità del soggetto fruitore del sistema intelligente;
c. Punteggio sociale, ovvero la pratica di attribuzione di punteggio ai cittadini sulla base del comportamento, è vietato in particolare alle pubbliche autorità, e spesso viene basato sull'identificazione biometrica o strumenti di identità digitale;
d. Valutazione o previsione del rischio di reato, vale a dire sistemi di polizia predittiva;
e. Riconoscimento facciale tramite ricerca ed estrazione da banche dati web o tramite sistemi di identificazione biometrica;
f. riconoscimento e inferenza delle emozioni nei luoghi di lavoro e negli istituti di istruzione;
g. categorizzazione biometrica basata su dati per trarre deduzioni o inferenze in merito a razza, religione o opinioni politiche;
h. identificazione biometrica remota in tempo reale in spazi accessibili al pubblico a fini di attività di contrasto, caratterizzato da una natura invasiva e il rischio di attuazione di una sorveglianza di massa;

Viene precisato tuttavia che l'utilizzo[9] di tali sistemi è strettamente vietato se non nei rari casi previsti dalla legge per finalità di sanità e sicurezza pubblica, o per proteggere diritti e libertà di terzi soggetti.

[9] A. D'ALOIA, *Ripensare il diritto nel tempo dell'intelligenza artificiale*, cit., 92.

2- **Sistemi ad alto rischio**: individuati in modo dettagliato nell'allegato III[10] della normativa, questa categoria comprende come descritto nel Considerando n. 27 quei sistemi che "producono un impatto nocivo significativo sulla salute, sulla sicurezza e sui diritti fondamentali delle persone nell'Unione". *Tali sistemi sono soggetti a requisiti e obblighi specifici in capo a produttori, sviluppatori e operatori per l'immissione nel mercato, cercando di rispettare il principio di *accountability* e assicurare l'assenza di rischi ritenuti inaccettabili. Tra questi sistemi vi rientrano:

   a. Componenti di sicurezza dell'IA nelle infrastrutture critiche, il cui guasto potrebbe mettere a rischio la vita e la salute dei cittadini;
   b. Soluzioni di IA utilizzate negli istituti di istruzione, che possono determinare l'accesso all'istruzione e al corso della vita professionale di determinati soggetti;
   c. Componenti di sicurezza dei prodotti basati sull'IA;
   d. Strumenti di IA per l'occupazione, la gestione dei lavoratori e l'accesso al lavoro autonomo;
   e. Alcuni casi d'uso dell'IA utilizzati per dare accesso a servizi pubblici e privati essenziali;
   f. Sistemi di IA utilizzati per l'identificazione biometrica remota, il riconoscimento delle emozioni e la categorizzazione biometrica;
   g. Casi d'uso dell'IA nell'applicazione della legge che possono interferire con i diritti fondamentali delle persone;
   h. Casi d'uso dell'IA nella gestione della migrazione, dell'asilo e dei controlli alle frontiere;
   i. Soluzioni di IA utilizzate nell'amministrazione della giustizia e nei processi democratici;

All'Allegato III ne sono previste delle specifiche illustrazioni, nel quale questi

[10] F.M. MANCIOPPI, *La regolamentazione dell'intelligenza artificiale come opzione per la salvaguardia dei valori fondamentali dell'UE*, cit., 15.

ultimi vengono annoverati secondo logiche di flessibilità e revisione, e individuandone inoltre i requisiti obbligatori di conformità. Alcuni esempi possono essere la qualità dei dati utilizzati, la loro conservazione e documentazione, la trasparenza e la cybersicurezza; il rispetto di questi requisiti viene quindi prima vagliato da appositi organismi di valutazione predisposti da ciascun'azienda, e successivamente anche dimostrato mediante una dichiarazione di conformità europea, emessa dalla competente autorità designata da ciascuno Stato membro. Ad essa si aggiunge inoltre la previsione d'introduzione dal Regolamento di una *governance*[11] sia nazionale che europea, che preveda l'istituzione di comitati e autorità indipendenti delegati all'indagine e al controllo dell'utilizzo di tali sistemi nel caso di violazioni. Come si può osservare quindi i suddetti sistemi sono subordinati ad un controllo *ex ante*[12] basato su obblighi e requisiti, e completato inoltre da una dimensione *ex-post* basata su meccanismi di monitoraggio successivi all'immissione sul mercato, dimostrando la consapevolezza dell'Unione nel ritenere che il tema del rischio riguardi l'intero ciclo di vita del sistema di intelligenza artificiale.

3- **Sistemi a rischio limitato**: sistemi ai quali sono previsti in particolare obblighi di trasparenza, in modo che il soggetto[13] sia consapevole di star reagendo con una macchina o di star interagendo con contenuti generati tramite strumento di intelligenza artificiale generativa, tema importante soprattutto per il caso dei *deepfake*[14], ovvero immagini, audio o video che assomigliano a persone, oggetti o eventi reali che possono trarre in inganno l'osservatore. Secondo questo principio appunto tali contenuti dovrebbero essere identificabili ed etichettati in modo chiaro e visibile, e che non

[11] E. LONGO, *I processi decisionali automatizzati e il diritto alla spiegazione*, in A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Bologna, 2022, 357.
[12] E. LONGO, *I processi decisionali automatizzati e il diritto alla spiegazione*, cit., 353.
[13] A. D'ALOIA, *Ripensare il diritto nel tempo dell'intelligenza artificiale*, cit., 90.
[14] G. D'ACQUISTO, C.A. TROVATO, L. DE BENEDETTI, *Alcune riflessioni sul concetto di autonomia decisionale della macchina e sulle sue implicazioni regolamentari*, in A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Bologna, 2022, 337.

comportino un pregiudizio per i diritti fondamentali o la sicurezza delle persone;

4- **Sistemi a rischio minimo o nullo**: questi sistemi invece non presentano delle precise norme atte a regolarli in quanto vi è un rischio troppo basso affinché vi si possano riscontrare delle effettive violazioni di diritti e libertà tutelati dall'Unione nei confronti dei cittadini. Per queste ultime due categorie in particolare è importante che vengano rispettati i principi etici e giuridici UE, e la normativa vi promuove il semplice rispetto di codici di condotta.

Successivamente alle categorie di rischio è doveroso ora indagare nello specifico i principi e gli obbiettivi sulla quale si fonda questa normativa. Nella regolamentazione di questi sistemi è stato necessario rilevare nuovi principi e impostare limiti adeguati, principalmente attribuiti a sistemi con rischio alto o superiore, con lo scopo di incentivare il corretto utilizzo di quest'ultimi nel rispetto dei diritti umani fondamentali e l'adattamento dei principi costituzionali alle applicazioni IA. Tra questi principi il più emblematico è sicuramente quello indirizzato alla configurazione e commercializzazione di sistemi di intelligenza artificiale[15] ***human-centric*** e ***trustworthy***, che quindi siano indirizzati da principi etici, e obblighi di conformità ai valori fondamentali della convivenza civile e del rispetto della dignità umana e dei diritti. Una premessa fondamentale che permetterà inoltre una maggiore fiducia della società civile in questi sistemi, garantendo un utilizzo sicuro e incentivando l'innovazione e lo sviluppo del mercato unico. Prendendo in esame la dignità umana in particolare, nella sua intersezione con questi sistemi si declina nel diritto delle persone di sapere se e quando stanno interagendo con una macchina o con un altro essere umano, e di decidere se, come e quando attribuire determinati compiti ad un sistema artificiale autonomo o ad una persona. Un altro principio poi spesso rimarcato

[15] A. D'ALOIA, *Ripensare il diritto nel tempo dell'intelligenza artificiale*, cit., 90.

nell'utilizzo di questi sistemi è il principio di **trasparenza**[16]. Secondo questo principio, spesso declinato in un principio di conoscibilità[17] dell'algoritmo, il sistema di intelligenza artificiale sia esso di *machine learning* o *deep learning*, deve essere reso noto al privato in quanto utilizzato per la produzione di processi decisionali che lo riguardano, ma soprattutto deve presentare un algoritmo che sia quanto più possibile conoscibile e spiegabile. Sulla base di questo principio vengono tuttavia imposti degli obblighi di carattere relativo, perché trattandosi di sistemi dotati[18] di "opacità interna" e della quale non è sempre possibile tracciare i passaggi che, successivi alle premesse (input), producono il risultato (output), vi è difficile assicurarne una completa trasparenza. Per questo motivo l'AI Act predispone degli obblighi minimi proporzionati sulla base del rischio che nonostante la facoltà limitata si dimostrano allo stesso tempo essenziali per l'etica e consapevole regolazione degli stessi. Un ulteriore principio specialmente rivolto ai sistemi IA ad alto rischio è inoltre quello dello ***human oversight***[19], che considera necessario il contributo umano nel processo decisionale. In particolare viene precisato come tali sistemi debbano essere progettati e sviluppati incorporando specifiche funzionalità che permettano un controllo umano sulla decisione algoritmica, con lo scopo di assicurarne ragionevolezza e correttezza. Successivamente si introduce inoltre il principio della **non discriminazione algoritmica**[20], secondo cui è previsto l'impegno del titolare del trattamento nell'utilizzare procedure matematiche o statistiche appropriate per la profilazione, affinché vengano rettificati i fattori che comportano inesattezze di dati e sia minimizzato il rischio di errori, riducendo quindi anche la possibilità di effetti discriminatori. Assieme a quest'ultimo viene

---

[16] F.M. MANCIOPPI, *La regolamentazione dell'intelligenza artificiale come opzione per la salvaguardia dei valori fondamentali dell'UE*, cit., 5.
[17] A. D'ALOIA, *Ripensare il diritto nel tempo dell'intelligenza artificiale*, cit., 103.
[18] F.M. MANCIOPPI, *La regolamentazione dell'intelligenza artificiale come opzione per la salvaguardia dei valori fondamentali dell'UE*, cit., 17.
[19] A. D'ALOIA, *Ripensare il diritto nel tempo dell'intelligenza artificiale*, cit., 92.
[20] F.M. MANCIOPPI, *La regolamentazione dell'intelligenza artificiale come opzione per la salvaguardia dei valori fondamentali dell'UE*, cit., 6.

poi spesso associato anche il principio di **non esclusività della decisione algoritmica**[21], previsto espressamente dall'art. 22 del Regolamento UE 679/2016, che recita: *"L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona"*. Secondo quanto espresso quindi, il soggetto dovrebbe essere prima informato dell'utilizzo di processi decisionali automatizzati che lo riguardano (principio di conoscibilità), e nel caso in cui non ne sia favorevole ha inoltre la possibilità di opporvisi. Sono da aggiungere inoltre tra i vari obbiettivi, come già menzionati pocanzi, *in primis* la garanzia di sicurezza dei sistemi IA presenti sul mercato UE in conformità con i valori e diritti fondamentali dell'Unione, successivamente il sostegno alla certezza del diritto per agevolare gli investimenti e l'innovazione, e infine la promozione di un mercato unico per l'applicazione dei sistemi IA che ne prevenga la frammentazione e che stabilisca regole condivise con cui realizzare lo scambio di beni e servizi. Obbiettivi mirati, predisposti sulla base dello specifico percorso intrapreso dall'Unione, che prevede un chiaro orientamento alla creazione di una griglia di strumenti di tutela *ex-ante*, i cui capisaldi sono tre regolamentazioni[22] connesse tra loro su diversi filoni, ovvero: *cybersecurity*, *data protection* e *artificial intelligence*. I capisaldi qui sopra menzionati vengono quindi a formare il **tridente** sulla quale viene basato il *framework* regolatorio complessivo europeo atto alla garanzia dell'autentica protezione dei dati personali e dei diritti degli interessati. E sempre in merito al rispetto di diritti fondamentali del cittadino è peculiare osservare la connessione che può sorgere tra sistemi di intelligenza artificiale e il **tema della libertà di pensiero**. Questo perché spesso questi sistemi algoritmici possono portare a situazioni di

[21] F.M. MANCIOPPI, *La regolamentazione dell'intelligenza artificiale come opzione per la salvaguardia dei valori fondamentali dell'UE*, cit., 6.
[22] E. LONGO, *I processi decisionali automatizzati e il diritto alla spiegazione*, cit., 371.

microtargeting[23] degli elettori, con seguente rischio di impoverimento del dibattito democratico e la creazione di casi quali *filter bubbles* ed echo chambers. Contestualizzando, le *filter bubbles*[24] sono un sistema di personalizzazione dei contenuti che mostra solo ciò che gli utenti preferiscono, limitando l'accesso a informazioni opposte o differenti, mentre le echo chambers sono ambienti in cui le persone condividono idee e opinioni simili, creando un ciclo di rafforzamento delle convinzioni. Questi fenomeni, quindi, possono portare alla polarizzazione delle opinioni e alla disinformazione, poiché le persone vengono esposte solo a contenuti che confermano le loro opinioni, senza la possibilità di confrontarsi con diverse prospettive. L'obbiettivo dell'AI Act è proprio quello di limitare la formazione di questi fenomeni in modo da poter garantire un corretto svolgimento della libertà di pensiero, permettendo quindi una consapevole e corretta informazione, e permettere alla società civile di avere a portata di mano gli strumenti atti al lineare funzionamento della democrazia.

