Dalla Decisione per il rafforzamento della protezione delle informazioni su internet alla Legge sulla tutela delle informazioni personali della RPC "con caratteristiche cinesi"*

Enrico Toti

Abstract

La Cina è uno dei principali attori dell'economia globale che si basa fortemente sulla gestione dei *big data* e sul progresso tecnologico, ed in cui un ristretto numero di attori ne controlla e domina ampi segmenti. Le ragioni ed implicazioni sono molte, anche in considerazione della connessione al tema della sicurezza nazionale, del controllo politico sull'economia volto a garantire la stabilità sociale, e dell'integrità territoriale. Notevoli gli sforzi da parte del legislatore cinese al fine di dotarsi di un apparato normativo in materia di privacy che tenga conto dei modelli preesistenti, in modo particolare di Europa e Stati Uniti, ma che fa proprio un modello in funzione della specifica e complessa realtà del territorio.

China is a major player in the global economy, which heavily relies on big data and technological progress and where a small number of players control and dominate large segments of the economy. The reasons and implications are many, not least in terms of national security, political control over the economy to ensure social stability and territorial integrity. Significant efforts have been made by the Chinese legislator to provide a regulatory apparatus on privacy taking into account pre-existing models, especially those of Europe and the United States, though building its own model according to the specific and complex local reality.

Sommario

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

della Legge sulla tutela delle informazioni personali. - 5. Posizione e ruolo della Legge sulla protezione delle informazioni personali all'interno dell'ordinamento. La coerenza del sistema. - 6. Diritto alla riservatezza e tutela delle informazioni personali. - 7. Lo specifico ambito delle informazioni personali sensibili. - 8. Privacy con caratteristiche cinesi.

Keywords

autoritarismo digitale - codice civile cinese - diritto alla riservatezza - Cina - dati sensibili

Premessa

La Cina è uno dei principali attori dell'economia globale che si basa fortemente sulla raccolta e gestione dei big data e sul progresso tecnologico, in cui un ristretto numero di operatori controlla e domina ampi segmenti del mercato. La protezione delle informazioni personali, la maggior parte delle quali viene veicolata attraverso la rete, è fondamentale per mantenere integra la fiducia delle persone, anche come consumatori, delle imprese e di tutti i protagonisti di questa economia, al fine di garantire una concorrenza leale sul mercato, allineare la Cina alle tendenze mondiali, mantenere fede all'impegno assunto di diventare un leader tecnologico, con particolare attenzione ai servizi digitali innovativi e al commercio elettronico. Le ragioni ed implicazioni sono molte, anche in considerazione della connessione al tema della sicurezza nazionale ed in alcune fasi del controllo politico sull'economia volto a garantire la stabilità sociale, l'integrità territoriale e la guida del governo sullo sviluppo economico[1].

Illuminante, a mio parere, per inquadrare e comprendere la materia è la Spiegazione della Bozza della Legge sulla protezione delle informazioni personali della Repubblica Popolare Cinese (中华人民共和国个人信息保护法 (草案) 的说明) pronunciata da Liu Junchen (刘俊臣) Vicedirettore della Commissione per gli Affari Legislativi del Comitato permanente dell'Assemblea Popolare Nazionale, il 13 ottobre 2020 nel corso della Ventiduesima Sessione del Comitato permanente della Dodicesima Assemblea Popolare Nazionale, in cui sono riportate riflessioni degne di nota e, nel medesimo tempo, per porre le basi della decodificazione e comprensione del testo normativo della Legge[2]. Riporto la traduzione, a mia cura, di alcune parti della Spiegazione:

> «Con la continua e profonda integrazione dell'informatizzazione e della società economica, la rete è diventata un nuovo spazio di produzione e di vita, un nuovo motore per lo sviluppo economico e un nuovo strumento per la comunicazione e la cooperazione. A marzo 2020, gli utenti internet del mio paese hanno raggiunto i 900 milioni, ci sono più di 4 milioni di siti internet e più di 3 milioni di applicazioni. La raccolta e l'uso delle informazioni personali è sempre più ampia. Sebbene

[1] R. Bertinelli, *Economia e politica nella Cina contemporanea*, Roma, 1990.

[2] Il testo è disponibile in The National Peolple's Congress of the People's Republic of China.

la protezione delle informazioni personali del mio paese sia stata continuamente rafforzata negli ultimi anni, nella vita reale alcune aziende, istituzioni e persino individui, a partire da interessi commerciali, raccolgono casualmente, ottengono illegalmente, abusano e scambiano illegalmente informazioni personali. Questioni quali la sicurezza abitativa delle persone e il pericolo per la vita, la salute e la sicurezza della proprietà delle persone sono ancora molto importanti. Nell'era dell'informazione, la protezione delle informazioni personali è diventata uno degli interessi più diretti e pratici del grande pubblico. Vari aspetti della società hanno ampiamente richiesto l'introduzione di una legge speciale sulla protezione delle informazioni personali. […] Il Comitato centrale del Partito attribuisce grande importanza alla costruzione dello stato di diritto nel ciberspazio […] Il segretario generale Xi Jinping ha ripetutamente sottolineato che dobbiamo aderire al principio della sicurezza della rete per le persone, garantire la sicurezza delle informazioni personali e salvaguardare i diritti e gli interessi legittimi dei cittadini nel ciberspazio, proporre requisiti chiari per rafforzare la protezione delle informazioni personali. Al fine di rispondere tempestivamente alle voci e alle aspettative del pubblico in generale […] è di grande importanza formulare una legge speciale sulla protezione delle informazioni personali.

In primo luogo, la formale emanazione della Legge è un requisito per rafforzare ulteriormente la protezione giuridica delle informazioni personali. Dal 18° Congresso Nazionale del Partito Comunista Cinese, l'Assemblea Popolare Nazionale e il suo Comitato Permanente hanno stabilito le regole principali per la protezione delle informazioni personali di cui il rafforzamento della protezione delle informazioni di rete è parte, quali la Legge sulla sicurezza della rete e la Legge sul commercio elettronico, emendando al contempo la Legge sulla tutela dei consumatori. Nella revisione del diritto penale, è stato migliorato il sistema normativo per punire i reati comportanti la violazione delle informazioni personali; nella compilazione del Codice civile, le informazioni personali sono protette dalla legge come un importante diritto civile. Il sistema normativo di protezione delle informazioni personali del mio Paese è stato gradualmente stabilito, ma è ancora difficile adeguarlo alla realtà del rapido sviluppo dell'informatizzazione e alle crescenti esigenze delle persone per una vita migliore. Pertanto, le leggi speciali dovrebbero essere formulate e promulgate sulla base delle leggi esistenti per migliorare la sistematicità, la pertinenza e l'operatività delle norme, dar vita ad un sistema più completo e fornire una tutela più forte in termini di protezione delle informazioni personali.

In secondo luogo, la formulazione di una Legge sulla protezione delle informazioni personali è un'esigenza pratica per mantenere una buona ecologia nel ciberspazio. Il ciberspazio è la casa comune di centinaia di milioni di persone e deve operare sul binario dello stato di diritto. La raccolta e l'uso illegale di informazioni personali e altre attività non solo danneggiano gli interessi vitali delle persone, ma mettono anche in pericolo la sicurezza delle transazioni, interrompono la concorrenza di mercato e turbano l'ordine del ciberspazio. Pertanto, dovrebbero essere formulate leggi speciali per regolamentare le attività di elaborazione delle informazioni personali con sistemi rigorosi, standard rigorosi e responsabilità rigorose,

fissare obblighi e responsabilità dei responsabili del trattamento delle informazioni personali.
In terzo luogo, la formulazione di una Legge sulla protezione delle informazioni personali è una misura importante per promuovere il sano sviluppo dell'economia digitale. Al momento, l'economia digitale quale nuovo fattore di produzione è in forte espansione e la concorrenza sui dati è diventata un campo importante della concorrenza internazionale e i dati sulle informazioni personali sono il nucleo e il fondamento dei big data. Il rapporto del Diciannovesimo Congresso Nazionale del Partito comunista cinese ha presentato i requisiti del compito per costruire un paese forte nella rete, una Cina digitale e una società intelligente. In base a questo requisito, la protezione e l'utilizzo delle informazioni personali devono essere coordinate a livello di sistema, regole, diritti e responsabilità chiari, la protezione deve essere efficace.
[…]
La redazione della Legge sulla protezione delle informazioni personali è stata inclusa nella Programmazione legislativa e nel Piano di lavoro legislativo annuale del Comitato permanente della Tredicesima Assemblea Popolare Nazionale.
[…]
Il lavoro di redazione presta attenzione ai seguenti punti: in primo luogo, combinare le condizioni nazionali e attingere all'esperienza internazionale».

Nonostante questi intenti, sforzi e progressi, sono ancora diverse le questioni non risolte in Cina in materia di privacy. Il crescente uso della tecnologia da parte del governo, si pensi all'utilizzo di sistemi di riconoscimento facciale[3] e di analisi dei big data che possono essere utilizzati per tracciare e monitorare le persone, seppur indicato come necessario per la sicurezza nazionale, accresce la preoccupazione da parte dei cittadini per il potenziale abuso di queste misure e la conseguente violazione della propria privacy[4].
La regolamentazione sulla protezione delle informazioni personali in Cina è assai recente a differenza dell'Unione europea e degli Stati Uniti, che vantano modelli ben consolidati: il modello dell'Unione europea, infatti, riconosce la riservatezza e la tutela delle informazioni personali quali diritti fondamentali, la normativa ha un vasto spettro di applicazione, la definizione di dati personali è assai ampia e molte sono le garanzie di protezione offerte. Negli Stati Uniti, diversamente, non esiste una normativa unitaria che disciplini la materia nella sua interezza, ma le disposizioni sono frammentate in fonti primarie e secondarie e la protezione risulta nel complesso meno

[3] V. L. Wang *Face Recognition in Law Enforcement: A Comparative Analysis of China and the United States*, in *Open Journal of Social Sciences*, 2021, 9; Y. Liu – W. Yan – B. Hu, *Resistance to Facial Recognition Payment in China: The Influence of Privacy-Related Factors*, in *Telecommunications Policy*, 45, 2021, 5.

[4] Riguardo alla vaghezza della normativa cinese che vieta contenuti internet, v. F. Proutè, *Censoring Pornography, the role of sexual media in the fight for freedom of expression in the People's Republic of China*, in *Mapping China Journal*, 2018, 135 ss.; G. Kostka - L. Steinacker - M. Meckel, *Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States*, in *Public Understanding of Science*, 30(6), 2021, 671 ss.; G. Santoni, *La Cina e lo spazio digitale. Questioni di governance nello spazio digitale globale*, in *Orizzonte Cina*, 11, 2020, 70 ss.; S. Del Gatto, *Il riconoscimento facciale in Cina. Interviene la Corte Suprema*, in *IRPA*, 2021.

efficace se paragonata a quella europea. La Cina, come è accaduto per altri settori del diritto, tiene in debita considerazione modelli precedentemente elaborati e, considerata la delicatezza della materia, e le specifiche caratteristiche del contesto, ha proceduto ad elaborare la normativa con gradualità. Ad una prima fase, caratterizzata da una regolamentazione frammentaria e non sempre coordinata, è seguita l' elaborazione di un testo legislativo unitario e comprensivo della disciplina dell'intero settore in cui, come si vedrà più avanti, emergono le peculiarità proprie del contesto sociale e politico.
Il presente contributo, alla luce di quanto sopra anticipato, facendo riferimento ad una ampia bibliografia[5], intende esaminare solo alcuni specifici profili che, a parere dello scrivente, raccolgono l'attenzione degli studiosi e degli esperti della materia: ai paragrafi introduttivi, necessari a fornire un quadro chiaro del contesto e dei testi normativi di riferimento, segue una seconda parte volta ad affrontare alcune importanti e poco note questioni per far emergere la configurazione del modello concepito dal legislatore cinese.
I testi utilizzati a conforto del presente lavoro sono, come di consueto, principalmente in lingua cinese, al fine di avvicinare, per quanto possibile, il lettore alla mentalità del legislatore cinese ed analizzarne dal più fedele angolo visuale le diverse implicazioni.