2.2.2 REGOLAMENTO 679/2016 SULLA PROTEZIONE DEI DATI PERSONALI: PRINCIPI E IMPLICAZIONI

Conclusa qui la premessa sul Regolamento dell'intelligenza artificiale, è ora doveroso indagare il Regolamento relativo alla protezione dei dati personali, ovvero il *"General Data Protection Regulation"*, il secondo dei tre pilastri fondanti del tridente normativo europeo. Il Regolamento europeo 679/2016 sulla protezione dei dati è stato approvato nel 2016 ed entrato ufficialmente in vigore nel 2018, abrogando la precedente Direttiva 95/46/CE. È composto da 99 articoli

[23] A. D'ALOIA, *Ripensare il diritto nel tempo dell'intelligenza artificiale*, cit., 94.
[24] M. ANTENORE, E. VALENTINI, *Echo chambers e filter bubble. Effetti limitati e contraddizioni tra ipotesi teoriche e ricerche sul campo*, In *COMUNICAZIONEPUNTODOC,* 2018, 21-33, reperibile a questo link.

suddivisi in 10 capi, anticipati dai 173 Considerando che ne presentano i principi. Tra gli obbiettivi e principi fondamentali sulla quale si basa questo Regolamento, troviamo in primis la protezione dei dati personali dei soggetti, diritto fondamentale da tempo codificato nello spazio giuridico europeo. L'introduzione di questo nuovo Regolamento serve infatti per migliorare e ampliare la portata di questo diritto rispetto alla normativa precedente, garantendo maggiore protezione e controllo delle persone nel trattamento dei loro dati e alla loro libera circolazione. Allo stesso modo ha inoltre permesso di assicurare un'applicazione omogenea della disciplina sulla privacy su tutto il territorio dell'Unione europea, un principio espressamente affermato nel *considerando* 9[25] con lo scopo di garantire un clima di maggiore affidabilità e fiducia per i cittadini e lo sviluppo economico del mercato unico all'interno dell'Unione, un principio che ha altresì ispirato anche la successiva marcatura del AI Act. Per garantire ciò è stata inoltre avviata la proposta di istituire un sistema di autorità di controllo completamente indipendenti, incaricate di monitorare e garantire il rispetto di queste norme, e un chiaro esempio nazionale è il Garante per la Protezione dei Dati Personali (GDPD), o Garante Privacy. Questa normativa presenta inoltre diverse conseguenze nel panorama dei diritti già dapprima esistenti e quelli precedentemente sconosciuti; in particolare essa prevede:

- **un migliore accesso ai propri dati**;
- **un nuovo diritto alla portabilità dei dati**, che agevola la trasmissione dei dati personali tra prestatori di servizi;
- **un più chiaro diritto alla cancellazione** (diritto all'oblio);
- **il diritto di sapere se i propri dati personali sono stati violati.**

Esso presenta inoltre delle regole per la protezione dati concernente le imprese, adottando un approccio neutrale che prevede:

- **un unico complesso di norme a livello di Unione**, in modo da rafforzare la certezza del diritto e ridurre gli oneri amministrativi;

[25] C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *federalismi.it*, 11/2018, 3.

- **un responsabile della protezione dei dati**, designato da autorità pubbliche e imprese che trattano dati su larga scala o la cui attività principale è il trattamento di categorie speciali di dati;
- **l'affidamento ad una sola autorità di controllo** per Stato membro dell'Unione, alla quale le imprese devono rivolgersi;
- **norme dell'Unione per le aziende extra unionali**. Le aziende con sede al di fuori dell'Unione devono applicare le stesse norme quando offrono servizi o beni, o quando monitorano i comportamenti delle persone all'interno dell'Unione;
- **norme favorevoli all'innovazione**. Garanzia del fatto che la protezione dei dati sia incorporata nei prodotti e nei servizi fin dalle primissime fasi di sviluppo;
- **tecniche rispettose della privacy**. È incoraggiato ad esempio il ricorso alla pseudonimizzazione (utilizzo di identificatori) e alla cifratura (codificazione conosciuta solo da utenti autorizzati), al fine di limitare l'invasività del trattamento;
- **eliminazione delle notifiche**. Il GDPR ha eliminato la maggior parte degli obblighi di notifica e i costi ad essi associati;
- **valutazioni d'impatto sulla protezione dei dati**. Le organizzazioni dovranno effettuare valutazioni d'impatto qualora il trattamento dei dati presentasse un rischio elevato per i diritti e le libertà delle persone;
- **tenuta dei registri**. Le piccole e medie imprese non sono tenute alla registrazione delle attività di trattamento dei dati, a esclusione di casi particolari;
- **un moderno pacchetto di strumenti per il trasferimento internazionale dei dati**. Il GDPR offre vari strumenti per trasferire i dati al di fuori dell'Unione, tra cui le decisioni in materia di adeguatezza adottate dalla Commissione europea laddove il paese terzo offra un adeguato livello di protezione.

E oltre ai vari obbiettivi qui sopra elencati, vi sono una serie di principi al quale questo Regolamento si ispira nella protezione dei dati personali. In primis, il passaggio fondamentale di questo Regolamento rispetto alla normativa precedente è quello di distaccarsi dalla concezione[26] sostanzialmente *statica* del diritto al rispetto della vita privata, che era perciò caratterizzato da una tutela eminentemente negativa. Nell'attuale stato dell'arte il dato è considerato come un'estensione della personalità dell'individuo, e come tale deve essere protetto e tutelato in tutto il suo ciclo di vita. Vi è quindi una concezione *dinamica* dello stesso, che nella sua accezione prevede poteri d'intervento che possano controllarne e salvaguardarne la circolazione, permettendo quindi l'espressività di un pieno diritto *"all'autodeterminazione informativa"*, inteso come diritto di accesso ai propri dati, diritto di rettifica, diritto di cancellazione, diritto di limitazione e diritto di opposizione al trattamento dei propri dati, nonché alla stessa attività di profilazione. Ed è con queste premesse che si delinea quindi il passaggio fondamentale dall'*habeas corpus*, precedentemente tipizzato, all'*habeas data*[27]. Ovviamente però la dinamicità del dato non è l'unica cosa di rilievo che è stata riportata in esame. Come già visto precedentemente, e sottolineato nel sesto *considerando* del suddetto Regolamento, vi è chiara consapevolezza del legislatore europeo sia nel ruolo che nel valore economico[28] dei nostri dati, i quali con la combinazione dei fenomeni di digitalizzazione e globalizzazione presentano rischi sempre maggiori alla loro salvaguardia. Questi sono altri due motivi fondanti che hanno spinto l'ideazione di questo Regolamento, con lo scopo di garantire appunto una maggiore fiducia generale e un quadro più solido e coerente nella tutela della privacy, con successive ripercussioni sulla crescita economica del mercato interno e la tutela dei diritti

[26] C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, cit., 4.
[27] C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, cit., 14.
[28] C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, cit., 5.

fondamentali. Proprio nella misura del trattamento, l'art. 5[29] specifica che i dati personali devono essere trattati secondo tre principi, ovvero liceità, correttezza e trasparenza. Il primo di questi in particolare è poi ancorato a due requisiti alternativi, ovvero la necessità del trattamento, oppure il consenso del trattamento. A questo proposito è utile inserire una breve parentesi sull'articolo 9[30], che appunto impone *"il divieto generale di trattamento senza l'esplicito consenso dell'interessato per quanto attiene ai cc.dd. dati sensibili"*, rimarcando appunto il presupposto del consenso. Il secondo presupposto viene inoltre enunciato alla lettera c del primo comma dell'art. 5[31], secondo cui i dati raccolti devono essere caratterizzati da un nesso di pertinenza e adeguatezza rispetto alle finalità, in modo tale che non possano essere raccolti dati eccedenti le finalità predeterminate. In particolare questo principio viene anche declinato nella minimizzazione, secondo cui i sistemi di trattamento devono ridurre al minimo l'utilizzazione dei dati personali, soprattutto nel caso in cui tali obbiettivi pattuiti possano essere raggiunti mediante dati anonimi o che non consentano l'immediata identificazione dell'interessato. Ad esso si riferiscono poi diversi altri principi, tra cui quello di precauzione che come suggerito dal nome impone al titolare del trattamento una valutazione *ex-ante* di pertinenza del dato rispetto al fine; e infine quello di proporzionalità che allo stesso modo vieta oneri eccessivi nelle quantità di dati utilizzati. Successivamente, sempre al primo comma dell'art. 5, viene ripreso il secondo pilastro del potere di autodeterminazione, che si sdoppia nei principi di correttezza e trasparenza. Essi devono essere presentati attraverso un'adeguata informativa, che si dimostra «funzionale alla formazione ed espressione di un consenso al trattamento autenticamente libero e consapevole, nonché all'eventuale esercizio di tutti i diritti dell'interessato». Questo trattamento oltretutto deve articolarsi secondo il

[29] C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, cit., 20.
[30] C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, cit., 21.
[31] C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, cit., 22-24.

rispetto dei principi di *fairly manner* e di finalità, secondo cui rispettivamente, in primis il leale comportamento del titolare si dovrebbe dimostrare attraverso una libera scelta dell'interessato, anche mediante un duplice grado di informativa che consenta agli utenti di esprimere scelte realmente consapevoli e informate, e successivamente il trattamento dei dati deve inoltre limitarsi alle strette finalità che si intende perseguire, e che allo stesso modo devono essere chiaramente presentate tramite l'informativa. Quindi secondo questi principi, accompagnata dal corretto trattamento del titolare nella consapevolezza di scelta è prevista inoltre la stretta corrispondenza tra obiettivi di raccolta ed effettivo utilizzo dei dati personali. Infine sempre riguardo alla responsabilità si rinviene come il qui presente e già menzionato nuovo approccio del legislatore europeo alla valutazione e gestione del "*rischio*" fondato sul *principio di accountability*[32], ispirazione al successivo approccio del Regolamento IA, ripreso anche nell'art. 32 e che non solo dà luogo ad una forma di responsabilità del titolare e del responsabile del trattamento, ma ha anche lo scopo di trasformare i principi generali della protezione dati in politiche e procedure concrete nel rispetto delle legge e dei regolamenti applicabili".

2.2.3 REGOLAMENTO SUI SERVIZI DIGITALI, O DSA

Completata la premessa sul Regolamento sulla protezione dei dati, è doveroso ora introdurre una breve premessa sul Regolamento sui servizi digitali, ovvero il Digital Service Act. Questo Regolamento è stato approvato nel 2022 ed ufficialmente entrato in vigore nella sua piena applicabilità nel 2024, diventando vincolante per tutte le piattaforme di diversa dimensione. Il fulcro del Regolamento è la creazione di un ambiente online più sicuro per i consumatori e

[32] C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, cit., 26.

le imprese nell'Unione europea, attraverso una serie di norme con diversa finalità, tra cui:

- proteggere i consumatori e i loro diritti fondamentali in modo più efficace;
- definire responsabilità chiare per le piattaforme online e i social media;
- gestire i contenuti e i prodotti illeciti, l'incitamento all'odio e la disinformazione;
- raggiungere una maggiore trasparenza con una migliore comunicazione e vigilanza;
- incoraggiare l'innovazione, la crescita e la competitività nel mercato interno dell'Unione.