1. Sovranità informatica e autoritarismo digitale in Cina

Negli ultimi anni in Cina è stata avvertita l'esigenza di creare un adeguato impianto normativo che fosse in grado di garantire la sicurezza del trattamento delle informazioni personali in un più ampio ecosistema normativo[6]. I testi di riferimento sono la Legge sulla sicurezza della rete della Repubblica Popolare Cinese (*Cyber security La*w, CSL, 中华人民共和国网络安全法) promulgata il 7 novembre 2016, in vigore dal 1° giugno 2017 la cui finalità è fissata dall'art.1:

> «La presente legge è elaborata al fine di garantire la sicurezza informatica, di proteggere la sovranità del ciberspazio, la sicurezza nazionale e l'interesse pubblico, di salvaguardare i legittimi diritti ed interessi dei cittadini, delle persone giuridiche e delle altre organizzazioni e di promuovere un sano sviluppo dell'informatizzazione dell'economia e della società».

La Legge sulla sicurezza dei dati della Repubblica Popolare Cinese (*Data security Law*, DSL, 中华人民共和国数据安全法) promulgata il 10 giugno 2021, in vigore dal 1° settembre 2021 la cui finalità è fissata dall'art. 1:

[5] Per una prima bibliografia della Legge sulla tutela delle informazioni personali della Repubblica Popolare Cinese, P. De Hert - E. Papakonstantinou, *The Data Protection Regime in China*, in *Brussels Privacy Hub Working Paper,* 1, 2015, 1 ss.; E. Pernot-Leplay, *China's approach on data privacy flaw: a third way between the US and the EU?* in *Penn State Journal of Law & International Affa*ir, 2020, 49 ss.

[6] I. Calzada, *Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)*, in *Smart Cities*, 5, 2022, 1129 ss.

> «Questa Legge è promulgata per regolare le attività di elaborazione dei dati, garantire la sicurezza dei dati, promuovere l'elaborazione e l'utilizzo dei dati, proteggere I diritti e gli interessi legittimi degli individui e delle organizzazioni, e salvaguardare la sovranità, la sicurezza e gli interessi di sviluppo dello Stato».

La Legge sulla tutela delle informazioni personali (Personal Information Protection Law, PIPL, 中华人民共和国个人信息保护法) promulgata il 20 agosto 2021, in vigore dal 1° novembre 2021 la cui finalità è fissata dall'art. 1:

> «Questa legge è emanata in conformità con la Costituzione per proteggere i diritti e gli interessi delle informazioni personali, disciplinare il trattamento dei dati personali e promuovere l'uso ragionevole delle informazioni personali».

Tale ecosistema deve essere compreso alla luce del principio dell'autoritarismo digitale[7] esercitato dalla Cina attraverso la progressiva costituzione di un consistente numero di strumenti e organi di sorveglianza sottoposti al controllo ed alla supervisione dell'Amministrazione per la sicurezza del ciberspazio (*Cyberspace Administration of China*, *CAC*)[8]. Il controllo governativo della rete ha previsto la creazione del *Great Firewall*[9], ossia una struttura di leggi, software e forme di controllo realizzata allo scopo di sorvegliare, intercettare e bloccare le trasmissioni di dati che risultino in contrasto con le direttive governative, gestendo in tal modo la circolazione dei dati in generale e la loro fuoriuscita dai confini nazionali[10]. Sotto la guida politica di Xi Jinping l'attività di controllo del governo cinese sulle persone è stata ulteriormente estesa, sono stati implementati meccanismi informatici di valutazione dell'affidabilità dei cittadini attraverso il sistema di credito sociale (*social credit system*, 社会信用体系, *shèhuì xìnyòng tǐxì*) . La Cina è contestualmente diventava uno dei leader mondiali nel settore tecnologico, grazie a politiche di settore quali la *National IT Development Strategy*, *Made in China 2025* e la *China Standards 2035*, inoltre le tecnologie utilizzate da parte del governo sono al centro della Via della Seta digitale (*Digital Silk Road*) e costituiscono una delle punte di diamante del settore export del Paese. In particolare, esse sono oggetto di numerosi accordi commerciali con paesi del Nord Africa e del Medio Oriente[11] che

[7] Con il termine "autoritarismo digitale" si intende «l'uso delle tecnologie dell'informazione digitale da parte di regimi autoritari al fine di sorvegliare, reprimere e manipolare la popolazione locale e straniera» secondo la definizione di A. Polyakova - C. Meserole, *Exporting digital authoritarianism*, in *Brookings Institute Foreing Policy Reports*, 2019. Sul tema Qiang X., *Chinese Digital Authoritarianism and Its Global Impact*, in *Digital Activism and Authoritarian Adaptation in the Middle East*; A.N. Liaropoulos, *Digital Authoritarianism "Made in China": Installing a Digital Dystopia*, 23, 1, 2022, 124 ss.

[8] W. Miao - W. Lei, *Policy review: The Cyberspace Administration of China*, in *Global Media and Communication*, 12, 2016, 337 ss.

[9] S. Chandel - Z. Jingji - Y. Yunnan - S. Jingyao - Z. Zhipeng, *The Golden Shield Project of China: A Decade Later - An In Depth Study of the Great Firewall*, in *Conference proceeding of 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, Guilin, China, 2019, 111 ss.

[10] X. Qiang, *Chinese Digital Authoritarianism and Its Global Impact*, in *Digital Activism and Authoritarian Adaptation in the Middle East*, 2021, 35 ss.; J. Rudolph, *Sharper Eyes: Surveilling the Surveillers (Part 1)*, in *China Digital Times*, 2019.

[11] M. Chen - J. Grossklags, *Social Control in the Digital Transformation of Society: A Case Study of the Chinese*

si candidano a divenire, in un prossimo futuro, i nuovi esponenti dell'autoritarismo digitale sul modello cinese[12].
Importanti le considerazioni di Rogier Creemers che ben sintetizzano il quadro attuale:

> *«[…] Chinese legislation and regulation are inextricably linked with the "bigger picture" (daju) of the project that the Chinese Communist Party aims to achieve. Overall, its major objectives are restoring China to a position of wealth and strength (fuqiang), but the specific policy implications of this have varied and evolved over time. In 2014, Xi Jinping announced a drive to turn China into a "cyber power" (wangluo daguo) through the combination of informatization, the introduction of digital technologies in social, economic, and political life, and cybersecurity. In other words, informatization is concerned with the realization of positive plans and policies that leverage digital capabilities for national development goals, which include economic growth and effective governance, applied by both the state and private actors [..]*»[13].

2. Evoluzione normativa

La cultura cinese, sin dall'antichità, ha anteposto l'interesse del gruppo agli interessi dell'individuo sottolineando la posizione subordinata del singolo al gruppo, scelta confermata dal Confucianesimo nel seguente passo "修身,齐家,治 国平天下"[14] in cui prevale il contributo alla famiglia, allo Stato, alla collettività: la riservatezza risiede principalmente nell'unità familiare, distinta dallo Stato[15]. Successivamente, a seguito dei mutamenti sociali a livello globale, anche in Cina, l'individuo ha acquisito un ruolo centrale nella società, non solo come cittadino[16].
Si è intenzionalmente scelto, quale punto di partenza della ricognizione della materia, il periodo della riforma economica cinese in funzione dell'apertura della Cina al resto del mondo, tramite la Politica della porta aperta varata da Deng Xiaoping sotto l'attento controllo del Partito Comunista Cinese[17]. Al fine di sostenere ed accrescere il sistema economico, la Cina ha accolto parziali forme di de-collettivizzazione dell'agricoltura, ha fatto ricorso ad un massiccio ingresso di investimenti stranieri, ha proceduto alla privatizzazione di numerose aziende statali, ha monitorato e gestito l'emersione

Social Credit System, in *Soc. Sci.,* 2022, 11*,* 229 ss.

[12] J. Kurlantzick, *China's Digital Silk Road Initiative: A Boon for Developing Countries or a Danger to Freedom?* in *The Diplomat*, 2020.

[13] Sulla Via della seta digitale e per una prima bibliografia, di interesse *Assessing China's Digital Silk Road Initiative*, in *Council on Foreign Relations.*

[14] R. Creemers, *China's emergin data protection framework*, in *Journal of Cybersecurity*, 2022, 1 ss.

[15] Il passo, contenuto nel Grande insegnamento (大学 *dàxué*), è uno dei principi centrali dell'antica filosofia confuciana ed è stato citato dal Presidente Xi Jinping nel 2014, *The governance of China*, Beijing, 2014, 187.

[16] Y. Yan, *The Chinese path to individualization*, in *The British Journal of Sociology*, 2010, 489 ss.

[17] Sull'emersione del quadro normativo della protezione dei dati in Cina riguardo a singoli periodi e per indicazioni bibliografiche R. Creemers, *China's emerging data protection framework*, cit.

del mercato dei capitali[18]. Le riforme si sono, quindi, concentrate sull'incentivazione degli individui a partecipare in modo attivo alla costruzione economica, valorizzando la crescita del benessere individuale accanto a quello della collettività[19]. Ciò è stato accompagnato da una progressiva, seppur lenta, protezione dei diritti dei singoli, incluso quello alla riservatezza. A tale cambiamento ha contribuito, non solo per far fronte alle istanze dei governi esteri, l'adesione della Cina alla WTO[20], alle organizzazioni internazionali ed una crescente interazione con l'Occidente[21].

Dal 2012 sono stati molteplici gli interventi normativi settoriali relativi alla protezione dei dati personali[22] e gli sforzi del legislatore cinese hanno portato a risultati significativi, in particolar modo nel settore creditizio e della sicurezza informatica, tra i quali: la Decisione per il rafforzamento della protezione delle informazioni su internet (*Resolution to Strengthen the Protection of Information on the Internet*, 全国人民代表大会常务委员会关于加强网络信息保护的决定) pubblicata il 28 dicembre 2012[23]; il Regolamento sull'amministrazione del settore dell'informazione creditizia (*Regulation on Credit Information Industry Administration*, 征信业管理条例) sul modello americano del Fair Credit Reporting Act , pubblicato il 21 gennaio 2013 ; la Decisione del Comitato permanente dell'Assemblea Popolare Nazionale sulla revisione della Legge della Repubblica Popolare Cinese sulla tutela dei diritti e degli interessi dei consumatori (*Decision of the Standing Committee of the National People's Congress on Revision of the Law of the People's Republic of China on the Protection of Rights and Interests of Consumers,* 全国人民代表大会常务委员会关于修改《中华人民共和国消费者权益保护法》的决定) del 25 ottobre 2013 in cui è riconosciuta la protezione delle informazioni personali dei consumatori [24].

Nel 2015 il IX emendamento alla Legge Penale della Repubblica Popolare Cinese (*Ninth Amendment to the People's Republic of China's Criminal Law*, 中华人民共和国刑法修正案-九) ha stabilito che chiunque venda o fornisca informazioni personali a terze parti, in violazione della legge, è soggetto a responsabilità penale. La previsione della

[18] Sul tema con valutazioni critiche ad opera di autori cinesi, v. W. Mengkui, *China's Economic Transformation Over 20 Years*, Beijing, 2000; C. Fulin, *China's Economic Reform at the Turn of the Century*, Beijing, 2000; C. Fulin, *China. The New Stage of Reform*, Beijing, 2004; F. Spigarelli, *Politica industriale e cambiamenti strutturali: la via cinese alla crescita*, in *L'industria. Rivista di economia e politica industriale*, 2018, 511 ss.

[19] S. L. Nah - J. Wong, *China's Emerging New Economy: The Internet and E-Commerce*, Singapore, 2000, 1 ss.; I. Claus – L. Oxley, *China's Economy: A Collection of Surveys*, New Jersey, 2015, 1 ss.; J.A.G. Roberts, *Storia della Cina. La politica, la realtà sociale, la cultura, l'economia dall'antichità ai nostri giorni*, Roma, 2002, 590 ss.

[20] T. Cheek, *Vivere le riforme. La Cina dal 1989*, Torino, 2008, 119: «L'esperienza della riforma non è affatto uniforme, né nella Cina nel suo complesso, né all'interno di una singola comunità . In larga misura, le reazioni ai suoi effetti si possono suddividere, semplicemente, in risposte dei vincitori e risposte dei perdenti».

[21] S. Chiarlone - A. Amighini, *L'economia della Cina*, Roma, 2007, 71 ss.