Nel seguente Regolamento vengono introdotti sistemi di responsabilità scalabile e trasparenza per i prestatori intermediari di servizi, e norme dettagliate per piattaforme online e motori di ricerca con dimensioni molto grandi. Esso inoltre ha lo scopo di tutelare i diritti fondamentali degli interessati, con annoverati principi tra i quali:

- **la lotta ai contenuti illeciti e affini** come l'incitamento all'odio;
- **responsabilizzazione degli utenti e della società civile**;
- **valutazione e mitigazione dei rischi** come garanzie per minori, e limitazioni nell'uso di dati sensibili per la pubblicità mirata;
- **il rafforzamento dei meccanismi di vigilanza e di applicazione** per tutti i prestatori di servizi intermediari.

2.3 I SISTEMI A IDENTIFICAZIONE BIOMETRICA A DISTANZA: IMPLICAZIONI DELLA SORVEGLIANZA SUI DIRITTI E LA SOCIETÀ CIVILE

I "sistemi a identificazione biometrica a distanza in tempo reale"[33] sono tecnologie che, particolarmente mediante sistemi di intelligenza artificiale, permettono di identificare con esattezza una persona a partire da alcune sue caratteristiche biometriche uniche, come ad esempio i tratti fisici (es: immagine del volto), oppure tratti del suo comportamento, come il timbro della voce o il modo di parlare e interagire con le altre persone. La particolarità di questi sistemi, come già menzionato in precedenza, è la loro alta pericolosità nel rischio di violazione dei diritti umani fondamentali; per tale motivo il legislatore europeo ha previsto il completo divieto dell'utilizzo di questi ultimi se non in speciali casi di sicurezza e sanità pubblica come anche prescritto nell'ultimo Regolamento sull'intelligenza artificiale, nel quale vengono compresi nella categoria dei sistemi a rischio inaccettabile. Diversamente da altri tipi di dati biometrici come il DNA, questi sistemi non richiedono alcun contatto fisico ma hanno la possibilità di acquisire immagini[34], video o registrazioni vocali del soggetto interessato. Questi dati vengono poi comparati con altri, prontamente inseriti in un database, e processati da algoritmi di intelligenza artificiale in modo da poterne trovare delle corrispondenze e quindi ricavarne le generalità soggettive e ulteriori informazioni estrapolabili tramite predizioni. Questi strumenti presentano delle incredibili potenzialità sia nell'ambito privato che pubblico, ma allo stesso tempo riportano gravi rischi nell'ambito della sorveglianza, la quale può evolversi in accezioni sempre più pervasive e lesive, e che può essere sfruttato anche per controllare, tracciare e manipolare singoli individui o interi gruppi di persone, perseguendo scopi tutt'altro che legittimi.

---

[33] G. MOBILIO, *I sistemi di identificazione biometrica a distanza: un esempio paradigmatico delle sfide lanciate dalla tecnologia al diritto costituzionale,* in *Consulta Online,* 09/2021, 3.
[34] G. MOBILIO, *I sistemi di identificazione biometrica a distanza: un esempio paradigmatico delle sfide lanciate dalla tecnologia al diritto costituzionale,* cit., 3-5.

Questi i motivi che hanno spinto il legislatore europeo a inserire un insieme di limiti e vincoli invalicabili a questi sistemi, indicando inoltre ulteriori requisiti, finalità e obblighi per i casi di autorizzazione. Le problematicità rilevate nell'utilizzo di tali sistemi si rifanno in particolare alla grande velocità alla quale essi si evolvono, implicazione al quale il diritto ha sempre riscontrato difficoltà nello stare al passo, e questo porta conseguenze peculiari sia nel settore privato che in quello pubblico. In prima battuta, gli stessi consumatori hanno interesse nell'appropriarsi di tali sistemi sviluppati da aziende private che sembrano promettere prestazioni e funzionalità innovative, ma che di fronte alle esigenze di tutela spesso non hanno la possibilità di essere commercializzati, un classico esempio è quello degli occhiali smart dotati di tecnologie di riconoscimento facciale; mentre in seconda battuta spesso sono gli stessi poteri pubblici che nel loro operato si rivolgono ad aziende private per l'impiego di questi sistemi intelligenti, e questo chiaramente fornisce agli stessi archivi dell'operatore privato un'incredibile fonte di dati personali sfruttabili per fini predittivi e di scelta, garantendo quindi oltre che un immenso valore economico in mano a questi *players*, anche la possibilità di sfruttarli per ottenere un vantaggio a livello politico. Questo potere infatti ha la possibilità di influire nell'esercizio dei diritti fondamentali e nella libera espressione di scelte democratiche, e come tale necessita di una limitazione imposta dai rimedi costituzionalistici e le relative normative europee. In capo agli operatori pubblici si rilevano invece un altro insieme di diversi potenziali rischi nell'utilizzo di tali tecnologie, in primis l'incisione diretta sull'esercizio delle libertà personali legate alla partecipazione politica e sul tenore democratico dell'ordinamento statale. L'esempio più eclatante e successivamente rilevante a questo proposito è proprio il sistema di *Social Scoring* della Repubblica Popolare Cinese, che basandosi su questi sistemi è in grado di esercitare una sorveglianza capillare di massa su tutta la popolazione, permettendole di osservarne i comportamenti e valutare i soggetti sulla base degli stessi, con seguenti annesse discriminazioni e violazioni dei diritti fondamentali. È proprio a questo proposito che nella suddetta Repubblica

in particolare, e in maniera più moderata e controllata nel nostro continente, si presenta un quadro nel quale la persona è sempre più digitalizzata, profilata e trasparente. Vi è una società dell'accesso e della trasparenza[35] che legittima la pretesa di altri (Stato e aziende) di richiedere e ottenere dati e informazioni soggettive in qualsiasi ambito, e la successiva possibilità di classificarli sulla base di parametri predefiniti. Da queste classificazioni vengono poi estrapolate delle analisi per l'offerta di beni e servizi e la dettagliata profilazione di clienti e potenziali sostenitori per un determinato ente. Una vera e propria sorveglianza liquida orientata in senso predittivo, nel quale viene venduto un controllo indiscriminato travestito da trasparenza e fiducia incontrovertibile. I dati e le informazioni estrapolabili, infatti, hanno un enorme valore economico sia per esponenti politici che economici e permettono una completa identificazione della persona. Ed è proprio in funzione di questo fattore che risulta necessario operare un controllo sui propri dati attraverso la conoscenza della logica del trattamento degli stessi, in modo da evitarne la spersonalizzazione e garantire a sé stessi poi una migliore tutela.

[35] F. MOLLO, *Sorveglianza di massa, rispetto della vita privata e trattamento di categorie particolari di dati nel quadro multilivello di tutela della persona*, cit., 3-5.

3. IL MODELLO CINESE

3.1 CENNI STORICI

Le origini della storia cinese[36] risalgono a più di 5000 anni fa, delineando una presenza millenaria e un'evoluzione temporale strategica e radicale che la ha portata allo status di potenza globale che attualmente ricopre. Le radici più rilevanti del diritto cinese si ritrovano tuttavia nel periodo della Cina Imperiale, quindi diversi millenni dopo l'effettiva nascita di quest'ultima. Questo periodo era infatti caratterizzato da un peculiare modo di intendere diritto e cultura, e che si distinguerà come influenza anche nei millenni a venire, basato sul doppio binario di regole morali e prescrizioni giuridiche. Vi era quindi un concetto totalmente diverso di diritto rispetto ai canoni tipici della civiltà occidentale, caratterizzato da ordinamenti e relative norme mentre le regole morali hanno più una dimensione meta-giuridica. La società cinese si è invece sviluppata con la visione opposta, basata su un binario nel quale la morale prevaleva sull'altra nel regolamentare i comportamenti dell'individuo, mentre il diritto aveva più un'accezione negativa come materia invocatrice del conflitto e della rottura della pace sociale. Questa particolare visione è da imputare principalmente alla presenza degli insegnamenti del Confucianesimo nella cultura cinese; una filosofia basata sulla natura genuina dell'uomo, le usanze della tradizione e i principi di altruismo, generosità e amicizia. Il diritto cinese era appunto costruito dall'elaborazione di queste due correnti[37], ovvero il *li*, che riprendeva i principi confuciani e si imponeva come la dottrina capostipite basata sull'insieme dei riti e degli obblighi morali che l'uomo doveva rispettare per vivere in armonia con la natura, e il *fa*, elaborato dalla scuola dei legisti e riprendeva l'insieme delle leggi

[36] R.TARCHI (a cura di), *Appunti di diritto cinese, Istituto universitario Carolina Albasio, 6-8.* Scritto che riproduce lo schema delle lezioni integrative svolte per i corsi di Sistemi giuridici comparati della Facoltà di Giurisprudenza di Pisa dal Prof. XUE JUN dell'Università di Wuhan e di Pechino nell'anno 2005, e l'aggiunta delle relazioni svolte al quinto Seminario italo cinese, svoltosi a Pisa il 13 dicembre 2008 da docenti dell'Università di Wuhan . Revisione avvalsa della collaborazione dei dottori M. MOTRONI e D. FIUMICELLI. (Reperibile al seguente link)

[37] R.TARCHI (a cura di), *Appunti di diritto cinese,* cit., 7-11, reperibile a questo link.

scritte, dei decreti e delle decisioni giudiziali, e rispetto al precedente aveva appunto un ruolo più marginale sulla base della reputazione negativa nella gestione dei conflitti. Questa lotta ha oltretutto caratterizzato grandissima parte del diritto cinese, fino agli inizi del XX secolo. Va inoltre aggiunto che nella società tradizionale cinese non era giuridicamente configurabile la nozione di "diritto soggettivo", poiché ai sudditi dell'impero non venivano riconosciuti diritti, ma solo doveri di sottomissione e di obbedienza. La rivendicazione di diritti individuali era infatti vista come un potenziale elemento di disgregazione dell'armonia complessiva e degli equilibri sociali che costituivano il fondamento della società. Un successivo grande cambiamento di prospettiva può rinvenirsi alla fine del XIX secolo, dove a seguito delle crisi interne dopo le sconfitte delle guerre dell'oppio e quella contro il Giappone, avviene una procedurale sgretolatura delle fondamenta dell'assetto istituzionale e sociale. È da questo periodo di crisi che si avvierà un condiviso movimento d'opinione che riteneva fosse necessario avviare una profonda fase di modernizzazione, che inizierà dalla dinastia Qing e che nonostante il mantenimento del sistema feudale prevedeva l'adozione di una serie di modelli normativi ispirati ai modelli occidentali. Ed è proprio sulla base di questi modelli che verrà avviato un movimento riformatore che aveva come scopo l'istituzione di un nuovo sistema politico ed economico ispirato alle monarchie costituzionali europee. Come nella precedente riforma normativa avvenuta anche in Giappone, l'imperatore commissionò a 5 ministri l'osservazione degli ordinamenti giuridici europei alla ricerca di un modello ideale che venne poi ritrovato negli ordinamenti europei di matrice romanistica, che in quanto rappresentati da norme codificate e quindi da *civil law*, erano sicuramente più semplici da assimilare[38] considerata inoltre la loro grande carenza di giuristi ben formati che potessero contribuire in modo adeguato alla formazione di un diritto in via giurisprudenziale. Più problematica si presentò tuttavia l'introduzione del concetto di diritto soggettivo, in quanto la cultura

[38] R.TARCHI (a cura di), *Appunti di diritto cinese,* cit., 11-13, reperibile a questo *link*.

cinese era ormai da secoli improntata ad un modello di organizzazione sociale che si basava sulla configurazione di soli doveri in capo ai sudditi, e che guardava con disprezzo a qualsiasi forma di rivendicazione individuale che si ponesse in contrasto con le esigenze della collettività. Questo probabilmente il principale tratto distintivo dell'approccio cinese rispetto alla concezione occidentale. Il definitivo cambiamento si avrà tuttavia in seguito, infatti nel 1911 verrà sancita la fine dell'antico impero cinese, spodestato dalla rivoluzione che porterà poi all'instaurazione della Repubblica e la fondazione della stessa sul principio della separazione dei cinque poteri in cinque organi, ovvero: legislativo, esecutivo, giudiziario, organi di controllo e organi di riesame. Nello stesso periodo vennero inoltre promulgati diversi codici e la prima Costituzione della Cina nel 1931. Essi tuttavia non goderono a lungo di ampio consenso, poiché quest'opera di codificazione faticò a conciliarsi con la flessibilità ed il consensualismo della società cinese, che la soppiantò presto in favore del diritto giurisprudenziale, che si adatta in maniera più omogenea alle tradizioni culturali. Proprio da questo scontro si verrà a creare una bipartizione del diritto cinese, sulle orme dell'antica dialettica tra il *li* e il *fa*, tra diritto legislativo e diritto giurisprudenziale. Nonostante l'ampio dissenso, le riforme legislative rimasero formalmente in vigore a causa del grande contesto di instabilità politica dell'epoca, fino al 1949 con l'avvento della rivoluzione socialista. Con la vittoria del Partito Comunista infatti il sistema giuridico cinese ha subito una serie di grandi cambiamenti, guidati in particolare dall'approvazione del "Programma comune" del partito, che si impegnava ad abrogare tutte le leggi precedentemente approvate dai rivali del *Kuomintang* e che si impose come Costituzione provvisoria. Questo programma[39] oltremodo fu oggetto di una successiva spaccatura più profonda tra coloro che volevano in qualche modo mantenere una linea di continuità con il Programma comune, dando vita ad un sistema politico basato sulla dittatura democratica popolare e ad un sistema economico ancora

[39] R.TARCHI (a cura di), *Appunti di diritto cinese,* cit., 13-14, reperibile a questo *link*.

aperto al capitalismo, e coloro che sostenevano l'esigenza di aderire al modello socialista. Tra i due prevalse poi la seconda linea di pensiero, che portò all'approvazione della successiva Costituzione del 1954 e all'inizio di una nuova era della storia cinese sotto il modello socialista.