[22] E.W Capen, *The Western Influence in China*, in *The Journal of Race Development*, 1913, 412 ss. Per una attenta ricostruzione in chiave storica del quadro regoalmentare di internet in Cina, v. M. Weishan – H. Zhu – Z. Chen, *Who's in charge of regulating the internet in China: the history and evolution of China's internet regulatory agencies*, in *China Media Research*, 2018.

[23] Le normative analizzate nel paragrafo sono reperibili in lingua originale nel sito del Consiglio degli Affari di Stato della Repubblica Popolare Cinese.

[24] Il testo in lingua cinese è disponibile sul sito internet della SAMR.

pena è maggiore quando l'attività illecita è compiuta nell'esercizio dei propri doveri[25]. Nel Maggio 2017 sono stati individuati alcuni standard nazionali di classificazione dei sistemi di sicurezza informatica sulla base di requisiti tecnici e gestionali: Specificazioni relative alla sicurezza delle informazioni personali (GB/T 35273-2020) (*Information Security Technology - Personal Information Security Specification (GB/T 35273-2020)*, 信息安全技术 个人信息安全规范) successivamente emendate il 6 marzo 2020 ed in vigore dal 1° ottobre 2020[26]; Linee Guida per la protezione della sicurezza delle informazioni personali su internet (*Guidelines for the Protection of Personal Information Security on Internet,* 互联网个人信息安全保护指南) pubblicate dal Ministero della Pubblica Sicurezza il 10 aprile 2019 che, pur non avendo carattere coercitivo costituiscono riferimento della materia[27]; Regolamento sulla protezione della sicurezza delle infrastrutture critiche informatizzate (*Critical Information Infrastructure Security Protection Regulations*, 关键信息基础设施安全保护条例) pubblicato il 27 aprile 2021 ed in vigore dal 1° settembre 2021. Accanto al formante legislativo è emerso, in via marginale, il formante giurisprudenziale, per cui si menzionano due decisioni, seppur non recentissime, in grado di aiutare a meglio comprendere il quadro regolamentare: nel 2014, la Corte Suprema del Popolo si è pronunciata con le Disposizioni della Corte Suprema del Popolo su diverse questioni relative all'applicazione della legge nei processi civili che coinvolgono l'uso delle reti informatiche per la violazione dei diritti e degli interessi personali (最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定) riconoscendo la tutela del nome, dell'immagine, della reputazione e dell'onore, oltre che dei dati personali dei cittadini cinesi; nel 2017, con le Interpretazione della Corte Suprema del Popolo e della Procura Suprema del Popolo su diverse questioni riguardanti l'applicazione della legge nella gestione di casi penali di violazione delle informazioni personali dei cittadini (最高人民法院 最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解)[28].

La Cina ha, pertanto, ritenuto opportuno dotarsi di un apparato normativo efficace e moderno, collegandolo ad alcuni riferimenti normativi preesistenti, primi fra tutti, l'art. 40 della Costituzione del 1982[29], l'art. 252 del Codice penale[30], l'art. 101 dei Prin-

[25] Il testo in lingua cinese della Decisione è disponibile nel sito internet del Consiglio degli Affari di Stato della Repubblica Popolare Cinese.

[26] Per una approfondita disamina del testo delle Specificazioni relative alla sicurezza delle informazioni personali, J. Wizhi, *Breve analisi del valore della versione 2020 delle Specificazioni per la sicurezza delle informazioni personali nell'orientare le politiche aziendali di protezione delle informazioni personali*.

[27] Le "Linee guida" stabiliscono in modo esaustivo i requisiti di attuazione che devono essere rispettati dalle imprese per la protezione delle informazioni personali in termini di misure di gestione, impostazioni del personale, raccolta e utilizzo delle informazioni, archiviazione, condivisione e risposta agli incidenti e si sovrappongono parzialmente ai contenuti delle "Principali norme di sicurezza" ed altri documenti.

[28] I testi in lingua cinese sono disponibili nel sito della Corte Suprema del Popolo della Repubblica Popolare Cinese.

[29] Art. 40: «La libertà e la riservatezza relativa alla corrispondenza dei cittadini della Repubblica Popolare Cinese sono protette dalla legge. Nessuna organizzazione o individuo può, per nessun motivo, violare la libertà e la riservatezza della corrispondenza dei cittadini, salvo nei casi in cui, per soddisfare le esigenze della sicurezza dello Stato o delle indagini penali, gli organi di pubblica sicurezza o i procuratori sono autorizzati a censurare la corrispondenza secondo le procedure previste dalla legge».

[30] Art. 252: «Chiunque nasconde, distrugge o apre illecitamente una corrispondenza altrui, violando

cipi generali del diritto civile, questi ultimi abrogati con l'ingresso del Codice civile, ed istituendo una pluralità di autorità deputate al funzionamento dell'intero sistema. Su questo complesso quadro regolamentare poggiano le basi le tre leggi, precedentemente menzionate, che ne costituiscono i pilastri, integrate da fonti ulteriori che lo completano e ne consentono la concreta attuazione[31].

così il diritto del cittadino alla libertà di corrispondenza, se le circostanze sono gravi, è condannato alla reclusione a tempo determinato non superiore a un anno o alla detenzione penale».

[31] Accanto alla molteplicità di autorità coinvolte, sempre alla luce di meglio comprendere l'ecosistema normativo, si è ritenuto opportuno riportare, per completezza, una serie di fonti poche note che regolamentano la materia al fine di predisporre un quadro il più esauriente possibile: Linee guida per la protezione delle informazioni personali su Internet 2019 (*Guidelines on Internet Personal Information Security Protection*, 2019, 互联网个人信息安全保护指南) pubblicate dal Ministero della Pubblica Sicurezza il 19 aprile 2019 con effetti a decorrere dal 19 aprile 2019; Disposizioni sulla protezione online dei dati personali dei bambini (*Provisions on Online Protection of Children's Personal Information*, 2019, 儿童个人信息网络保护规定) pubblicate dall'Amministrazione per la sicurezza del ciberspazio il 22 agosto 2019 con effetti a decorrere dal 1° ottobre 2019; Tecnologia di protezione delle informazioni - Guida per l'anonimizzazione dei dati personali (*Information Security Technology - Guide for De-identifying Personal Information* -GB/T37964-2019 - 信息安全技术†- 个人信息去标识化指南) pubblicate dal Comitato tecnico nazionale per la standardizzazione della sicurezza delle informazioni (TC 260) il 30 di agosto 2019 con effetti a decorrere dal 1° marzo 2020; Avviso sulla protezione dei dati personali e utilizzazione di Big data per sostenere gli sforzi congiunti per la prevenzione e il controllo del COVID-19, 2020 (*Notice on Ensuring Personal Information Protection and Utilization of Big Data to Support Joint Efforts for COVID-19 Prevention and Control, 2020,* 做好个人信息保护利用大数据支撑联防联控工作的通知) pubblicato dall' Amministrazione per la sicurezza del ciberspazio il 4 febbraio 2020 con effetti a decorrere dal 4 febbraio 2020; Specifiche tecniche sulla protezione delle informazioni finanziarie personali, 2020 (*Personal Financial Information Technical Protection Specification, JR/T0171-2020*, 个人金融信息技术保护规范) pubblicate dalla Banca popolare cinese il 13 febbraio 2020 con effetti a decorrere dal 13 febbraio 2020; Tecnologia per la sicurezza delle informazioni - Specifiche per la sicurezza delle informazioni personali (*Information Security Technology - Personal Information Security Specification - GB/T 35273-2020*- 信息安全技术†- 个人信息安全规范), pubblicate dal Comitato tecnico nazionale per la standardizzazione della sicurezza delle informazioni (TC 260) il 6 marzo 2020 con effetti a decorrere dal 1° ottobre 2020, in sostituzione della versione pubblicata il 29 dicembre 2017; Misure attuative per la protezione dei diritti e degli interessi dei consumatori finanziari (*Implementing Measures for Protection of the Rights and Interests of Financial Consumers, 2020*, 中国人民银行金融消费者权益保护实施办法) pubblicate dalla Banca popolare cinese il 15 settembre 2020 con effetti a decorrere dal 1° novembre 2020; Tecnologia di protezione delle informazioni - Guida alla valutazione dell' impatto sulla sicurezza dei dati personali (*Information Security Technology - Security Impact Assessment Guide of Personal Information, GB/T 39335-2020*, 信息安全技术†- 个人信息安全影响评估指南), pubblicate dal Comitato tecnico nazionale per la standardizzazione della sicurezza delle informazioni (TC 260) il 19 novembre 2020 con effetti a decorrere dal 1° giugno 2021; Disposizioni su diverse questioni riguardanti l'applicazione della legge nel processo di cause civili relative all'uso della tecnologia di riconoscimento facciale per il trattamento dei dati personali, 2021 (*Provisions on several issues concerning the application of law in the trial of civil cases related to the use of facial recognition technology to process personal information*, 2021, 审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定) pubblicate dalla Corte suprema del popolo il 27 luglio 2021 con effetti a decorrere dal 1° agosto 2021; Misure per la gestione dei servizi di indagine creditizia, 2021 (*Measures for Credit Investigation Services Management, 2021*, 征信业务管理办法) pubblicate dalla Banca popolare cinese il 17 settembre 2021 con effetti a decorrere dal 1° gennaio 2022; Disposizioni sulla gestione della raccomandazione algoritmica nel servizio di informazione su Internet, 2021 (*Provisions on Administration of Algorithmic Recommendation in the Internet Information Service, 2022*, 互联网信息服务算法推荐管理规定) pubblicate congiuntamente dall' Amministrazione per la sicurezza del ciberspazio, dal Ministero per l'industria e l'informazione tecnologica, Ministero della Pubblica Sicurezza e l'Amministrazione statale per la regolamentazione del mercato il 1° marzo 2022 con effetti a decorrere dal 1° marzo 2022; Tecnologia di protezione delle informazioni - Specifica sulla valutazione del rischio per la sicurezza delle informazioni (*Information Security Technology - Risk Assessment method for Information Security*, 信息安全技术信息安全风险评估方法) pubblicata dal Comitato tecnico nazionale per la standardizzazione della sicurezza delle informazioni (TC 260) il 15 aprile 2022 con

A capo delle autorità garanti del corretto funzionamento del quadro normativo rinveniamo l'A Amministrazione per la sicurezza del ciberspazio (*Cyberspace Administration of China,* CAC, 国家互联网信息办公室)[32] a cui si affiancano il Ministero della Pubblica Sicurezza (*Ministry of Public Security*, MPS, 公安部)[33], il Ministero per l'Industria e l'Informazione Tecnologica (*Ministry of Industry and Information Technology,* MIIT, 国家

effetti a decorrere dal 1° novembre 2021; Pareri su diversi problemi relativi all'applicazione della legge nel giudizio di cause penali (*Opinions on Several Issues in the Application of Criminal Procedures in Handling Cases of Information Network Crimes*, 2022, 最高人民法院 最高人民检察院 公安部关于办理信息网络犯罪案件适用刑事诉讼程序若干问题的意见), pubblicati congiuntamente dalla Corte suprema del popolo, dalla Procura suprema del popolo e dal Ministero della Pubblica Sicurezza il 26 agosto 2022, con effetti a decorrere dal 1° settembre 2022; Tecnologia di protezione delle informazioni - Linee guida per l'ingegnerizzazione della protezione dei dati personali [*Information Security Technology - Guidelines for personal information security engineering* (GB/T 41817-2022) 信息安全技术†- 个人信息安全工程指南) (征求意见稿], pubblicate il 14 ottobre 2022 con effetti a decorrere dal 1° maggio 2023; Legge sul commercio elettronico, 2018 (*Electronic Commerce Law, 2018,* 电子商务法), promulgata il 31 agosto 2018, in vigore dal 1° gennaio 2019; Interpretazioni su diverse questioni riguardanti l'applicazione della legge nella gestione dei giudizi penali, quale la questione dell'uso illegale delle reti informatiche e del sostegno alle attività criminali informatiche, 2019 (*Interpretations on Several Issues concerning the Application of Law in Handling Criminal Cases such as Making Illegal Use of Information Networks and Assisting Information Network Criminal Activities*, 2019, 办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释), pubblicate di concerto dalla Corte suprema del popolo e dalla Procura suprema del popolo con effetti a decorrere dal 1° novembre 2019; Misure per la valutazione della sicurezza del trasferimento transfrontaliero dei dati (*Measures on Cross-Border Data Transfer Security Assessment,* 数据出境安全评估办法) pubblicate dall' Amministrazione per la sicurezza del ciberspazio il 7 luglio 2022, con effetti a decorrere dal 1° settembre 2022; Contratto standard per il trasferimento transfrontaliero di informazioni personali (*Standard contract for cross-border transfer of personal information* 个人信息出境标准合同) e Misure definitive sul contratto standard per il trasferimento transfrontaliero di informazioni personali *(Final version of the Measures for the Standard Contract for Cross-Border Transfer of Personal* 个人信息出境标准合同办法) pubblicate dall' Amministrazione per la sicurezza del ciberspazio il 22 febbraio 2023 con effetti a decorrere dal 1° giugno 2023; Guida pratica agli standard di sicurezza di rete - Specifiche tecniche per la certificazione di sicurezza del trattamento transfrontaliero delle informazioni personali (*Network Security Standards Practice Guide - Technical Specifications for the Security Certification of Personal Information Cross-Border Processing,* 网络安全标准实践指南—个人信息跨境处理活动安全认证规范) pubblicata il 16 marzo 2023 da parte del Comitato Tecnico Nazionale per la Standardizzazione della Sicurezza Informatica (TC260), in aggiornamento rispetto alla precedente versione del 24 giugno 2022 la cui finalità è di fornire ai responsabili del trattamento delle informazioni personali maggiore chiarezza riguardo alle aspettative delle autorità cinesi in merito alle modalità di trasferimento transfrontaliero dei dati in conformità con la legge sul trattamento dei dati personali.