3.2 OBBIETTIVI DI CENTRALIZZAZIONE E CONTROLLO DELLA REPUBBLICA POPOLARE CINESE

Gli obbiettivi fondanti del seguente modello possono quindi ritrovarsi all'interno di una serie di fattori distinti. *In primis* è necessario menzionare la lunga storia ricca di tradizioni della seguente civiltà, la quale appunto reduce dagli insegnamenti confuciani prevede una prevaricazione dell'interesse dell'individuo a favore dell'armonia dell'ambiente circostante, degli interessi della collettività e soprattutto della salvaguardia dello Stato. Quest'ultimo elemento ha poi ricevuto un'accezione oltremodo rilevante in seguito all'ingresso dell'ideologia socialista al potere, con conseguente rifiuto del concetto di diritti umani fondamentali che verrà poi ripreso solo all'inizio degli anni Ottanta, e l'avvio di un forte incremento del controllo dello Stato nell'economia e nell'organizzazione della vita sociale. Con il successivo ingresso dell'attuale presidente Xi Jinping al potere la visione stato-centrica cinese è poi ulteriormente aumentata. Nonostante l'approvazione della Costituzione nel 1982, la tanto prevista e attesa riforma della Cina verso gli standard occidentali fallisce, e al contrario è la stessa Repubblica Popolare a voler esportare la propria visione nel resto del mondo. I diritti umani non hanno un valore assoluto ma continuano a venir messi in secondo piano rispetto allo sviluppo economico, all'innovazione e alla sicurezza dello Stato, la visione caratterizzante è quella di questi ultimi come un insieme di valori forzatamente esportati dall'occidente in contrapposizione alle giuste e

rispettabili virtù asiatiche, e in quanto tali perdono di rilevanza. Allo stesso modo come sancito dal documento numero 9[40] rilasciato nel 2013 dal presidente Xi, l'insieme di valori ed istituti quali stampa libera, democrazia e società civile sono definiti concetti importati e in quanto tali banditi. Questa una tendenza peraltro riscontrabile anche nell'attuale modalità di gestione statale governata dall'utilizzo di sistemi di intelligenza artificiale per il controllo e la valutazione dei cittadini della Repubblica Popolare, nella quale i diritti umani non sempre vengono tutelati. Il popolo è costantemente sotto sorveglianza attraverso l'utilizzo di telecamere con sistemi di identificazione biometrica, che controllano il comportamento di ogni cittadino, il quale viene poi classificato sulla base di una serie di parametri preimpostati. Il dissenso viene censurato, gli attivisti e oppositori bloccati, arrestati e indottrinati. Lo Stato possiede il totale controllo delle informazioni sui cittadini, siano essi ricavati da analisi delle forze di polizia sulla popolazione, dalla sorveglianza biometrica o dalle informazioni obbligatoriamente fornite dai cittadini e dalle aziende private. Il tutto per raggiungere lo scopo ultimo dell'attuale Presidente, ovvero il mantenimento del potere nelle mani del partito comunista per l'interesse del corretto e incontenibile sviluppo della Repubblica, e del raggiungimento dello status indiscusso di più grande potenza statale a livello globale tramite l'innovazione dei sistemi di intelligenza artificiale e la sorveglianza di massa.

[40] A. COLARIZI, *la storia della Cina con la lente dei diritti umani*, in *Gariwo Magazine*, 04/2023, reperibile a questo link.

3.3 GLI SVILUPPI DEI SISTEMI INTELLIGENTI E IL FRAMEWORK NORMATIVO DELLA RPC

La Repubblica Popolare cinese, similarmente con quanto accaduto all'Unione, ha dovuto confrontarsi con l'insorgere del sempre più veloce sviluppo e frequente utilizzo dei sistemi di intelligenza artificiale nella vita dei cittadini. Di fronte a quest'immediata rivoluzione la risposta di quest'ultima e linearmente con quanto stabilito dai vari Paesi e organizzazioni sovranazionali è stata la medesima, ovvero l'obbiettivo di raggiungere il ruolo di leader nella regolazione di questi sistemi a livello globale. Questo è in particolare uno dei tre punti sul quale i vari Paesi stanno competendo, in accordo col livello di sviluppo di questi sistemi, e il ritmo col quale essi vengono sviluppati. Al momento la RPC è al primo posto[41] per ritmo di sviluppo, e solo dietro agli Stati Uniti come livello di sviluppo di tali sistemi, un obbiettivo che mira a superare nel prossimo decennio tramite l'infinito ammontare di dati in loro possesso grazie all'attuale sistema di sorveglianza di massa. Allo stesso modo presenta una posizione dominante anche in merito allo sviluppo di regolamentazioni concernenti l'intelligenza artificiale, stando sullo stesso piano dell'Unione ma con alcune peculiari differenze strutturali e di fine. L'avvio nella produzione di queste complesse e numerose regolamentazioni è cominciato nel 2017, con l'approvazione del *"New Generation Artificial Intelligence Development Plan",* un piano di sviluppo che aveva l'obbiettivo prioritario della produzione e innovazione di suddetti sistemi, con lo scopo di innalzare la Repubblica Popolare ad un ruolo di leader mondiale nel settore entro l'anno 2030. Questo piano di sviluppo prevedeva un insieme di step, cominciati con la pubblicazione di linee guida etiche nel 2018 a cura di una coalizione di accademie, università e leader cinesi nell'industria dell'I.A., che sono poi terminati nell'approvazione del *"Beijing Artificial Intelligence*

[41] I.A. FILIPOVA, *Legal Regulation of Artificial Intelligence: Experience of China, Journal of digital technologies and law*, 2/2024, 3, reperibile a questo link.

Principles" nel 2019[42]. Successivamente è doveroso menzionare le tre normative principali della Repubblica Popolare, ovvero la *Cybersecurity Law*, entrata in vigore nel 2017, la *Data Security Law*, approvata nel 2021, e la *Personal Information Protection Law*, anch'essa approvata nel 2021. La combinazione di queste ultime compone il robusto e interconnesso *framework* normativo atto a stabilire principi, obbiettivi, poteri e responsabilità per la protezione dei dati personali e la salvaguardia della sicurezza nazionale. È importante specificare che il ruolo principale di queste normative non è quello di regolare questioni predeterminate ma di stabilire i principi sulla quale basare le successive valutazioni caso per caso, che vengono protratte da diverse autorità di regolamentazione statali, primo tra tutti il *"Cyberspace Administration of China"*.

Il primo tra questi, ovvero il *Cybersecurity act*[43], è stato approvato nel novembre del 2016 e presenta 79 articoli divisi in 7 capitoli[44]. I dettami della normativa si articolano nell'esposizione dei principi di sicurezza informatica e sicurezza delle informazioni in rete, e tra i suoi obbiettivi principali infatti si ritrovano la protezione delle operazioni in rete, la protezione dei dati e la tutela della sovranità cibernetica nazionale. Con esso vengono inoltre introdotte ampie definizioni e prescrizioni per i vari operatori di rete e in particolare per i "*critical information infrastructure operators"* (CIIOs, includono enti operativi in attività di servizi energetici, finanza e pubblici servizi), sui quali vengono imposti requisiti stringenti in materia di sicurezza di rete, localizzazione dei dati e trasferimento dei dati oltre i confini nazionali.

Successivamente nel 2021 sono state approvate due diverse normative, prima tra le due la *Data Security Law*[45], operativa da settembre 2021. Essa è composta da

---

[42] I.A. FILIPOVA, *Legal Regulation of Artificial Intelligence: Experience of China*, *cit.*, 4-6, reperibile a questo link.
[43] *What are the distinctions between China's Cybersecurity Law, Data Security Law and PIPL?*, *Hi-com*, 11/2025, reperibile a questo link.
[44] Testo ufficiale Cybersecurity Law cinese del 11/2016, reperibile a questo link.
[45] I.A. FILIPOVA, *Legal Regulation of Artificial Intelligence: Experience of China*, *cit.*, 02/2024, 4-6.

55 articoli suddivisi in 7 capitoli[46], e rappresenta un ulteriore evoluzione nei sistemi di *governance* dei dati in circolazione nella Repubblica Popolare. Vi è infatti non più una semplice concentrazione sulla sicurezza di rete come previsto dalla normativa precedente ma è lo stesso dato che diviene oggetto centrale, per il quale viene istituito un sistema di categorizzazione nazionale[47] e protezione gerarchica, che classifica i dati sulla base della loro importanza in classi quali generali, importanti e CORE Nazionali, con successivi requisiti di sicurezza sempre più stringenti tanto più aumenta l'importanza degli stessi. Tramite queste misure viene quindi ampliata la tutela dei dati nell'interezza delle attività di elaborazione e trattamento degli stessi, una condizione varata sia per le aziende interne alla Repubblica che in alcuni casi anche per quelle esterne ad essa, come ad esempio le attività impegnate in questioni di sicurezza nazionale e interesse pubblico.

E per concludere l'ultima normativa portante del framework normativo cinese è la *Personal Information Protection Law*[48], spesso considerata come la controparte cinese del GDPR. Essa è entrata in vigore a novembre 2021, è composta da 74 articoli suddivisi in 8 capitoli e il suo focus principale è la regolazione concernente la protezione delle informazioni personali, allineandosi agli approcci di regolazione della privacy istituiti a livello globale. Si concentra[49] sulla protezione delle informazioni personali dei residenti sul suolo cinese, e si applica a qualunque ente o individuo che ottiene, utilizza, trasferisce o esterna questi dati. I principi sulla quale viene basata questa normativa, similarmente al GDPR europeo, sono i principi di trasparenza, minimizzazione, limitazioni basate sullo scopo del trattamento, accuratezza, sicurezza e *accountability*. Sulla base di questi principi garantisce poi ai cittadini una serie di diritti connessi alla gestione dei loro dati, come il diritto all'accesso ai dati, alla loro correzione ed

[46] Testo ufficiale Data Security Law cinese del 9/2021, reperibile a questo link
[47] *What are the distinctions between China's Cybersecurity Law, Data Security Law and PIPL?*, cit.
[48] Testo ufficiale Personal Information Protection Law cinese del 11/2021, reperibile a questo link.
[49] *Secure Privacy, Protecting Your Personal Information in the Age of the Personal Information Protection Law (PIPL) by the People's Republic of China, 11/2023,* reperibile a questo link.

eliminazione e la possibilità di opporsi al loro trattamento. A questa normativa devono adeguarsi tutti quegli enti che, sebbene pur non residenti sul suolo cinese, trattano dati appartenenti ai cittadini della Repubblica Popolare, e indipendentemente dal tipo di trattamento al quale questi dati sono soggetti e alla grandezza dell'organizzazione. Questo chiaramente fa sorgere delle perplessità in merito al concetto di sovranità statale e delle ulteriori difficoltà per le aziende estere che di conseguenza devono adeguarsi ai dettami della normativa nel caso in cui trattassero dati appartenenti ai suoi cittadini. Per concludere è necessario menzionare che in seguito ai requisiti di compliance vengono poi definiti nello specifico sia quali informazioni personali vengono tutelate e quali invece vengono categorizzate come sensibili e quindi meritevoli di una maggiore tutela e requisiti aggiuntivi per il loro trattamento, in quanto possono causare danno e violazioni alla dignità personale dell'individuo. Il rispetto dei seguenti requisiti e degli obblighi previsti nel trattamento dei dati personali dei cittadini viene gestito dall'autorità nazionale già prima menzionata, che è stata specificamente designata per assicurare l'adeguamento ai principi delle varie normative presentate prime tra tutte la PIPL, con l'ulteriore possibilità di effettuare investigazioni sui casi di violazione e di punirne successivamente i trasgressori, ovvero il *Cyberspace Administration of China* (CAC).