[32] L' Amministrazione per la sicurezza del ciberspazio (国家互联网信息办公室, *Cyberspace Administration of China,* CAC), fondata nel 2011, opera a partire dal 2014 sotto la diretta supervisione del Gruppo dirigente centrale per gli affari del ciberspazio (中共中央网络安全和信息化领导小组办公室, *Central Leading Group for Cyberspace Affairs*). L'Amministrazione è responsabile della sicurezza del ciberspazio e della regolamentazione dei contenuti di internet; le sue funzioni principali sono: la direzione, il coordinamento e la supervisione della gestione dei contenuti online e la gestione della procedura amministrativa di autorizzazione per le imprese operanti nel campo della informazione online.

[33] Il Ministero della Pubblica Sicurezza (公安部,*Ministry of Public Security*, MPS), istituito nel 1954, è la principale autorità cinese per la sicurezza pubblica nazionale. Si occupa della prevenzione e dell'investigazione sulle attività illegali, criminali e terroristiche, della salvaguardia della sicurezza pubblica e dell'ordine sociale, oltre ad essere coinvolto nella gestione dell'immigrazione, della registrazione di famiglie e carte d'identità dei residenti, nella gestione di assemblee, cortei e manifestazioni e ad essere responsabile della sicurezza della rete di informazione pubblica. Inoltre, svolge una generica funzione di coordinamento degli altri organi statali, delle organizzazioni pubbliche, imprese e istituzioni che operano nell'ambito della sicurezza pubblica. Il sito web del Ministero della Pubblica sicurezza è disponibile qui.

市场监督管理总局), l'Amministrazione Statale per la Regolamentazione del Mercato (*State Administration for Market Regulation,* SAMR, 国家市场监督管理总局)[34], l'Amministrazione della Cina per la Standardizzazione (*Standardisation Administration of China,* SAC, 国家标准化管理委员会), il Comitato tecnico nazionale per la standardizzazione della sicurezza delle informazioni (*National Information Security Standardisation Technical Committee*, TC 260, 全国信息安全标准化技术委员会) i quali pubblicano linee guida e standard nazionali non vincolanti volti o a colmare le lacune o funzionali alla predisposizione di una normativa sperimentale da convertire successivamente in disciplina cogente.

3. Il Codice civile cinese, artt. 1032 - 1039

In linea con la generale attenzione riservata al tema in esame, il Cod. civ. cin., in vigore dal 1° gennaio 2021, contiene norme specifiche in materia di tutela delle informazioni personali nel Libro Quarto "Dei diritti di personalità", Titolo Sesto "Dei diritti alla riservatezza e alla protezione delle informazioni personali" (artt. 1032 - 1039).
Il primo articolo ad occuparsi della materia è il 1032 che qualifica in termini di diritto soggettivo quello alla riservatezza e fissa il generale divieto di violazione, descrivendone il contenuto:

> «Ogni persona fisica ha diritto alla riservatezza. Nessuna organizzazione o individuo può ledere l'altrui diritto alla riservatezza attraverso l'indagine, l'intromissione, la divulgazione o la pubblicizzazione e simili.
> La riservatezza consiste nella serenità della vita privata di una persona fisica e della sua sfera intima, delle sue attività private e nelle sue informazioni private che non vuole siano rese note ad altri».

La tutela di questo diritto in Cina ha attraversato una profonda evoluzione passando dall'inesistenza, all'esistenza, ed infine ad un progressivo rafforzamento. Il primo riferimento a tale ambito di tutela si rinviene nella Legge di procedura civile (民事诉讼法试行) del 1982 e successivamente nell'art. 140 delle Opinioni sui Principi generali del diritto civile (民法通则意见) del 1988 in cui si pongono le basi per la previsione di una protezione più articolata. In prosieguo di tempo, nell'Interpretazione giudiziaria sul risarcimento dei danni morali (精神损害赔偿司法解释) del 2001, la tutela giudiziaria è concepita in termini di interesse così come nell' Interpretazione giudiziaria sul risarcimento dei danni alla persona (人身损害 赔偿司法解释) del 2003. Solo nel 2005, per la prima volta, a seguito dell'emendamento della Legge sulla protezione dei diritti e degli interessi delle donne (妇女权益保障法) si riconosce la riservatezza quale diritto. Ulteriore avanzamento si ha, poi, nell'art. 2 della Legge sulla responsabilità civile (侵权责任法) del 26 novembre 2009:

[34] L'Amministrazione Statale per la Regolamentazione del Mercato (国家市场监督管理总 *State Administration for Market Regulation*, SAMR) è stata istituita nell'aprile 2018, consolidando le responsabilità di supervisione del mercato precedentemente suddivise tra diverse agenzie.

> «Coloro che violano i diritti e gli interessi civili sono soggetti alla responsabilità per illecito civile ai sensi della presente legge.
> I diritti e gli interessi civili utilizzati nella presente legge comprendono il diritto alla vita, il diritto alla salute, il diritto al nome, il diritto alla reputazione, il diritto all'onore, il diritto alla propria immagine, il diritto alla riservatezza, l'autonomia coniugale, la tutela, la proprietà, l'usufrutto, gli interessi di sicurezza, il diritto d'autore, il diritto di brevetto, il diritto esclusivo all'uso di un marchio, il diritto di invenzione, i titoli di credito, il diritto di successione e altri diritti e interessi personali e patrimoniali».

La Legge non solo distingue il diritto alla riservatezza dal diritto alla reputazione ma compensa le carenze dei Principi generali del diritto civile del 1987, oggi sostituiti dalla disciplina del Cod. civ. cin. che, nella Parte generale, all'art. 110 dispone:

> «La persona fisica ha diritto alla vita, all'integrità del corpo, alla salute, al nome, all'immagine, alla reputazione, all'onore, alla riservatezza e all'autonomia coniugale.
> La persona giuridica o l'organizzazione priva di personalità giuridica ha diritto alla denominazione, alla reputazione e all'onore».

confermando e chiarendo che si tratta di un diritto civile riferito alle persone fisiche rientrante tra i diritti della personalità. Parte della dottrina cinese va oltre ed introduce la riservatezza correlata, relativa cioè al diritto alla riservatezza di soggetti terzi; l'esercizio del proprio diritto alla riservatezza, include l'interesse alla tutela del medesimo diritto di altri[35].
L'art. 1033 tratta del diritto alla riservatezza e della protezione delle informazioni personali. Enumera alcuni atti tipici che costituiscono violazione della riservatezza salvo che la legge non preveda diversamente o le parti non lo concordino. La disposizione, pertanto, conferma e consolida quanto contenuto nella Decisione del Comitato permanente dell'Assemblea Popolare Nazionale (全国人民代表大会常务委员会关于加强网络信息保护的决定) del 2012, ma conferisce una accezione più ampia riguardo ai comportamenti che configurano la violazione:

> «Salvo diversa disposizione di legge o espresso consenso del titolare del diritto,

[35] Il Comitato Tecnico Nazionale per la Standardizzazione della Sicurezza delle Informazioni (全国信息安全标准化技术委员会 *National Information Security Standardization Technical Committee*, TC260), istituito il 15 aprile 2002 a Pechino con l'approvazione dell'Amministrazione per la Standardizzazione della Repubblica Popolare Cinese (中国国家标准化管理委员会, *Standardization Administration of the People's Republic of China*, SAC), è un'organizzazione di natura tecnica impegnata nella formulazione a livello nazionale di standard di sicurezza informatica le cui principali attività sono l'emanazione di standards nel campo della sicurezza tecnologica, dei servizi di sicurezza, del *security managment* e del *security assesment*. Il 7 marzo 2020 ha annunciato l'approvazione e la pubblicazione di otto standard di sicurezza informatica ("Cybersecurity Standards"). In particolare, uno degli standard, le *Specifiche tecniche per la sicurezza delle informazioni personali GB / T 35273-2020* ("Standard di sicurezza delle informazioni"), fornisce i principi di base per la salvaguardia delle informazioni personali, nonché indicazioni sulla loro raccolta e la conservazione.

nessuna organizzazione o individuo deve compiere gli atti di seguito indicati:
(1) intromettersi nella vita privata di un'altra persona tramite telefonate, invio di messaggi di testo, utilizzo di strumenti di messaggistica istantanea, invio di posta elettronica e volantini e simili;
(2) entrare, scattare fotografie o spiare negli spazi privati altrui come la residenza o la camera d'albergo di un'altra persona;
(3) scattare fotografie, spiare, intercettare o divulgare le attività private di un'altra persona;
(4) scattare fotografie o spiare le parti intime del corpo di un'altra persona;
(5) elaborare le informazioni private di un'altra persona;
(6) violare la riservatezza di un'altra persona con altri mezzi».

Con riferimento al punto 5, la dottrina chiarisce che l'espressione "informazioni private" si riferisce a qualsiasi informazione che i privati non vogliono che sia resa nota ad altri, purché tale occultamento non violi la legge e la moralità sociale. Nello specifico, le informazioni private possono includere: le informazioni biologiche personali quali altezza, peso, gruppo sanguigno, colore della pelle, aspetto, sesso, geni, stato di salute, informazioni sulle malattia *et cetera*; informazioni riguardo al proprio corpo in riferimento alle parti del corpo che il singolo non vuole mostrare ad altri ed in particolare organi sessuali, parti disabili *et cetera*; riservatezza della proprietà privata, riservatezza riguardo alla famiglia come ad esempio, relazioni familiari, parentela di sangue, relazione matrimoniale *et cetera*, riservatezza della comunicazione quali processi di comunicazione e contenuti generati con vari mezzi quali lettere, email e telefonate che non devono essere monitorati o intercettati da altri; riservatezza delle conversazioni, contenuti che gli individui non desiderano che siano resi noti al pubblico durante il processo di comunicazione; riservatezza delle esperienze personali, storia lavorativa, amicizie, la riservatezza alla vita personale quale nome di una persona fisica, occupazione, luogo di lavoro, ambito di amicizia, preferenze di consumo, indirizzo, residenza, telefono, etnia , credo religioso, diario e altri documenti privati . La violazione, per configurarsi tale, deve essere integrata da un comportamento attivo, con ciò intendendosi atti di intrusione, monitoraggio, spionaggio, perquisizione, divulgazione, pubblicità e altri metodi di violazione. La violazione della riservatezza si manifesta, quindi, principalmente nella divulgazione di informazioni private altrui come l'interferenza nella vita privata di altre persone ed intromissione nello spazio e dominio privato altrui.
La dottrina si è occupata in modo accurato del tema precisando che non sia necessario che l'atto di violazione sia compiuto in un luogo pubblico, accogliendo un'accezione di violazione assai ampia ed inclusiva che appare privilegiare l'elemento oggettivo del comportamento. Di interesse, sempre secondo la dottrina, è che le conseguenze della violazione del diritto alla riservatezza si manifestino principalmente come danno psicologico, pur potendo provocare, in via indiretta, danni al diritto di proprietà di cui la persona sia titolare[36].
Il successivo art. 1034:

[36] W. Liming (王利明), *Ricerca sui diritti della personalità* (人格权法研究), Beijing, 2004, 600.

> «Le informazioni personali di una persona fisica sono tutelate dalla legge.
> Le informazioni personali sono quelle registrate elettronicamente o in altri modi che possano essere utilizzate, da sole o in combinazione con altre, per identificare una persona fisica, inclusi nome, data di nascita, numero di carta di identità, informazioni biometriche, indirizzo di residenza, numero di telefono, indirizzo email, informazioni sanitarie, ubicazione e simili della persona.
> Alle informazioni personali sensibili si applicano le disposizioni sul diritto alla riservatezza o, in mancanza, si applicano quelle sulla protezione delle informazioni personali».

riprende quanto già fissato dall'art. 111 del Cod. civ. cin:

> «Le informazioni personali di una persona fisica sono protette dalla legge. Qualsiasi organizzazione o soggetto che abbia necessità di ottenere informazioni altrui deve ottenerle in conformità alla legge e garantire la sicurezza di tali informazioni e non deve raccogliere, utilizzare, elaborare o trasmettere illegalmente le informazioni personali di altre persone, né può acquistare, vendere, fornire, o pubblicare illegalmente informazioni personali»,

nella Decisione del Comitato permanente dell'Assemblea Popolare Nazionale sul rafforzamento della protezione delle informazioni di rete (全国人民代表大会常务委员会关于加强网络信息保护的决定) del 28 dicembre 2012 e nelle Interpretazioni su diverse questioni relative all'applicazione della legge nella gestione dei casi penali di violazione delle informazioni personali dei cittadini (办理侵犯公民个人信息刑事案件 适用法律若干问题的解释) del 1° giugno 2017. In tal senso la dottrina rileva che l'utilizzo dei *big data* e della tecnologia legata allo sviluppo dell'intelligenza artificiale ha reso molto semplice l'analisi e l'utilizzo di grandi quantità di dati e il potenziale uso improprio delle informazioni personali è aumentato drasticamente, accrescendo il rischio di danneggiamento della dignità delle persone fisiche e di libero sviluppo della personalità[37] per cui il Cod. civ. cin. mira a porre un argine, imponendo con l'art. 999 l'uso ragionevole delle informazioni personali:

> «Il nome, la denominazione, l'immagine, i dati personali e simili di un soggetto di diritto possono essere ragionevolmente utilizzati da coloro che si occupano della diffusione di notizie, del monitoraggio di opinioni pubbliche o simili, per interessi pubblici. Se vi sia un loro irragionevole utilizzo, lesivo dei diritti della personalità del soggetto, si è tenuti a risponderne civilmente in conformità con la legge»

e prevedendo, agli artt. 1029 e1030, la facoltà di rettificare o eliminare informazioni funzionali alla determinazione del *social credit system*:

> «Un soggetto di diritto può consultare la propria valutazione di credito in conformità con la legge; ha diritto di sollevare un'obiezione e chiedere la rettificazione,

[37] Y. Lixin (杨立新), *Trattato sulla responsabilità civile* (侵权法论), Beijing, 2013, 464.

la cancellazione o altre misure necessarie da adottare se riscontri che il rapporto di credito non è corretto. I valutatori della sua affidabilità devono essa minare tempestivamente la relazione e prendere le misure necessarie in modo tempestivo se si accerta che è non veritiera».
«Le disposizioni di questo libro sulla protezione delle informazioni personali e le disposizioni pertinenti di altre leggi e regolamenti amministrativi si applicano al rapporto tra i soggetti di diritto e gli elaboratori di informazioni di credito come il sistema di informazioni creditizie».

Le due disposizioni, sia pur operanti in un ambito specifico, conferiscono una efficace tutela alle informazioni personali, in funzione di protezione della dignità umana e della libertà personale .
L'art. 1035 fissa i principi che devono essere rispettati nel trattamento delle informazioni personali e, contestualmente, le condizioni necessarie affinché il trattamento possa avvenire:

«Il trattamento delle informazioni personali deve essere conforme ai principi di liceità, legittimità, necessità, proporzionalità e deve avvenire nel rispetto delle condizioni di seguito indicate:
(1) il consenso deve essere ottenuto dalla persona fisica o dal suo tutore, salvo quanto diversamente previsto da leggi o dai regolamenti amministrativi;
(2) le regole per il trattamento delle informazioni devono essere rese pubbliche;
(3) lo scopo, il metodo e l'ambito del trattamento delle informazioni sono espressamente indicati;
(4) non vi sia violazione di leggi o regolamenti amministrativi o dell'accordo tra entrambe le parti.
Il trattamento delle informazioni personali include la raccolta, l'archiviazione, l'utilizzo, il perfezionamento, la trasmissione, la fornitura, la divulgazione e simili dei dati personali.
Durante il trattamento delle informazioni personali, un soggetto non risponde civilmente in presenza di una delle condizioni di seguito indicate:
(1) esegue ragionevolmente l'atto nella misura in cui la persona fisica o il suo tutore acconsente;
(2) tratta ragionevolmente le informazioni divulgate dalla persona fisica stessa o le altre informazioni che sono già state divulgate legalmente, a meno che detta persona lo rifiuti esplicitamente o il trattamento delle informazioni leda un interesse significativo della persona;
(3) esegue ragionevolmente gli altri atti necessari per proteggere l'interesse pubblico o i diritti e gli interessi legali della persona».

La disposzione trova un suo precedente nell'art. 41 della Legge sulla sicurezza della rete e nell'art. 29 della Legge sulla tutela dei diritti e degli interessi dei consumatori. Requisito fondamentale riguardo alla raccolta e al trattamento delle informazioni personali è che questi abbiano una base giuridica e soddisfino le condizioni fissate

dalla legge. L'oggetto della raccolta e del trattamento delle informazioni deve essere lecito; la determinazione di quali soggetti siano autorizzati a raccogliere ed elaborare le informazioni personali altrui deve essere effettuata in conformità alle disposizioni di legge.
In generale, esistono due tipi di organi che raccolgono ed elaborano le informazioni personali: le autorità statali che possono raccogliere, elaborare e utilizzare le informazioni personali nell'ambito dei loro poteri, indipendentemente dal consenso dell'interessato e i soggetti che raccolgono informazioni solo con il consenso dell'interessato e le cui modalità di raccolta devono essere conformi a quanto stabilito dalla legge. Correlati a questa disposizione l'art. 12, c. 1, della Legge sulla prevenzione e il controllo delle malattie infettive (传染 病防治法) emendata da ultimo il 28 agosto 2004[38]:

> «Tutte le unità e gli individui all'interno del territorio della Repubblica Popolare Cinese devono accettare le misure di prevenzione e controllo, come le indagini, i test, la raccolta di campioni e l'isolamento e il trattamento delle malattie infettive da parte delle istituzioni di prevenzione e controllo delle malattie e delle istituzioni mediche, e fornire informazioni pertinenti in modo veritiero. Le istituzioni di prevenzione e controllo delle malattie e le istituzioni mediche non devono divulgare informazioni o dati relativi alla privacy delle persone».

e l 'art. 25 del Regolamento sulla risposta alle emergenze di salute pubblica (突发公共卫生事件应急条例) del 9 maggio 2003 i quali prevedono che il Dipartimento amministrativo sanitario competente del Consiglio degli Affari di Stato sia responsabile della diffusione di informazioni al pubblico sull'emergenza. Inoltre, la conservazione delle informazioni personali deve essere conforme al principio del tempo minimo di conservazione, vale a dire che, se non diversamente previsto da leggi o regolamenti o autorizzato dall'interessato, le informazioni personali devono essere conservate per il tempo minimo necessario a raggiungere lo scopo per il quale l'interessato è autorizzato a utilizzarle.
Una particolare attenzione deve essere riservata al tema del consenso, la necessità del cui rilascio assurge, nella normativa generale, non solo cinese, a principio informatore della materia. Si pensi alla disciplina elaborata nell'ambito dell'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE), nelle sue Linee guida del 1980 sulla protezione della privacy e dei flussi transfrontalieri di dati personali[39]; alla direttiva 95/46/CE sulla protezione del trattamento dei dati personali e sulla libera circolazione di tali dati del 1995[40], art. 7 lett. a; alla Legge federale sulla protezione dei dati della Germania, nonché alla normativa emanata da Francia e Regno Unito che hanno previsto il consenso informato nelle rispettive leggi sulla protezione dei dati personali.

---

38 W. Liming (王利明), *Ricerca sui diritti della personalità,* cit.

39 Z. Xinbao (张新宝), *Lo sviluppo del sistema giuridico di protezione della privacy in Cina* (我国隐私权保护法律制度的发展), nel *Giornale del collegio statale dei procuratori*, Beijing, 2010, 2 ss. dove la riservatezza, partendo dalla Legge sulla responsabilità civile, è ricostruita quale diritto attraverso un ragionamento deduttivo.

40 C. Xiao (程啸), *Protezione delle informazioni dalla prospettiva di compilazione del Codice civile* (民法典编纂视野下的个人信息保护), in *China Legal Science*, 2019, 26 ss.

Nella Repubblica Popolare Cinese, nel 2012, l'art. 2 della Decisione del Comitato permanente dell'Assemblea Popolare Nazionale sul rafforzamento della protezione delle informazioni di rete (全国人民代表大会常务委员会关于加强网络信息保护的决定) ha esplicitamente stabilito che i fornitori di servizi di rete e le imprese nel corso delle loro attività commerciali e le istituzioni possono raccogliere ed utilizzare le informazioni elettroniche personali dei cittadini, richiedendo il consenso della persona le cui informazioni sono raccolte. In linea con quanto stabilito dall' art. 22, c. 3, della Legge sulla sicurezza della rete (网络安全法) ha chiaramente previsto, inoltre, che «quando i prodotti e i servizi di rete hanno la funzione di raccogliere informazioni sugli utenti, i loro fornitori devono renderlo chiaro agli utenti e ottenere il loro consenso». L'art. 41 della Legge sulla sicurezza della rete afferma, altresì, che l'operatore di rete deve ottenere il consenso della persona le cui informazioni personali devono essere raccolte per il trattamento. Per quanto riguarda il consenso informato, la dottrina rileva che esso deriva dal principio di volontarietà. In termini di natura dell'atto il consenso è, infatti, una forma di espressione della libera volontà del titolare del diritto riferito alle proprie informazioni. Positivo o negativo, il consenso della persona interessata dalla raccolta e dal trattamento dei suoi dati personali è inteso a rendere effettiva la libertà d'azione e l'autodeterminazione dell'individuo, e a conseguire gli effetti giuridici che intende ottenere[41].
L'art. 1036 delimita l'ambito di esclusione di responsabilità con riferimento al trattamento delle informazioni personali:

> «Durante il trattamento delle informazioni personali, un soggetto non risponde civilmente in presenza di una delle condizioni di seguito indicate:
> (1) esegue ragionevolmente l'atto nella misura in cui la persona fisica o il suo tutore acconsente;
> (2) tratta ragionevolmente le informazioni divulgate dalla persona fisica stessa o le altre informazioni che sono già state divulgate legalmente, a meno che detta persona lo rifiuti esplicitamente o il trattamento delle informazioni leda un interesse significativo della persona;
> (3) esegue ragionevolmente gli altri atti necessari per proteggere l'interesse pubblico o i diritti e gli interessi legali della persona».

In tale ambito la previsione del principio di presunzione della colpa è funzionale a conferire una adeguata tutela al titolare del diritto, stante la difficoltà per l'interessato a dimostrare che il responsabile del trattamento delle informazioni abbia commesso errori nel processo di raccolta, elaborazione, archiviazione e utilizzo delle informazioni[42].