3.4 ELEMENTI DI SVILUPPO TECNOLOGICO, CENTRALIZZAZIONE STATALE E SORVEGLIANZA DI MASSA

L'attuale sistema di sorveglianza e gestione dei dati presenti nell'infosfera attuato nella Repubblica Popolare Cinese presenta delle peculiarità innovative e ambigue rispetto al sistema adottato dai paesi occidentali, che merita una decisa presentazione e analisi di confronto. La Cina già dal 2017 con lo sviluppo del

"New Generation Artificial Intelligence Development Plan"[50] ha iniziato un processo di modernizzazione e innovazione atto all'efficace realizzazione di tre fasi successive, ovvero il perseguimento di una posizione competitiva nel mercato globale, la successiva innovazione nello sviluppo teorico e l'implementazione attiva di tali tecnologie in vari settori dell'economia cinese, e il completamento del piano di sviluppo attraverso il raggiungimento del ruolo di leadership globale nell'industria dei sistemi di intelligenza artificiale. Proprio grazie al sistema messo in atto è riuscita in poco tempo a costruire un nuovo contratto sociale[51] con i suoi cittadini, instaurando uno stato di polizia distopico armato di intelligenza artificiale e sostenuto da pensatori e accademici cinesi nel quale i cittadini si sottomettono al sistema di sorveglianza in cambio di una migliore governance in grado di rendere le loro vite più facili e sicure. Questa peculiare concezione dell'autorità dello Stato rispetto ai cittadini non è solo frutto del corrente modello socialista dominante e delle politiche del presidente Xi, ma ripercorre le sue radici nella filosofia confuciana che prevede una prevaricazione dell'interesse pubblico e dell'armonia collettiva sugli interessi dell'individuo. Ed è proprio sulla base di questi predicamenti che viene giustificato il capillare controllo[52] dei cittadini da parte della Repubblica Popolare. Un esempio lampante può essere ritrovato negli stessi articoli della Costituzione cinese secondo cui come annoverato agli artt. 51, 53 e 54, è previsto che *"i cittadini nell'esercizio dei loro diritti e libertà, non possano violare gli interessi dello Stato, della società o della collettività"*. Vi è quindi una sostanziale mancanza di assolutezza dei diritti umani fondamentali nel caso in cui essi vadano ad intromettersi nell'operato dell'attività politica e organizzativa del partito comunista cinese. Questo modello di sorveglianza viene protratto attraverso l'utilizzo di numerosi e differenti sistemi tecnologici, primo

[50] I.A. FILIPOVA, *Legal Regulation of Artificial Intelligence: Experience of China*, cit., 4.
[51] B. CALDERINI, *Sorveglianza di massa, la Cina è un sistema a "diritti affievoliti": perché lo tolleriamo e cosa rischiamo,* in *Agenda Digitale*, 11/2022, reperibile a questo link.
[52] B. CALDERINI, *Sorveglianza di massa, la Cina è un sistema a "diritti affievoliti": perché lo tolleriamo e cosa rischiamo,* cit.

tra tutti le telecamere a circuito chiuso con sistemi di identificazione biometrica a distanza in tempo reale. Ve ne sono 700 milioni sparse su tutto il suolo della Repubblica, una ogni due abitanti e più della metà di quelle attive a livello globale. Esse sono connesse a un database nazionale che assieme a documenti di identificazione, sistemi di riconoscimento di aziende cinesi, registrazioni di impronte digitali, cronologie di viaggio, etc. istituisce un utile strumento di monitoraggio a favore del governo cinese. Alcune telecamere vengono inoltre installate in posti comuni di svago sia pubblici che privati come ad esempio ristoranti, negozi, sale karaoke e hotel, e dei particolari sistemi come wi-fi sniffer e catcher IMSI raccolgono informazioni dagli smartphones dei cittadini consentendo agli organi di polizia di tracciare i loro movimenti e di andare a costituire nel suo insieme il sistema di sorveglianza anche detto "Xue Liang", ovvero "Occhio di falco", ottimizzato allo scopo di sorvegliare gli 1,4 miliardi di abitanti della Repubblica Popolare. I dati estrapolati vengono poi messi a disposizione delle forze di polizia e a una vasta gamma di terze parti sia pubbliche per scopi di intelligence e sicurezza pubblica, che private per scopi commerciali e di marketing. Un'ulteriore sistema degno di nota è quello costruito dai giganti tech cinesi Alibaba e Tencent[53], che dopo essere stati sottomessi al controllo del partito comunista condividono le loro enormi quantità di dati con il governo. Dal 2016 in particolare nella città di Hangzhou è stata sviluppata da Alibaba la piattaforma cloud *City Brain*, che ha lo scopo di monitorare le condizioni del traffico, rilevare incidenti stradali, regolare i semafori per ridurre i tempi di viaggio e persino i tempi di risposta dei veicoli di emergenza. Vi è quindi un capillare controllo delle città che presumibilmente ha l'opportunità di poter portare grandi vantaggi nella vita dei cittadini grazie alle opere di ottimizzazione, ma che al tempo stesso soprattutto nell'ultimo periodo col miglioramento dei sistemi accresce ulteriori dubbi e dibattiti in merito al

[53] B. CALDERINI, *Sorveglianza di massa, la Cina è un sistema a "diritti affievoliti": perché lo tolleriamo e cosa rischiamo,* cit.

tema della repressione causa eccessivi controlli ai cittadini e successive discriminazioni e privazioni sulla base delle decisioni del partito. Un esempio lampante è quello dell'auto autonoma che controllata da remoto abbia la possibilità di chiudere al proprio interno un cittadino ritenuto pericoloso o contrario al partito e di consegnarlo alle autorità per successive investigazioni contro il suo volere. Un'applicazione che andrebbe contro lo stesso principio di libertà personale dell'individuo, come una sorta di sanzione ingiustificata atta alla detenzione dell'individuo contro il suo volere e spesso senza giustificati motivi. Problematica che può ravvedersi inoltre nei casi di discriminazione e impedita fruizione nell'accesso dei servizi pubblici e nella manipolazione indiretta del comportamento e della scelta degli individui spesso invisibile nei seguenti sistemi. Nei più recenti sviluppi[54], tramite le successive implementazioni e innovazioni dei sistemi I.A. le modalità con cui viene attuata la sorveglianza e l'operato delle forze dell'ordine si sono profondamente trasformate. Mentre in precedenza erano gli stessi agenti a effettuare ronde di controlli e demandare informazioni private ai cittadini in modo da costruire un database condiviso con le generalità degli interessati, adesso la quasi totalità degli stessi è impiegata nel controllo delle città tramite schermi in appositi centri di comando[55]. La maggior parte dei ruoli di controllo è affidata a sistemi I.A. e i ruoli di gestione delle pattuglie prima affidato a operatori umani sta anch'esso progressivamente venendo delegato a questi ultimi, soprattutto grazie allo sviluppo dei cosiddetti *large language models* (LLMs). Gli stessi robot che prima svolgevano un solo ruolo di assistenza, con le ultime innovazioni tecniche saranno in grado di ottenere un ruolo dominante nell'arresto di dissidenti e oppositori. Da queste dimostrazioni si denota la possibilità di un intero apparato di forze dell'ordine completamente gestito da sistemi di intelligenza artificiale, un obbiettivo ora come mai prima realizzabile grazie alla profonda sorveglianza

[54] V. WEBER, *China's AI-powered surveillance State*, in *Journal of Democracy*, volume 36, Number 4, 10/2025.
[55] V. WEBER, *China's AI-powered surveillance State*, cit., 2-4.

in grado di ottenere enormi quantità di dati sulla totalità del suolo cinese. Una prospettiva decisamente invitante per il partito comunista al potere considerati gli immensi costi e sforzi umani impiegati per il corretto funzionamento del sistema, problematica che l'implementazione di un sistema digitale autonomo e con minima partecipazione umana andrebbe parzialmente a risolvere. Gli strumenti utilizzati per il raggiungimento di questo obbiettivo sono droni, robot umanoidi e veicoli autonomi, molti dei quali sono già attivi nella scena urbana e rurale del suolo cinese. Questi ultimi andrebbero a supporto del sistema di sorveglianza già in atto, comprensivo delle 700 milioni di telecamere e gli ulteriori dispositivi quali telefoni e smart watches che già superano il numero degli agenti a disposizione delle forze dell'ordine cinesi. Il cielo è occupato dalla presenza costante di droni, che controllano sia le città che diverse zone rurali, il quale controllo sta diventando sempre più comune. Già un decennio fa il sistema di sorveglianza era in grado di individuare e riconoscere le autovetture, mentre adesso è in grado di fare lo stesso anche con pedoni, ciclisti e il flusso di merci tramite aeroporti e stazioni ferroviarie. Un altro grande vantaggio estrapolabile dell'attuale sistema di sorveglianza[56] sarà quello di permettere al partito di rispondere con maggiore efficacia e velocità alle richieste dei cittadini prima che queste possano trasformarsi in situazioni di dissenso e frustrazione. L'utilizzo di sistemi intelligenti nei servizi municipali e chatbot personalizzati impegnati nel rispondere alle domande del pubblico in merito a questioni amministrative permetterebbe questo particolare scenario. L'ulteriore recente sviluppo del nuovo LLM di DeepSeek determina poi un importante passo avanti nell'operato del controllo dei cittadini. Esso può permettere alle forze di polizia di cercare e individuare un determinato soggetto in mezzo alla folla, e di suggerire le zone calde nel quale distribuire le pattuglie di polizia, trasformando quindi il sistema di sorveglianza in un organo attivo. Un cambiamento che porterebbe impatti significativi nelle libertà dei cittadini, specialmente la libertà di associazione

[56] V. WEBER, *China's AI-powered surveillance State*, cit., 3-5.

legata alle rivolte sfociate nel suolo cinese.