---

[41] C. Xiao (程 啸), *Sulla Legge sulla tutela delle informazioni personali del mio paese. Regole per il trattamento dei dati personali* (论我国个人信息保护法中的个人信息处理规则), in *Tsinghua University Law Journal*, 2021, 55 ss.

[42] Y. Zhiqiang (尹志强), *Rimedi di diritto civile per violazione delle informazioni personali nell'ambiente di rete* (网络环境下侵害个人信息的民法救济), in *Leggi applicabili*, 8, 2013, 14 ss. Per una diversa impostazione della dottrina che ritiene opportuno seguire il principio della responsabilità per colpa, v. Yang Lixin (杨立新), *Illeciti e responsabilità di violazione delle informazioni personali elettroniche dei cittadini* (侵害公民个人电

Riguardo all'art. 1037:

> «Una persona fisica può consultare o fare copie delle sue informazioni personali presso l'elaboratore del trattamento delle informazioni in conformità con la legge. Se la persona riscontra che le informazioni sono errate ha diritto di sollevare un'obiezione e chiederne rettifica o altre misure necessarie da adottare in modo tempestivo.
> Se una persona fisica rilevi che un elaboratore di informazioni ha violato le disposizioni di leggi o regolamenti amministrativi o l'accordo tra le parti durante l'elaborazione delle sue informazioni personali ha diritto di chiedere all'elaboratore di informazioni di cancellarle in modo tempestivo».

La disposizione trova un precedente nell'art. 34 della Legge federale tedesca sulla protezione dei dati, nell' art. 15 del GDPR, nell'art. 3.11 della Legge sulla protezione dei dati personali di Taiwan.
Ci avviamo alla conclusione di questa rassegna. L'art. 1038:

> «Il responsabile del trattamento delle informazioni non deve divulgare o manomettere le informazioni personali che raccoglie e memorizza e senza il consenso del titolare non può offrire illegalmente ad altri le informazioni personali, salvo che queste, dopo essere state elaborate, non siano più riconducibili a uno specifico soggetto e non possano essere riportati al loro stato originario.
> Il responsabile del trattamento delle informazioni deve adottare misure tecniche e altre misure necessarie, per garantire la sicurezza delle informazioni personali che raccoglie e archivia e impedire che le informazioni siano divulgate, manomesse o smarrite. Se le informazioni personali di una persona sono divulgate, manomesse o smarrite o è probabile che lo siano, si devono adottare misure correttive in modo tempestivo e informare le persone fisiche in conformità con i regolamenti e riferire alle autorità competenti interessate».

specifica il divieto di fornire illegalmente informazioni personali senza il consenso del titolare. Il termine "divulgare" comprende sia la diffusione a soggetti non specificati sia la fornitura di informazioni a persone specifiche. Nell'era dei big data, le informazioni o i dati sono un'importante risorsa produttiva e competitiva, i dati costituiscono il veicolo attraverso il quale le informazioni esistono nel mondo di internet. L'elaborazione tecnica e il trasferimento delle informazioni, così come l'accesso da parte di terzi, sono le situazioni principali in cui le informazioni personali vengono fornite ad altri. In tutti e tre i casi la divulgazione di informazioni personali richiede il consenso della persona.
Secondo l'art. 42, c. 1, della Legge sulla sicurezza della rete, l'anonimizzazione dovrebbe raggiungere un livello tale da non consentire l'identificazione di un individuo spe-

子信息的侵权行为及其责任), in *Journal of Legal Science (Journal of Northwest University of Political Science and Law)*, 2013, 147 ss.

cifico. Il c. 2 prevede, inoltre, un obbligo specifico, per i responsabili del trattamento delle informazioni di salvaguardarne la sicurezza. Questa disposizione, che riprende l'art. 4 della Decisione del Comitato permanente dell'Assemblea Popolare Nazionale sul rafforzamento della protezione delle informazioni di rete (全国人民代表大会常务委员会关于加强网络信息保护的决定) del 28 dicembre 2012, prevede che i responsabili del trattamento delle informazioni adottino misure tecniche e altre misure necessarie per garantire la sicurezza delle informazioni personali dagli stessi raccolte ed archiviate al fine di prevenirne la fuga, la distruzione o la perdita. La violazione dell'obbligo di garantire la sicurezza delle informazioni si differenzia dalla suddetta violazione del principio del consenso informato in quanto la prima si concentra sulla raccolta e sul trattamento delle informazioni effettuate intenzionalmente dai responsabili del trattamento senza il consenso dell'interessato. Richiamando anche le previsioni degli standard tecnici relativi alla sicurezza delle informazioni personali, gli artt. 10 e 11 delle Specificazioni relative alla sicurezza delle informazioni personali (*Information Security Technology Personal Information Security Specification*, 信息安全技术个人信息安全规范) forniscono disposizioni dettagliate su come i responsabili del trattamento delle informazioni personali debbano gestire i casi di "incidente" e sui requisiti per la gestione della sicurezza delle informazioni personali all'interno dell'organizzazione responsabile del trattamento delle informazioni personali.
L'ultimo articolo che il Cod. civ. cin. dedica in modo specifico alla materia è il 1039 con una disposizione generale:

> «Gli organi statali e le istituzioni previste dalla legge che svolgono funzioni amministrative nonché il loro personale, devono rispettare la riservatezza delle persone fisiche e i dati personali ottenuti nello svolgimento delle loro funzioni, non potendoli divulgare o fornire illegalmente ad altri».

Nella versione finale è stato aggiunto «Gli organi statali e le istituzioni previste dalla legge che svolgono funzioni amministrative», sul presupposto che gli organi statali raccolgono spesso informazioni personali su larga scala per lo svolgimento dei loro compiti. Alla luce di ciò, l'art. 10, c. 2, della Decisione del Comitato permanente dell'Assemblea Popolare Nazionale sul rafforzamento della protezione delle informazioni su internet (全国人民代表 大会常务委员会关于加强网络信息保护的决定) del 2012 emendato nel 2021 dispone che «[…] gli organi statali e il loro personale devono mantenere riservate le informazioni elettroniche personali dei cittadini conosciute nell'esercizio delle loro funzioni e non devono divulgarle, manometterle o distruggerle, né venderle o fornirle illegalmente ad altri». Medesima linea è fissata dall'art. 44 della Legge sulla sicurezza della rete:

> «Nessun individuo o organizzazione può sottrare o ottenere informazioni personali in modi illegali, o vendere o fornire illegalmente informazioni personali ad altri».

così come dall'art. 45:

> «I dipartimenti responsabili della supervisione e dell'amministrazione della sicurezza della rete in conformità con la legge e il loro personale devono proteggere rigorosamente le informazioni personali, la privacy e i segreti commerciali di cui vengono a conoscenza nell'esercizio delle loro funzioni».

La dottrina ha, a tal proposito, sostenuto che l'uso dei big data abbia rafforzato il differenziale di potere esistente tra le autorità statali e i soggetti interessati alla tutela delle informazioni[43].

4. Struttura e tratti salienti della Legge sulla tutela delle informazioni personali

La Legge sulla protezione delle informazioni personali si compone di 74 articoli raccolti in otto capitoli. Si è ritenuto opportuno riportare in questa sede, ed a fini di chiarezza dello scritto, le disposizioni salienti della Legge al fine di comprenderne il significato.
Il capitolo Primo "Disposizioni generali", fissa all'art. 1 l'ambito di applicazione della normativa da cui si evincono le diverse finalità della Legge medesima: proteggere i diritti e gli interessi relativi alle informazioni personali, disciplinarne il trattamento e promuoverne l'utilizzo ragionevole (合理*hélǐ*):

> «Questa legge è emanata in conformità con la Costituzione per proteggere i diritti e gli interessi relativi alle informazioni personali□, disciplinare il trattamento delle informazioni personali e promuoverne l'uso ragionevole».

È evidente la somiglianza con l'art. 1 del GDPR ma, in modo particolare, è interessante soffermarsi sul riferimento alla ragionevolezza, quale criterio che consente un certo margine di libertà nell'uso delle informazioni personali ed in funzione dei singoli obiettivi, di volta in volta, da raggiungere. Importante, inoltre, il riferimento alla conformità costituzionale, che conferisce alla Legge una posizione privilegiata riguardo alla finalità perseguita.
L'art. 3:

> «La presente legge si applica al trattamento delle informazioni personali delle persone fisiche all'interno del territorio della Repubblica Popolare Cinese.
> La presente legge si applica anche al trattamento delle informazioni personali di persone fisiche all'interno del territorio della Repubblica popolare cinese al di fuori del territorio della Repubblica popolare cinese in una delle seguenti circostanze:
> i) quando lo scopo è quello di fornire prodotti o servizi a persone fisiche nazionali;
> ii) quando le attività delle persone fisiche nazionali sono analizzate e valutate; e
> iii) altre circostanze previste dalle leggi e dai regolamenti amministrativi»,

[43] In lingua cinese 个人信息 *gèrén xìnxī*.

fissa il principio di extraterritorialità che garantisce una sorta di estensione extraterritoriale della Legge. La Legge sulla sicurezza della rete non ha validità extraterritoriale, mentre tale principio è contenuto nella Legge sulla sicurezza dei dati, all'art.2. La disposizione prevede l'applicazione della Legge sia al trattamento delle informazioni personali delle persone fisiche all'interno dei confini della Repubblica Popolare Cinese sia al trattamento delle medesime informazioni ma effettuato al di fuori dei confini della Repubblica Popolare Cinese, nelle ipotesi in cui la finalità ultima sia quella di fornire prodotti o servizi ad individui cinesi che si trovino entro i confini nazionali; sia alle ipotesi di analisi o valutazione delle attività di persone fisiche all'interno dei confini del Paese sia ad altre circostanze previste da leggi o regolamenti amministrativi. Nel contenuto, dunque, l'art. 3 è analogo al suo corrispondente nel GDPR.
L'art. 4 fornisce la nozione di informazione personale e di trattamento:

> «Per informazioni personali si intendono tutti i tipi di informazioni relative a persone fisiche identificate o identificabili, registrate con mezzi elettronici o di altro tipo, ad esclusione delle informazioni gestite in forma anonima.
> Il trattamento delle informazioni personali comprende la raccolta, l'archiviazione, l'uso, l'elaborazione, la trasmissione, la fornitura, la divulgazione e la cancellazione, ecc. delle informazioni personali».

Sono informazioni personali tutte quelle registrate con mezzi elettronici o altri mezzi, relative a persone fisiche identificate o identificabili, escluse le informazioni che risultino dal trattamento di anonimizzazione. Pertanto, ai sensi della Legge le informazioni anonimizzate non sono informazioni personali coperte dall'ambito di tutela della Legge. La disposizione ha un contenuto analogo all'art. 4 del GDPR secondo il quale è dato personale qualsiasi informazione riguardante una persona fisica identificata o identificabile. Si considera a tal fine identificabile la persona fisica che può essere individuata, direttamente o indirettamente, con particolare riferimento ad elementi quali il nome, un numero di identificazione, dati relativi alla sua generale ubicazione, identificativi presenti online o ad uno o più elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale con una sostanziale corrispondenza di tenore salva una maggiore attenzione della disposizione cinese circa la definizione di trattamento.
Gli artt. 6, 7, 8 ed 11 guidano il trattamento e l'utilizzo delle informazioni personali contemperando diversi interessi, circoscrivendo il trattamento ad uno "scopo preciso e ragionevole" quasi a proteggere in modo aperto e dichiarato il singolo, restituendo dignità e cercando di porre fine alla smisurata raccolta di dati:

> «Il trattamento delle informazioni personali deve avere uno scopo preciso e ragionevole, essere direttamente correlato allo scopo del trattamento e deve essere condotto in modo da ridurre al minimo l'impatto sui diritti e gli interessi personali.
> La raccolta di informazioni personali deve essere limitata al minimo indispensabile per raggiungere lo scopo del trattamento e non è consentita una raccolta eccessiva

di informazioni personali».

L'art. 7 fissa i principi guida e di interpretazione dell'intero testo di Legge:

> «Il trattamento dei dati personali deve seguire i principi di apertura e trasparenza, rendere pubbliche le regole per il trattamento dei dati personali e indicare espressamente le finalità, le modalità e la portata di tale trattamento».

La previsione è analoga a quella contenuta nel Considerando 39 del GDPR secondo cui qualsiasi trattamento dei dati personali deve essere lecito e corretto, le modalità con cui sono raccolti i dati, il loro utilizzo, la loro consultazione e trattamento devono essere chiari e precisi per le persone fisiche. I principi fondamentali qui elencati, chiave di lettura e di interpretazione dell'intero testo della Legge erano già presenti nelle linee guida sulla privacy dell'OCSE e della Convenzione 108 del Consiglio d'Europa, per poi trovare conferma sia nella direttiva 95/46/CE dell'Unione europea sia nell' *Asia-Pacific Economic Cooperation Privacy Framework*.
Tra i principi generalmente presenti nei diversi ordinamenti vi sono quelli secondo cui i dati devono essere trattati in modo equo e lecito, e solo per le finalità specificate all'individuo; devono essere raccolte e trattate solo le informazioni personali necessarie per tali finalità e poi cancellate; tali dati devono essere pertinenti, accurati e aggiornati, i soggetti devono essere messi al corrente del trattamento che ne viene effettuato e dei loro relativi diritti, tali da consentire loro di esercitare un controllo. Devono essere previste garanzie aggiuntive per categorie particolari di dati, tutti i dati devono essere protetti da rischi quali la perdita o l'accesso non autorizzato, la distruzione, l'uso, la modifica o la divulgazione ed i responsabili del trattamento rispondono della mancata attuazione a questi principi.
Alcuni di questi principi esistono sia nell' Unione europea che negli Stati Uniti, quali ad esempio i requisiti di minimizzazione dei dati, trasparenza e qualità dei dati e risultano essere più stringenti in Europa; altri, quali ad esempio la protezione aggiuntiva per i dati sensibili, le restrizioni sui trasferimenti transfrontalieri, la supervisione da parte di un'autorità di vigilanza indipendente ed i limiti alla profilazione, diversamente, sono assenti nella normativa degli Stati Uniti.
L'art. 8 della Legge prevede che il trattamento delle informazioni personali debba garantire la qualità delle informazioni personali ed evitare effetti negativi sui diritti e sugli interessi individuali derivanti da informazioni personali imprecise o incomplete:

> «La qualità delle informazioni personali deve essere garantita nel trattamento delle informazioni personali per evitare l'impatto negativo sui diritti e gli interessi personali causato da informazioni personali inesatte o incomplete».

Analoga previsione è contenuta nel Considerando 86 del GDPR, secondo il quale il titolare del trattamento dovrebbe comunicare all'interessato la violazione dei dati personali senza indebito ritardo, qualora questa violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine

di consentirgli di prendere le necessarie precauzioni.
L'art. 11, vera e propria proclamazione, analoga all'art. 51 del GDPR, afferma il ruolo centrale dello Stato, il quale istituisce un sistema efficiente e completo per la protezione delle informazioni personali al fine di prevenire e punire atti lesivi dei diritti e degli interessi sulle informazioni personali, rafforzare la pubblicità e l'educazione sulla protezione delle informazioni personali ed infine promuovere la creazione di un contesto idoneo alla protezione delle informazioni personali medesime:

> «Lo Stato stabilisce un solido sistema di protezione delle informazioni personali, previene e punisce la violazione dei diritti e degli interessi delle informazioni personali, rafforza la pubblicità e l'educazione alla protezione delle informazioni personali e promuove la formazione di un buon ambiente in cui il governo, le imprese, le organizzazioni sociali interessate e il pubblico partecipano congiuntamente alla protezione delle informazioni personali».

Alle modalità di trattamento delle informazioni personali e ai diversi tipi di consenso sono dedicati diversi articoli: 13, 15, 23, 29 e 39.
Art. 13:

> «Solo in una delle seguenti circostanze il responsabile del trattamento delle informazioni personali può trattarle:
> i) ove sia ottenuto il consenso dell'interessato;
> ii) quando il consenso è necessario per la conclusione o l'esecuzione di un contratto di cui l'interessato è parte, o per l'attuazione della gestione delle risorse umane in conformità con le norme e i regolamenti del lavoro formulati in conformità alla legge e al contratto collettivo concluso a norma di legge;
> iii) ove sia necessario per l'adempimento di doveri o obblighi di legge;
> iv) ove sia necessario per la risposta a un'emergenza sanitaria pubblica o per la tutela della vita, della salute e della sicurezza dei beni di una persona fisica;
> v) laddove atti come la segnalazione di notizie e la supervisione da parte dell'opinione pubblica siano effettuati nell'interesse pubblico e il trattamento dei dati personali rientri in uno scopo ragionevole;
> vi) quando è necessario trattare le informazioni personali divulgate dall'interessato o altre informazioni personali che sono state legalmente divulgate entro un ambito ragionevole in conformità con le disposizioni della presente legge;
> vii) altre circostanze previste da leggi e regolamenti amministrativi.
> Il trattamento delle informazioni personali è soggetto al consenso dell'interessato in conformità con le altre disposizioni pertinenti della presente legge; tuttavia, il consenso dell'interessato non è richiesto nelle circostanze di cui ai punti da ii) a vii) del comma precedente».

Quanto disposto dall'art. 13 della Legge è analogo a quanto previsto dall'art. 6 del GDPR, che indica come i dati personali possano essere utilizzati in modo lecito e trasparente, laddove il primo statuisce che il trattamento dei dati è lecito solo se e nella

misura in cui ricorrano determinate condizioni, tra cui la prestazione del consenso espresso dall'interessato, la necessità del trattamento rispetto all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso, *et cetera.*
Il consenso è disciplinato dall'art. 15:

> «Qualora il trattamento dei dati personali si basi sul consenso dell'interessato, l'interessato ha il diritto di revocare il consenso. Il responsabile del trattamento dei dati personali fornisce un metodo conveniente per l'individuo per revocare il proprio consenso.
> La revoca del consenso da parte dell'interessato non pregiudica la validità di qualsiasi attività di trattamento dei dati personali condotta sulla base del consenso dell'interessato prima di tale revoca».

La Legge stabilisce il principio di convenienza. Anche se non è specificato chiaramente in cosa consista, è generalmente inteso che la difficoltà di "rilevare il consenso" non dovrebbe essere maggiore di quella di prestarlo.
Riguardo alle informazioni sensibili queste trovano una propria regolamentazione negli artt. 28 - 32:

> «Le informazioni personali sensibili si riferiscono alle informazioni personali che potrebbero ledere la dignità personale di qualsiasi persona fisica, o danneggiare la sua sicurezza personale o patrimoniale una volta divulgate o utilizzate illecitamente, comprese informazioni quali l'identificazione biometrica, il credo religioso, l'identità specifica, lo stato di salute, i conti finanziari, la posizione e le tracce, nonché le informazioni personali dei minori di 14 anni.
> Solo per specifiche finalità e sufficienti necessità, e qualora siano state adottate rigorose misure di protezione, il responsabile del trattamento può trattare le informazioni sensibili»;

> «Il trattamento delle informazioni personali sensibili di un individuo è soggetto al separato consenso dell'interessato; ove le leggi e i regolamenti amministrativi prevedano che il trattamento delle informazioni personali sensibili sia subordinato al consenso scritto, prevalgono tali disposizioni»;

> «Riguardo alle informazioni personali sensibili di una persona fisica, il responsabile del trattamento dei dati personali deve informare la persona interessata, oltre alle fattispecie indicate dal comma 1 dell'articolo 17, della necessità del trattamento delle sue informazioni sensibili e dell'impatto sui suoi diritti soggettivi e interessi, ad eccezione delle circostanze per le quali può essere esentato dall'informare l'individuo in conformità con questa legge»;

> «Per operare il trattamento delle informazioni personali di un minore di età inferiore ai 14 anni, il responsabile del trattamento deve ottenere il consenso dei

genitori o di altri tutori del minore.
Per operare il trattamento delle informazioni personali dei minori di età inferiore ai 14 anni, il responsabile del trattamento predisporrà regole specifiche per il trattamento dei dati personali».

L'art. 31 della Legge e l'art. 8 del GDPR disciplinano entrambi il trattamento delle informazioni personali dei minori. Vi sono, tuttavia, alcune differenze tra le due disposizioni: l'art. 31 della Legge cinese richiede che i responsabili del trattamento ottengano il consenso esplicito dei tutori legali dei minori prima di procedere al trattamento dei dati; l'art. 8 del GDPR richiede, invece, che i responsabili del trattamento ottengano il consenso esplicito dei minori stessi se hanno un'età idonea a comprendere le implicazioni del loro consenso prestato. Inoltre, il Considerando 38 del GDPR riconosce espressamente che i minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia nonché dei loro diritti in relazione al trattamento delle informazioni personali.

«Qualora leggi e regolamenti amministrativi prevedano che il trattamento delle informazioni personali sensibili sia soggetto alla relativa autorizzazione amministrativa o ad altre restrizioni, prevarranno tali disposizioni».

Altro tema centrale affrontato dalla Legge riguarda il trasferimento e la localizzazione dei dati su cui già si è riferito nell'art. 3. Sul tema si sofferma un intero capitolo, il Terzo della Legge "Regole per la fornitura transfrontaliera di informazioni personali", artt. 38 - 43.
Gli artt. 38 e 39 impongono ai responsabili del trattamento dei dati che intendono fornire informazioni personali al di fuori del territorio della Repubblica Popolare Cinese di adottare una tra le seguenti misure: i) una valutazione del rischio di trasferimento dei dati da parte della Amministrazione per la sicurezza del ciberspazio (*Cybersecurity Administration of China*, CAC); ii) una certificazione legale rilasciata da un'agenzia specializzata nella protezione delle informazioni personali; iii) la sottoscrizione di clausole contrattuali standard (*Standard Contractual Clauses*, SCC) formulate dalla medesima Amministrazione; iv) l'adozione di altre misure richieste da leggi, regolamenti amministrativi o dall' Amministrazione per la sicurezza del ciberspazio. Si richiede, inoltre, il consenso separato dell'interessato. Sul tema, a dimostrazione del continuo aggiornamento, sono stati rilasciati sia un nuovo regolamento sulla valutazione del rischio di trasferimento "Misure di valutazione della sicurezza per i trasferimenti di dati in uscita" (*Security assessment measures for outbound data transfers,* 数据出境安全评估办法[44], di seguito "Misure") in vigore dal 1° settembre 2022 [45], sia le Disposizioni sui contratti

[44] Il Regolamento, pubblicato il 7 luglio 2022, è in vigore dal 1° settembre 2022. Disciplina il trasferimento dei dati in uscita, protegge diritti e interessi inerenti alle informazioni personali e mira a garantire al contempo la sicurezza nazionale e un flusso transfrontaliero libero. Le Misure sono formulate tenendo conto della previgente disciplina contenuta nelle tre principali leggi in materia di dati e nei regolamenti di dettaglio.

[45] Per la traduzione in lingua inglese del Regolamento, vedi qui.

standard per il trasferimento transfrontaliero di informazioni personali (*Provisions on Standard Contracts for Cross-border Transfers of Personal Information*, 个人信息出境标准合同规定) in vigore dal 1° giugno 2023.

Dalla lettura del combinato disposto dell'art. 40 della Legge e dell'art. 4 delle Misure, si evince che il responsabile del trattamento delle informazioni che fornisce informazioni all'estero deve, in una delle seguenti circostanze, richiedere una valutazione della sicurezza del trasferimento delle informazioni in uscita al Dipartimento nazionale per la sicurezza informatica e l'informatizzazione attraverso il dipartimento locale: i) il responsabile del trattamento dei dati fornisce dati importanti[46] all'estero; ii) gli operatori di infrastrutture informatiche critiche (CIIO)[47] o i responsabili del trattamento dei dati che elaborano i dati personali di oltre 1 milione di persone hanno la necessità di fornire informazioni personali all'estero; iii) i responsabili del trattamento dei dati hanno fornito all'estero informazioni personali di oltre 100.000 persone o informazioni personali sensibili[48] di oltre 10.000 persone, dal 1° gennaio dell'anno precedente; iv) altre circostanze stabilite dalla CAC.