3.5 L'IDENTITÀ DIGITALE COME STRUMENTO DI REPRESSIONE E CENSURA

I sistemi a identificazione biometrica[57] e l'automazione della sorveglianza non sono però gli unici strumenti sulla quale si appoggia l'operato del controllo statale. Da luglio 2025 infatti è stato introdotto un nuovo innovativo sistema di identificazione internet nazionale, che mira alla centralizzazione della verifica dell'identità degli utenti sotto la supervisione governativa. Questo sistema prevede infatti l'utilizzo di un ID digitale internet per accedere a tutte le piattaforme online; lo scopo principale di questa riforma è la protezione delle informazioni identificative[58] dei cittadini, ma allo stesso tempo diverse organizzazioni come il Network of Chinese Human Rights Defenders (CHRD) sollevano delle preoccupazioni sulla possibilità che tale misura possa ulteriormente minare la libertà di espressione online e ostacolare il lavoro dei difensori dei diritti umani. Il rischio principale sempre legato alla centralizzazione statale è la drastica riduzione dell'anonimato, con successivo targeting e censura dei dissidenti al partito. L'adesione viene presentata come volontaria, ma la diffusa adozione di quest'ultimo da parte di diverse piattaforme di servizi pubblici e di uso comune quale WeChat prospetta una stringente necessità di adesione per tutti i cittadini, innalzando ulteriormente il problema relativo alla libertà di scelta, di privacy e di espressione. Questo fenomeno è particolarmente evidenziato nell'art. 3 della misura, il quale incarica i vari dipartimenti del Consiglio di Stato come affari civili, cultura e turismo, radio e

[57] G. IUVINALE, N. IUVINALE, *Cina, la sorveglianza su internet è completa: l'ID digitale universale è schiaffo all'Occidente*, *Agenda Digitale*, 06/2025, reperibile a questo link.
[58] G. IUVINALE, N. IUVINALE, *Cina, la sorveglianza su internet è completa: l'ID digitale universale è schiaffo all'Occidente*, cit.

televisione, sanità, servizi ferroviari e postali, di promuovere e supervisionare l'implementazione della misura. Un ulteriore impatto negativo sorge sui difensori dei diritti umani, in quanto sebbene nell'art. 2 della misura venga affermata la sua importanza per la protezione della privacy e l'eliminazione di informazioni esplicite, il requisito per l'utilizzo di tali sistemi richiede agli utenti di fornire un'identificazione legale valida e di sottoporsi a riconoscimento facciale. È infatti già nota la diffusa e frequente repressione di attivisti e giornalisti da parte delle forze di polizia cinesi che spesso sfocia in casi di censura, restrizioni e arresti, e le seguenti modifiche ne renderanno ancora più facile il controllo e l'intervento immediato in tal senso. Questo chiaramente complicherà lo svolgimento delle attività essenziali quali la condivisione di informazioni sensibili, il mantenimento di comunicazioni sicure con le vittime di violazioni dei diritti e la creazione di reti con altri difensori per paura di successive ritorsioni. E non solo, perché trattandosi di un ID unico utilizzato su tutte le piattaforme[59] controllate dalle autorità cinesi, la condivisione di opinioni negative o dissidenti anche su un solo social network può prevedere l'eliminazione totale dell'ID digitale e del suo accesso a tutte le piattaforme online con estrema facilità, facendo sorgere ulteriori criticità sui principi della libertà d'espressione e la libertà di accesso ad internet. Allo stesso modo vi sono alte preoccupazioni in materia di privacy, in quanto sebbene l'art. 7 della stessa misura preveda la proibizione alle piattaforme di richiedere ulteriori informazioni personali agli utenti una volta adottato il nuovo sistema, questo fattore rappresenta comunque un altro elemento di centralizzazione delle informazioni sotto il controllo governativo. Sembra vi sia un rimedio previsto sulla seguente questione all'art. 10 della misura che richiede alle autorità di informare gli utenti su come i loro dati personali vengono utilizzati, ma allo stesso tempo all'articolo successivo la trasparenza viene meno a causa delle ampie esenzioni concesse per cosiddette "questioni riservate". Questo

[59] G. IUVINALE, N. IUVINALE, *Cina, la sorveglianza su internet è completa: l'ID digitale universale è schiaffo all'Occidente*, cit.

chiaramente fa sorgere di nuovo ulteriori preoccupazioni per la privacy degli utenti, cosa che nuovamente è di difficile segnalazione in quanto come menzionato pocanzi gli stessi attivisti e difensori dei diritti umani, con aggiuntiva difficoltà a causa delle qui descritte concessioni normative, possono essere monitorati e analizzati sulla base di semplici sospetti di "incitamento alla sovversione". Una delle questioni più spinose però è la potenzialità del sistema di infierire nella sovranità statale altrui. Questione riscontrabile *in primis* nello stesso articolo 15 della misura, che nonostante la differenza di giurisdizione per l'ottenimento del numero web e del certificato dell'ID digitale è necessario fornire l'identificazione per i cittadini cinesi residenti all'interno o all'esterno della Cina, i permessi di viaggio e di residenza o le carte d'identità di residenza permanente. Questa clausola tuttavia esclude i confini nazionali della Cina, applicandosi anche a regioni dove le leggi e i regolamenti sottostanti della misura non si applicano. Una chiara violazione dei limiti di sovranità che permetterebbe allo stesso governo cinese di individuare e perseguitare soggetti dissidenti anche al di fuori dei propri confini. Sono stati infatti documentati[60], in particolare da un'indagine *dell'International Consortium of Investigative Journalists* (ICIJ), numerosi casi di azioni punitive anche oltreconfine, colpendo dissidenti, minoranze etniche e attivisti rifugiati all'estero con l'uso di intimidazioni, strumenti legali e diplomatici. Tra le azioni riportate risultano molestie di vario genere, tra cui pedinamenti, minacce fisiche e aggressioni, e-mail sospette e attacchi informatici riconducibili ad attori statali, e frequenti pressioni e interrogatori anche contro i familiari.

[60] A. COLARIZI, *Cina, la repressione diventa globale: minacce, arresti e pressioni anche all'estero*, cit.

3.6 IL SOCIAL SCORING QUALE PRINCIPALE STRUMENTO DI DISCRIMINAZIONE DERIVATO DA SORVEGLIANZA E ASIMMETRIA INFORMATIVA

Il social scoring[61] è un sistema di valutazione creditizia attribuita a determinati soggetti sulla base di loro comportamenti, informazioni e dati, in questa sede principalmente ottenuti mediante l'utilizzo di sistemi di sorveglianza. Inizialmente è stato introdotto nei primi anni 2000 come sistema di credito finanziario, ma solo dopo l'approvazione del Programma di azione 2014-2020 del governo centrale vi è stata la costruzione del sistema di credito sociale come conosciuto ai giorni nostri. È cominciato infatti attraverso la formulazione di diverse regole e obbiettivi settoriali e regionali caratterizzati da uno sviluppo graduale fino al raggiungimento di una condivisa struttura definitiva composta da numerosi standard nel 2020. Il sistema[62] è stato riunito e messo in atto dalle autorità statali con l'obbiettivo di monitorare e valutare i comportamenti degli individui sulla base di una serie di standard nazionali imposti di "fedeltà allo Stato" e che mirano a venire modificati con l'applicazione di sanzioni e ricompense. Le tre principali funzioni prominenti del social scoring sono:

- la fornitura e la regolazione dei rating di credito finanziario;
- la regolazione del mercato e la governance sociale;
- la promozione di valori approvati dallo Stato

Il primo di questi fa riferimento all'utilizzo del sistema di credito nella valutazione dei rating creditizi tipica delle banche e dei centri adibiti al credito,

---

[61] A.S.Y. CHEUNG, Y CHEN, *From Datafication to Data State: Making Sense of China's Social Credit System and Its Implications*, in *Cambridge University press: law & social inquiry*, volume 47, issue 4, 11/2022, reperibile a questo link.

[62] A.S.Y. CHEUNG, Y CHEN, *From Datafication to Data State: Making Sense of China's Social Credit System and Its Implications*, cit., 1-6.

precedentemente governata dal sistema occidentale ma che è stata, successivamente al "piano di azione" del 2014, profondamente rinnovata. In secondo piano esso si è esteso dalla sua semplice accezione relativa al credito finanziario, espandendosi anche come valutazione comportamentale riguardante tematiche come l'interesse pubblico, la sicurezza sociale e l'applicazione di leggi, norme regolamentari e affidabilità sociale. Infine la terza funzione fa riferimento a un aggiuntivo fattore di valutazione dell'affidabilità, ma legato alla conformità degli individui con il rispetto dei valori socialisti ufficialmente espressi dallo Stato.

I meccanismi centrali che permettono il funzionamento di questo sistema sono due, ovvero;

- punizioni e ricompense elargite dallo Stato sulla base del comportamento individuale;
- un'unica infrastruttura di dati statale;

Il primo di questi meccanismi[63] è combinato in quanto intrapreso da multiple autorità statali sia a livello regionale che settoriale, e prevede una differenza dei comportamenti da monitorare sulla base delle regole presenti nelle rispettive giurisdizioni. Diversamente il secondo meccanismo prevede un'infrastruttura composta da due diversi databases, uno, il "National Basic Database for Financial Credit Information", che viene utilizzato per l'aggregazione di dati rilevanti per la stima dei rating di affidabilità finanziaria, e l'altro, il "National Credit Information Sharing Platform", che aggrega dati relativi alla generale affidabilità dei cittadini in senso ampio.

In seguito all'approvazione del sistema a ciascuno dei cittadini è stato dato un "social credit unified code", ovvero un codice identificativo a 18 cifre che ha semplificato l'aggregazione e la sincronizzazione dei dati grazie alla sua

[63] A.S.Y. CHEUNG, Y CHEN, *From Datafication to Data State: Making Sense of China's Social Credit System and Its Implications*, cit., 10-12.

uguaglianza con il codice delle carte d'identità di residenza, già associate a un insieme di dati personali. Sulla base dei comportamenti messi in atto dai cittadini vi sono due cataloghi nella quale possono essere categorizzati, ovvero la "black list" o la "red list". La "black list" è la lista riservata a coloro che mettono in atto comportamenti negativi a danno dello Stato e della società, i quali come previsto dalle linee guida nazionali emanate rientrano in quattro tipologie, ovvero:

- mettere in pericolo la salute, la vita o la sicurezza;
- minare severamente l'ordine del mercato o il regolare ordine sociale;
- il rifiuto di attuazione di doveri imposti da autorità amministrative o giudiziali;
- sottrarsi a obblighi di difesa nazionale o danneggiare gli interessi della stessa

L'inosservanza[64] delle regole prevede una serie di punizioni intra-settore o nei casi più gravi la stretta sorveglianza dell'interessato. Queste punizioni anche se effettuate in una sola area settoriale o geografica vengono riconnesse anche a uno o più soggetti al di fuori di quell'area, per fare in modo che tali complicazioni si riversino su tutte le sfaccettature della vita del soggetto e ovunque esso vada. Lo Stato ha inoltre la possibilità di pubblicare i nomi dei cittadini inseriti all'interno di queste liste nere e di condividerli attraverso diversi media online, primo tra tutti il portale nazionale "Credit China". Una questione particolarmente rilevante soprattutto per gli attivisti dei diritti umani, è quella delle frequenti discriminazioni causate dai sistemi di social scoring a danno delle minoranze etniche, in particolare i musulmani uiguri.

La "red list" invece è la lista adottata per la categorizzazione dei cittadini meritevoli che hanno messo in atto comportamenti positivi e basati sui valori statali, e per il quale meritano l'attribuzione di incentivi. Questi ultimi ricadono

[64] A.S.Y. CHEUNG, Y CHEN, *From Datafication to Data State: Making Sense of China's Social Credit System and Its Implications*, cit., 11-14.

generalmente in tre categorie:

- misure preferenziali nei processi amministrativi;
- vantaggi relativi ai pubblici servizi;
- maggiore possibilità di ottenere ricompense.

L'attuale sistema di credito sociale cinese è quindi così composto, ed è di fronte alla sua presenza che le democrazie occidentali devono ripensare alle meccaniche di gestione dei dati personali dei cittadini e al loro sfruttamento. Nonostante questi sistemi possano sembrare tanto lontani da noi la grande quantità di dati che gli Stati europei sono stati in grado di estrapolare nel corso e dopo la pandemia di Covid-19, specialmente dati sensibili dei cittadini come geolocalizzazione, contatti sociali, salute e cartella medica, possono diventare un fattore fondamentale per il rischio di una governance eccessivamente pervasiva e scorretta di tali dati e risultare terreno fertile per la formazione di un'organizzazione dell'anticipazione e della sorveglianza.

Secondariamente, un tema emerso dall'osservazione di diversi fenomeni empirici è il quasi totale appoggio della popolazione cinese (80%) in favore del sistema di credito sociale[65] assegnato ai cittadini. I principali fattori che permetterebbero un tale risultato di fronte alle dimostrate ripercussioni negative dell'applicazione di tali sistemi, si possono ritrovare in due meccanismi:

- i cittadini sembrano disposti e consapevoli nel rinunciare alla libertà politica in cambio di sicurezza personale, maggiore efficienza e benessere sociale. Questo fattore, tuttavia, può garantire la sua corretta applicazione solo nel caso in cui vi sia una piena conoscenza delle sue implicazioni da parte della società civile, una cosa che purtroppo non accade e che anzi viene pregiudicata dal fattore successivo;
- il governo cinese manipola l'informazione e le notizie condivise sui

[65] X. XU, G. KOSTKA, X. CAO, *Information Control and Public Support for Social Credit Systems in China*, in *University of Chicago press, The Journal of politics*, 08/2022, reperibile a questo link.

media, promuovendo la buona immagine del partito e della figura del sistema di credito sociale quale strumento fondamentale per garantire la moralità e la rispettiva fiducia sociale, e allo stesso tempo censurando tutte le notizie che raffigurano il social scoring quale strumento di repressione. La manipolazione della consapevolezza collettiva rispetto ai risvolti negativi del sistema presenta poi un ulteriore strato di complessità, in quanto le stesse sanzioni elargite ai cittadini ritenuti non meritevoli si distinguono dalla coercizione fisica e l'arresto, e si applicano attraverso differenti metodi come l'esclusione di prestiti bancari, la riduzione della velocità internet o la totale rimozione da alcune piattaforme. Questi metodi infatti risultano meno evidenti rispetto alla visibile violenza fisica, e ricevendo minore attenzione rendono più difficile al resto della popolazione vedere e comprendere ciò che il sistema comporta.

4. PRINCIPI NORMATIVI E TUTELE A CONFRONTO

È doveroso ora completare l'analisi dei due modelli attraverso un adeguato e breve confronto degli elementi che li caratterizzano. Innanzitutto, è innegabile la predisposizione del modello europeo per una posizione garantista sempre concentrata sul rispetto dei diritti umani fondamentali e la limitazione dei possibili casi di violazione di questi ultimi. L'approccio normativo adottato infatti tutela i soggetti dalle diverse criticità relative all'utilizzo dei sistemi di intelligenza artificiale individuandone diverse categorie di rischio, e si concentra sulla protezione dei dati degli individui attraverso una serie di misure che mirano al controllo diretto dei dati da parte degli individui attraverso l'espressione del proprio consenso al trattamento, e alla trasparenza dei contenuti di cui essi dispongono nelle varie piattaforme online. Diversamente la Cina presenta un modello basato sul controllo centralizzato dello Stato sull'infosfera nazionale,

con un coinvolgimento diretto del governo nei processi digitali. Enormi quantità di dati vengono estrapolati dai vari sistemi di sorveglianza, quali telecamere con identificazione biometrica, droni, robot e sistemi internet come l'identità digitale. Queste enormi quantità di dati permettono allo Stato cinese un'enorme efficienza e sviluppo innovativo, riscontrabile anche nell'intelligente gestione delle città tramite software di controllo, la riduzione della microcriminalità e l'alto sviluppo sia degli stessi sistemi intelligenti che del sistema economico nazionale, che ha reso la Cina una tra le più importanti potenze globali del nostro tempo. A questo proposito tuttavia vi sono pareri contrastanti in merito all'utilizzo di questi sistemi, tra soggetti che si dichiarano favorevoli a mettere a disposizione i propri dati per la creazione di un "ecosistema" più semplice e sano, e coloro che invece non sono d'accordo nel trattamento massivo degli stessi e che non ritengono che i benefici derivanti dalla sorveglianza di massa siano sufficienti a giustificare le violazioni della tutela della propria privacy e di altri diritti fondamentali. Confrontando nello specifico le varie normative a disposizione di ambo le parti, possiamo osservare dettagliatamente come le stesse questioni vengano regolate in modo peculiarmente diverso. Ad esempio mentre nella nostra organizzazione sovranazionale è presente la Carta dei diritti fondamentali dell'Unione Europea (CDFUE), che tutela imprescindibilmente determinati diritti fondamentali, quali tra i più rilevanti ai fini di quest'analisi il diritto alla libertà e alla sicurezza (art.6), il rispetto della vita privata e familiare (art. 7), la libertà di pensiero e di coscienza (art. 10), la libertà d'espressione e informazione (art. 11), la non discriminazione su ogni base (art. 21), la sicurezza sociale e assistenza sociale (art. 34) e il diritto di voto (art. 40); la Costituzione della RPC nonostante le diverse sottoscrizioni di importanti dichiarazioni internazionali dell'ONU[66] e le numerose riforme e revisioni atte a superare l'approccio collettivistico in favore di un'ottica maggiormente occidentale, presenta ancora molteplici criticità. Andando per ordine, l'art. 35 della Costituzione del 1982 garantisce la libertà di

[66] R.TARCHI (a cura di), *Appunti di diritto cinese,* cit., 48-50, reperibile a questo link

espressione, di stampa, di associazione e di dimostrazione. La questione viene inoltre ampliata poi all'art. 41, che al primo comma esprime il diritto dei cittadini di criticare e di rivolgere suggerimenti agli organi dello Stato e ai singoli funzionari, con l'unico limite del divieto di costruire e alterare i fatti allo scopo di diffamare o creare montature. Una formulazione che non sembra voler integrare vincoli e restrizioni ingiustificati, i quali vengono tuttavia ripresi in seguito. All'art. 51[67] infatti si afferma come il godimento di tali diritti non sia assoluto, in quanto "non deve violare gli interessi dello Stato, della società, della collettività, nonché i diritti e le libertà degli altri cittadini", mentre l'art. 52 prevede che le autorità cinesi si riservano di sanzionare e censurare qualsiasi espressione, scritta o orale, che esse ritengano in grado di minare "l'unità e l'integrità della nazione". Delle prescrizioni piuttosto generiche che lasciano ampio spazio a interpretazioni soggettive e che in generale dimostrano la diffusa mancanza di assolutezza dei diritti fondamentali nella concezione cinese, permettendo la possibilità di violazione degli stessi. Riprendendo quanto indicato prima per la CDFUE, molteplici sono le implicazioni e violazioni che scaturiscono per i diritti fondamentali dall'utilizzo degli attuali sistemi di sorveglianza e controllo della Repubblica Popolare. Il diritto alla libertà e alla sicurezza anche se garantito può venir utilizzato come pretesto da parte delle autorità nazionali per perpetrare l'abuso indiscriminato dei sistemi di sorveglianza e controllo anche nel trattamento di dati biometrici e sensibili di vario tipo. Il rispetto della vita privata e familiare può venire meno a causa delle molteplici violazioni della privacy riscontrabili dall'utilizzo dei sistemi di sorveglianza non solo per le strade cittadine ma anche in luoghi privati e di svago come hotel, ristoranti, negozi e sale karaoke, e dalle implicazioni derivanti dalla mancanza di anonimato nell'ID digitale, requisito ormai fondamentale per l'utilizzo di servizi pubblici e piattaforme social. La libertà di espressione e informazione e di conseguenza la libertà di pensiero sono oltremodo altamente

[67] R.TARCHI (a cura di), *Appunti di diritto cinese,* cit., 51 (Reperibile al seguente link)

manipolabili, a causa di diversi fattori tra cui la filtrazione delle informazioni e la manipolazione delle notizie da parte del partito limitando il pluralismo, e la censura di dissidenti e attivisti attraverso il blocco dell'ID digitale e l'impedimento dell'accesso alle principali piattaforme, con conseguenti minacce e persecuzioni. Lo stesso diritto alla non discriminazione è stato più volte ripreso soprattutto dai numerosi attivisti, in quanto a causa del sistema di credito sociale possono verificarsi sproporzionati casi di pene ed esclusioni dall'utilizzo dei servizi pubblici, prevalenza del soggetto-dato e della sua rappresentazione rispetto alla controparte reale, e repressioni e crimini specialmente perpetrati verso minoranze etniche come, ad esempio, quella dei musulmani uiguri. Il diritto al voto similarmente presenta una garanzia fallace, data dalla filtrazione dell'informazione e dalla diffusa censura utilizzati come mezzi per la promozione del partito unico, creando fenomeni quali *filter bubbles* e situazioni di pseudo-indottrinamento, spesso perpetrato anche in centri dediti alla riabilitazione dei soggetti dissidenti e oppositori al partito.

Le nuove normative in tema di intelligenza artificiale e protezione dei dati allo stesso modo presentano delle differenze sostanziali nella formulazione delle prescrizioni e gli obbiettivi da perseguire sulla base dei fini ultimi del modello. Un primo confronto esemplare può essere ricavato tra i dettami dell'AI Act e le pratiche quotidiane della Repubblica Popolare in materia di sorveglianza. L'AI Act infatti all'art. 5 comma 1 lettere a, c e d esprime rispettivamente il divieto di utilizzo di sistemi di intelligenza artificiale che utilizzano modalità atte alla manipolazione e al potenziale sfruttamento di vulnerabilità del soggetto, all'utilizzo di sistemi social scoring da parte delle autorità a causa dei frequenti problemi di discriminazione, e l'utilizzo di sistemi a identificazione biometrica remota negli spazi pubblici. Un bagaglio di prescrizioni che certamente trova forti discrepanze con l'operato della Repubblica Popolare, la quale è rinomata per l'utilizzo diffuso di questi sistemi nella quotidiana amministrazione statale, con conseguenti numerose violazioni dei diritti umani fondamentali. Lo stesso concetto viene poi rimarcato anche dall'art. 9 del GDPR che proibisce il

trattamento di determinate categorie di dati personali, tra cui i biometrici. Una somiglianza che invece dimostra la forte influenza del GDPR nel panorama normativo cinese e in particolare nella PIPL è la condivisa presenza di un'autorità indipendente adibita alla protezione dei dati. Sia all'art. 51 del GDPR che all'art. 60 della PIPL[68], infatti, viene prescritta l'istituzione di autorità di controllo che monitorino il rispetto dell'applicazione del rispettivo regolamento e la protezione dei dati, con una multipla gestione decentralizzata in ogni Stato nel caso dell'Unione, e la fondazione del Cyberspace Administration of China (CAC) nel caso della Repubblica Popolare. Un'ulteriore osservazione delle modalità operative cinesi di gestione dei dati può essere trovata nell'analisi combinata dell'art. 37 della Cybersecurity Law[69] e degli art. 21 e 36 della Data Security Law[70] (DSL). Questi infatti rispettivamente esprimono, *in primis* l'obbligo degli operatori di rete di archiviare e conservare i dati ottenuti e prodotti nel corso delle attività all'interno del territorio cinese, e successivamente nel caso della DSL prima la classificazione dei dati sulla base dell'importanza in "importanti" e "CORE Nazionali", e infine il divieto di condivisione dei dati personali conservati nella RPC ai paesi stranieri, se non su preventiva approvazione delle autorità competenti. Possiamo quindi osservare un approccio protezionistico e quasi egoistico ai dati, alimentato dalla centralizzazione statale e la forte necessità di un vantaggio competitivo offerto dalla massiccia presenza dei dati nazionali, fattore sfruttabile e garanzia di forte sviluppo e facile adattamento alle avversità. Diversamente in Europa, specialmente come previsto dall'art. 44 e 45 del GDPR, nel caso del trasferimento di dati personali all'interno dell'Unione non sono necessarie specifiche autorizzazioni, ma è doveroso verificare che lo Stato al quale vengono trasferiti tali dati garantisca un livello di protezione adeguato, cautamente vagliato secondo una serie di requisiti esposti alle lettere successive del comma 2. Un'addizionale differenza è

[68] Personal Information Protection Law cinese del 11/2021.
[69] Art. 37 Cybersecurity Law cinese del 11/2016.
[70] Art. 21 e 36 Data Security Law cinese del 9/2021.

riscontrabile poi nel trattamento dei dati e i suoi requisiti. All'art. 6 del GDPR infatti è prevista la liceità del trattamento solo sotto specificate condizioni ovvero il consenso e l'interesse legittimo, se non in casi emergenziali di pericolo del l'interessato o di sicurezza pubblica, mentre all'art. 13 della PIPL[71] sebbene sia allo stesso modo previsto il requisito del consenso e la delega per casi di emergenza, il successivo caso descritto ma non specificato di usi statali o legali quali elementi di prevaricazione del consenso lascia ampio spazio a possibilità di violazioni dei limiti del trattamento e potenziali rischi di pregiudicazioni dei diritti fondamentali. Infine mentre secondo quando descritto dai dettami del Digital Service Act (DSA) all'art. 26 e 27 le piattaforme non avrebbero un ruolo di subordinazione e cooperazione statale ma i loro unici obblighi sono quelli di trasparenza e chiarezza sia nei parametri dei loro sistemi di raccomandazione algoritmica che nella presentazione delle pubblicità, la CSL cinese all'art 28[72] prevede il supporto tecnico degli operatori di rete alle autorità di sicurezza nazionale, e all'art. 47 chiarisce l'obbligo degli stessi di interruzione delle trasmissioni, conservazione dei registri e segnalazione alle autorità competenti di qualunque possibile ritrovamento di informazioni che la legge vieta in alcun modo di pubblicare o trasmettere. Questa differente formulazione permette di scorgere ancora una volta la subordinazione di operatori di rete, piattaforme e aziende cinesi al volere statale. Un rapporto necessario alla totale pervasività della sorveglianza sui cittadini, controllandone le attività in rete e garantendo la prosecuzione del tanto nominato Great Firewall che blocca e censura le opinioni opposte al partito e garantisce la sicurezza nazionale pilastro del vivere cinese.

[71] Art. 13 Personal Information Protection Law cinese del 11/2021.
[72] Art. 28 e 47 Cybersecurity Law cinese del 11/2016.

5. CONCLUSIONI

L'analisi qui formulata permette una chiara visione del complesso e differente panorama normativo e filosofico dei due modelli. L'Unione Europea con un approccio maggiormente garantistico e orientato alla tutela dei diritti umani fondamentali e la Repubblica Popolare Cinese con la sua predisposizione a un approccio prevalentemente stato-centrico e dato-centrico, concentrato sul mantenimento del potere da parte del partito comunista, il primato dello status di potenza a livello mondiale e la forte sorveglianza atta a garantire una maggiore efficienza e controllo, sebbene spesso a discapito della tutela dei diritti. Nonostante la differenza di approccio e tutela già menzionate, è necessario rendere atto del diverso percorso che ha caratterizzato l'evoluzione della Repubblica Popolare; la stessa cultura millenaria basata sulla dottrina confuciana ha dapprima infatti gettato le basi per una concezione di prevaricazione dello Stato e dell'armonia sociale sull'individuo, e la stessa ha inoltre subito, nonostante la progressiva dispersione temporale, una rinascita con la riforma socialista del 1949. L'ingresso poi di una serie di leader politici tra i quali l'attuale presidente in carica Xi Jinping ha favorito la proliferazione di politiche socialiste e con quest'ultimo in particolare la formazione di un regime caratterizzato da una forte concentrazione del potere come leader di partito, Stato ed esercito. Questi fattori hanno contribuito alla creazione della Repubblica Popolare Cinese che conosciamo oggi, modificata e migliorata poi attraverso l'utilizzo dei sistemi di sorveglianza che si dimostrano una risorsa preziosa nell'elaborazione della grande mole di dati che permette alla stessa di ottenere ulteriori molteplici vantaggi competitivi a livello globale. Vi è quindi la presenza di una storia di tradizione forte che ha plasmato la visione dell'importanza dell'individuo nel corso del tempo, già anticipando una prevaricazione degli interessi collettivi sul singolo e una concezione superflua e impoverita dei diritti umani, che verrà infatti ripreso solo negli anni Ottanta e con le numerose approvazioni e riforme della Costituzione. L'attuale sistema di sorveglianza

cinese come già menzionato in precedenza pregiudica la tutela di numerosi diritti e il corretto esercizio delle libertà, tra cui il diritto alla privacy e alla vita privata, il diritto alla non discriminazione, la protezione dei dati personali, la libertà di espressione e associazione, la libertà di pensiero e informazione, il diritto di voto e il diritto alla sicurezza e assistenza sociale. Di fronte a tali violazioni, è nostro dovere in quanto cittadini di una democrazia quello di osservare ciò che ci circonda e prenderne ispirazione per la gestione delle nostre politiche statali e comunitarie, ponendoci le giuste domande e riflettendo sul rispettivo assetto con l'obbiettivo di raggiungere la massima efficienza e garanzia possibile. Dovremmo prendere la Cina come modello lontano e da non imitare nel trattamento dei diritti umani fondamentali, ma allo stesso tempo rivolgerci con occhio critico anche in merito alle ulteriori questioni che caratterizzano le differenze sostanziali dei due modelli. Ad esempio, nonostante la deriva dei diritti umani, è innegabile riconoscere l'incredibile sviluppo tecnologico garantito dalle politiche messe in atto dalla Repubblica Popolare Cinese, la sorprendente gestione e ottimizzazione delle città sia per quanto riguarda la qualità di vita che il basso tasso di criminalità, i vantaggi e privilegi per i cittadini "virtuosi" e una maggiore efficienza amministrativa e commerciale. I lati positivi sono numerosi ma spesso vengono offerti ad alti costi, tra cui quelli già pocanzi menzionati. È proprio qui che occorre ragionare sul connubio efficienza/garanzia o libertà/sicurezza nel quale gli Stati occidentali intendono cimentarsi, ricercando quindi una maggiore efficacia ma senza pur sempre cadere nelle possibili derive autoritarie o lesive come possibili conseguenze dell'utilizzo indiscriminato di questi sistemi. Un'altra riflessione peculiare sempre a questo proposito è l'opinione dei cittadini dell'Unione sul qui presente tema. Alla luce del diffuso scetticismo verso l'inefficienza e la lentezza delle istituzioni governative, sarebbero favorevoli i cittadini europei alla sottile compromissione dei loro diritti fondamentali in cambio di una migliore amministrazione, migliore qualità della vita e dei servizi pubblici e una maggiore sicurezza? O si verificherebbe lo stesso fenomeno presente nella Repubblica Popolare, con un

condiviso appoggio delle politiche governative e di sorveglianza semplicemente alimentato dalla diffusa disinformazione e mancata consapevolezza dei lati negativi conseguenti all'utilizzo di tali sistemi? Quesiti incerti ma che sicuramente portano aggiuntive riflessioni utili, nel quale è necessario cimentarsi per poter comprendere a pieno le implicazioni estrapolabili dalle nostre scelte e permetterci di intraprendere con più consapevolezza e sicurezza la strada da perseguire per il nostro futuro.

6. BIBLIOGRAFIA

- A. ADINOLFI, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione: considerazioni sulla (difficile) costruzione di un quadro normativo dell'Unione,* in ASTRID – A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Bologna, 2022,

- A. COLARIZI, *Cina, la repressione diventa globale: minacce, arresti e pressioni anche all'estero*, in *Gariwo Magazine*, 05/2025 https://it.gariwo.net/magazine/diritti-umani-e-crimini-contro-lumanita/cina-la-repressione-diventa-globale-minacce-arresti-e-pressioni-anche-allestero-28592.html

- A. COLARIZI, *la storia della Cina con la lente dei diritti umani*, in *Gariwo Magazine*, 04/2023 https://it.gariwo.net/magazine/editoriali/la-storia-della-cina-con-la-lente-dei-diritti-umani-26104.html

- A. D'ALOIA, *Ripensare il diritto nel tempo dell'intelligenza artificiale*, in ASTRID – A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Bologna, 2022

- A.M. ALAIMO, *Il Regolamento sull'Intelligenza Artificiale. Un treno al traguardo con alcuni vagoni rimasti fermi*, in *federalismi.it*, 10/2024

- A.S.Y. CHEUNG, Y CHEN, *From Datafication to Data State: Making Sense of China's Social Credit System and Its Implications*, *Cambridge University press: law & social inquiry*, volume 47, issue 4, 11/2022 https://www.cambridge.org/core/journals/law-and-social-inquiry/article/from-datafication-to-data-state-making-sense-of-chinas-social-credit-system-and-its-implications/EDF66228C909BE5A24180EFC1904BE00

- B. CALDERINI, *Sorveglianza di massa, la Cina è un sistema a "diritti affievoliti": perché lo tolleriamo e cosa rischiamo, Agenda Digitale*, 11/2022 Sorveglianza di massa, la Cina è un sistema a "diritti affievoliti": perché lo tolleriamo e cosa rischiamo - Agenda Digitale

- B. HAN, *Perché oggi non è possibile una rivoluzione*, Milano, 2022

- C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *federalismi.it*, 11/2018

- Carta dei diritti fondamentali dell'Unione Europea, Nizza, 2000 https://www.europarl.europa.eu/charter/pdf/text_it.pdf

- D. NERI, *Filosofia morale. Manuale introduttivo*, Milano, 2013

- E.C. RAFFIOTTA, M. BARONI, *intelligenza artificiale, strumenti di identificazione e tutela dell'identità*, in ASTRID – A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Bologna, 2022

- E. LONGO, *I processi decisionali automatizzati e il diritto alla spiegazione*, in ASTRID – A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Bologna, 2022

- European Convention on Human Rights, Roma, 1950, https://www.echr.coe.int/documents/d/echr/Convention_ITA

- F. MOLLO, *Il trattamento dei dati biometrici nell'IA Act: intersezioni tra la normativa di protezione dei dati e la nuova disciplina europea dell'intelligenza artificiale*, in *federalismi.it*, 11/2024

- F. MOLLO, *Sorveglianza di massa, rispetto della vita privata e trattamento di categorie particolari di dati nel quadro multilivello di tutela della persona*, in *federalismi.it, 07/2023*
- F.M. MANCIOPPI, *La regolamentazione dell'intelligenza artificiale come opzione per la salvaguardia dei valori fondamentali dell'UE*, in *federalismi.it, 03/2024*

- G. D'ACQUISTO, C.A. TROVATO, L. DE BENEDETTI, *Alcune riflessioni sul concetto di autonomia decisionale della macchina e sulle sue implicazioni regolamentari*, in ASTRID – A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Bologna, 2022

- G. IUVINALE, N. IUVINALE, *Cina, la sorveglianza su internet è completa: l'ID digitale universale è schiaffo all'Occidente*, *Agenda Digitale*, 06/2025
  Cina, la sorveglianza su internet è completa: l'ID digitale universale è schiaffo all'Occidente - Agenda Digitale

- G. MOBILIO, *i sistemi di identificazione biometrica a distanza: un esempio paradigmatico delle sfide lanciate dalla tecnologia al diritto costituzionale,* in *consulta online,* 09/2021

- I.A. FILIPOVA, *Legal Regulation of Artificial Intelligence: Experience of China, Journal of digital technologies and law*, 02/2024
https://www.lawjournal.digital/jour/article/view/373

- M. ANTENORE, E. VALENTINI, *Echo chambers e filter bubble. Effetti limitati e contraddizioni tra ipotesi teoriche e ricerche sul campo, In COMUNICAZIONEPUNTODOC. – 2018*
https://iris.uniroma1.it/handle/11573/1279319

- R.TARCHI, *Appunti di diritto cinese,* Istituto universitario Carolina Albasio, *https://constitutions.albasio.eu/wp-content/uploads/Appunti-di-Diritto-cinese.pdf*

- Secure Privacy, *Protecting Your Personal Information in the Age of the Personal Information Protection Law (PIPL) by the People's Republic of China*, 11/2023
https://secureprivacy.ai/blog/china-pipl-personal-information-protection-law

- V. WEBER, *China's AI-powered surveillance State*, *Journal of Democracy*, volume 36, Number 4, 10/2025

- *What are the distinctions between China's Cybersecurity Law, Data Security Law and PIPL?,* Hi-com, 11/2025 https://translate.hicom-asia.com/question/what-are-the-distinctions-between-chinas-cybersecurity-law-data-security-law-and-pipl/

- X. XU, G. KOSTKA, X. CAO, *Information Control and Public Support for Social Credit Systems in China*, in *University of Chicago press, The Journal of politics*, 08/2022 https://www.journals.uchicago.edu/doi/full/10.1086/718358

Fonti normative Repubblica Popolare cinese:

- Testo ufficiale Cybersecurity Law cinese del 11/2016 https://service.weber.digital/wes-uploads/Cybersecurity_Law_of_the_Peoples_Republic_of_China.pdf

- Testo ufficiale Data Security Law cinese del 9/2021 http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209_385109.html

- Testo ufficiale Personal Information Protection Law cinese del 11/2021 https://personalinformationprotectionlaw.com/chapter-viii-supplementary-provisions/

7. RINGRAZIAMENTI