In base agli articoli 60, 63 e 64 della Legge, la Cina ha implementato meccanismi diversificati riguardo alla protezione delle informazioni personali. L' Amministrazione per la sicurezza del ciberspazio è responsabile del coordinamento della protezione delle informazioni personali e delle relative attività di supervisione e amministrazione, così come i competenti dipartimenti del Consiglio degli Affari di Stato sono responsabili della protezione, supervisione e amministrazione della protezione delle informazioni personali in conformità con le leggi e i regolamenti vigenti:

> «L'Amministrazione per la sicurezza del ciberspazio è responsabile per il coordinamento della protezione dei dati personali e del relativo lavoro di supervisione e di amministrazione. I dipartimenti pertinenti del Consiglio di Affari di Stato sono responsabili per la protezione, la supervisione e l'amministrazione della pro-

[46] Gli "*important data*" erano già previsti sia dalla CSL, sia dalla DSL, sebbene in nessuna delle due Leggi fosse fornita una definizione precisa. La lacuna è stata colmata dall'art 19 delle nuove Misure, che li definisce come «dati che, se alterati, distrutti, trapelati, acquisiti o utilizzati illegalmente, ecc. possono danneggiare la sicurezza nazionale, le operazioni economiche, la stabilità sociale, la salute o la sicurezza pubblica, ecc.».

[47] L'art. 2 dei Regolamenti sulla sicurezza e la protezione delle infrastrutture critiche informatizzate (*Critical Information Infrastructure Security Protection Regulations* - 关键信息基础设施安全保护条例), in vigore dal 1° settembre 2021, le identifica in infrastrutture di rete e sistemi informativi, impegnati in importanti settori come le telecomunicazioni pubbliche e i servizi informativi, l'energia, i trasporti, l'acqua, la finanza, i servizi pubblici, l'*e-government*, la scienza, la tecnologia e l'industria della difesa nazionale, o qualsiasi altra importante struttura di rete o sistema informativo che possa danneggiare gravemente la sicurezza, l'economia nazionale e i mezzi di sussistenza delle persone, o l'interesse pubblico in caso di incapacità, danni o fughe di dati.

[48] I dati personali sensibili vengono definiti dall'art 28 della PIPL come «i dati personali che, una volta divulgati o utilizzati illegalmente, potrebbero causare un danno alla dignità personale di una persona fisica o un danno alla sua sicurezza personale o patrimoniale, compresi i dati di identificazione biometrica, il credo religioso, l'identità specifica, la salute medica, il conto finanziario e gli spostamenti e le tracce, nonché i dati personali dei minori di 14 anni». Lo stesso articolo specifica, a seguire, che tali dati possono essere trattati solo «per uno scopo specifico e per una necessità sufficiente, e se sono state adottate misure di protezione rigorose».

tezione delle informazioni personali nell'ambito delle loro rispettive funzioni in conformità con le disposizioni della presente legge, delle leggi e dei regolamenti amministrativi pertinenti.
Le funzioni dei dipartimenti pertinenti dei governi del popolo locali a un livello pari o superiore alla contea per la protezione, la supervisione e l'amministrazione della protezione dei dati personali devono essere determinati in conformità con le relative disposizioni dello Stato.
I dipartimenti menzionati nei precedenti due paragrafi sono collettivamente indicati come le autorità preposte alle funzioni di protezione dei dati personali».

«Le autorità che svolgono compiti di protezione dei dati personali possono adottare le seguenti misure nello svolgimento di tali compiti:
(1) informare le parti interessate e indagare sulle circostanze relative alle attività di trattamento dei dati personali;
(2) esaminare e copiare contratti, registrazioni, libri contabili e altro materiale pertinente relativo alle attività di trattamento dei dati personali delle parti interessate;
(3) svolgere ispezioni in loco e indagini sulle attività di trattamento dei dati personali sospettate illecite;
(4) ispezione dei dispositivi e degli oggetti relativi alle attività di trattamento dei dati personali; i dispositivi e gli oggetti risultanti utilizzati per attività illecite di trattamento dei dati personali possono essere sequestrati o confiscati previa istanza scritta e approvazione del responsabile principale dell'autorità interessata.
Le autorità che svolgono compiti di protezione dei dati personali adempiono a tali obblighi ai sensi di legge, gli interessati prestano assistenza e collaborazione, non rifiutano od ostacolano tale adempimento».

Quanto disposto dall'art. 63 della Legge è paragonabile a quanto previsto dall'art. 58 del GDPR, il quale indica i poteri di indagine, correttivi, autorizzativi e consultivi delle autorità. L'art. 63 conferisce alle autorità di protezione dei dati il potere di imporre multe e altre sanzioni amministrative nei confronti dei responsabili e degli incaricati del trattamento dei dati che violano le disposizioni della Legge, così come l'art. 58 del GDPR conferisce alle autorità di protezione dei dati il potere di imporre multe e altre sanzioni amministrative ai responsabili e agli incaricati del trattamento che violano le disposizioni del Regolamento.

«Qualora le autorità che svolgono compiti di protezione dei dati personali rilevino nell'esercizio di tali compiti che vi sono rischi elevati nelle attività di trattamento dei dati personali o si sono verificati incidenti di sicurezza dei dati personali, possono, secondo i limiti e le procedure prescritte, avere un colloquio con il legale rappresentante o il principalmente responsabile del gestore del trattamento dei dati personali interessato, o richiedere a tale gestore di affidare a un'agenzia specializzata lo svolgimento di un controllo di conformità sulle sue attività di trattamento dei dati personali. Il gestore del trattamento dei dati personali adotta come richiesto delle misure al fine di rettificare ed eliminare i pericoli nascosti.

> Qualora le autorità preposte alla protezione dei dati personali riscontrino nell'esercizio di tali compiti che un trattamento illecito di dati personali sia sospettato di costituire reati, ne informano tempestivamente le autorità di pubblica sicurezza al fine di provvedere a norma di legge».

Infine, meritevole di considerazione è il Capitolo settimo "Responsabilità legale", artt. 66 - 71. Rispetto alla normativa precedentemente elaborata, le sanzioni previste dalla Legge in esame sono assai più elevate in connessione alle maggiori responsabilità configurate in capo sia agli individui che alle organizzazioni.

> «Nel caso in cui i dati personali siano trattati in violazione delle disposizioni della presente legge, o i dati personali siano trattati senza adempiere all'obbligo di protezione dei dati personali previsto dalla presente legge, le autorità che svolgono compiti di protezione dei dati personali ordina all'interessato di apportare correzioni, notificare avvertimenti, confiscare i ricavati illeciti, a qualsiasi applicazione che tratti illecitamente dati personali è ordinata la sospensione o la cessazione della prestazione dei servizi; colore che rifiutano il giusto adempimento, si applica la sanzione pecuniaria non superiore a 1 milioni di yuan; per coloro che sono principalmente e direttamente responsabili si applica la sanzione pecuniaria non inferiore a 10.000 yuan e non superiore a 100.000 yuan.
> Per ogni atto illecito precedentemente indicati, con circostanze gravi, le autorità che svolgono compiti di protezione dei dati personali a livello provinciale o superiore ordinano all'interessato di apportare correzioni, confiscare i ricavi illeciti e si applica la sanzione pecuniaria non superiore a 50 milioni di yuan o non più del 5% del fatturato dell'anno precedente, e può anche ordinare la sospensione dell'attività pertinente o sospendere l'attività per la rettifica e informare le autorità competenti pertinenti di revocare il relativo permesso commerciale o licenza commerciale; alle persone principalmente e direttamente responsabili si applica la sanzione pecuniaria non inferiore a 100.000 yuan e non superiore a 1 milione di yuan, è possibile inoltre vietare a tali persone di agire come amministratori, supervisori, alti dirigenti e responsabili della protezione dei dati personali delle imprese interessate entro un determinato periodo di tempo».

Può essere effettuato un parallelismo tra la disposizione dell'art. 66 della Legge e l'art. 83 del DGPR. L'art. 66 della Legge prevede che le aziende debbano ottenere il consenso degli utenti prima di raccogliere le loro informazioni personali e richiede che esse informino gli utenti sul loro utilizzo e sul loro diritto di richiederne la cancellazione. Disposizione simile si rinviene all'art. 83 del GDPR, il quale stabilisce le condizioni generali per comminare sanzioni amministrative di tipo pecuniario, che le sanzioni amministrative pecuniarie debbano essere efficaci, proporzionate e dissuasive, che qualora un titolare del trattamento o un responsabile del trattamento violi, con dolo o colpa più disposizioni del Regolamento l'importo totale della sanzione amministrativa pecuniaria non possa superare l'ammontare previsto per la violazione più grave.

«Gli atti illeciti previsti dalla presente legge sono registrati negli archivi dei crediti secondo le disposizioni di legge e di regolamento amministrativo in materia e sono portati a conoscenza del pubblico».

«Qualora un organo statale non adempia all'obbligo di protezione delle informazioni personali previsto dalla presente legge, il suo organo superiore o le autorità che svolgono compiti di protezione delle informazioni personali ordinano alle persone principalmente o direttamente responsabile di apportare correzioni, e gli sono comminate sanzioni ai sensi di legge».

Una disposizione simile all'art. 68 della Legge è totalmente assente nel GDPR, probabilmente ciò è dovuto alla natura indipendente della autorità europea di controllo e dell'applicabilità, a tali casi, degli ordinari rimedi previsti dal diritto amministrativo. La disposizione più simile presente nel GDPR è quella dell'art. 83 secondo cui, fatti salvi i poteri correttivi delle autorità di controllo a norma dell'art. 58, par. 2, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti nello Stato membro.

«Qualora un membro del personale delle autorità che svolge compiti di protezione dei dati personali trascuri il proprio dovere, abusa del proprio potere, fa favoritismi e commette irregolarità, che non costituiscono reato, gli sono comminate sanzioni in conformità con la legge»;

«Qualora il trattamento dei dati personali leda i diritti e gli interessi in materia di dati personali e causi un danno, il gestore del trattamento dei dati personali, se non può dimostrare di non avere colpa, è considerato responsabile per i danni e per le altre violazioni responsabili»;
«La responsabilità per i danni precedentemente indicati è determinata sulla base delle perdite così subite dall'interessato o dei benefici così ottenuti dal gestore del trattamento; se le perdite così subite dall'interessato o i benefici così ottenuti dal gestore del trattamento delle informazioni sono difficili da determinare, l'importo dei danni deve essere determinato in base alle circostanze effettive»;

«Qualora un gestore del trattamento delle informazioni personali elabori informazioni personali in violazione della presente legge, che lede i diritti e gli interessi di un gran numero di persone, la Procura del popolo, le organizzazioni dei consumatori riconosciute dalla legge e le organizzazioni determinate dall'ACC possono portare una querela davanti a un tribunale del popolo ai sensi di legge»;

«Qualora la violazione delle presenti disposizioni costituisca violazione dell'amministrazione di pubblica sicurezza, si applica la sanzione amministrativa di pubblica sicurezza a norma di legge e, se si configura reato, la responsabilità penale è accertata a norma di legge».

5. Posizione e ruolo della Legge sulla protezione delle informazioni personali all'interno dell'ordinamento. La coerenza del sistema

Come anticipato nei precedenti paragrafi, è evidente il crescente impegno del legislatore cinese per la costruzione di un regime di protezione delle informazioni personali. A fronte della presenza di un testo legislativo unitario di riferimento, permane riferibile ad una pluralità di fonti di diverso grado, di Interpretazioni della Corte Suprema del Popolo nonché di standard tecnici che regolamentano la materia.
In tal senso merita di essere verificata la coerenza interna dell'ordinamento, nello specifico il rapporto tra la Legge ed il Cod. civ. cin.[49] i cui libri sono stati pubblicati in periodi diversi: il 1° ottobre 2017 è entrato in vigore il Libro Primo del Codice "Parte generale"; il 1° gennaio 2021 sono entrati in vigore i restanti sei libri del Codice; il 1° novembre 2021, come già riportato, è entrata in vigore la Legge sulla tutela delle informazioni personali[50].
L'art. 1 della Legge, già precedentemente menzionato:

> «Questa legge è emanata in conformità con la Costituzione per proteggere i diritti e gli interessi delle informazioni personali, disciplinare il trattamento dei dati personali e promuovere l'uso ragionevole delle informazioni personali».

indica la conformità alla Costituzione, quale fattore essenziale che conferisce alla Legge una posizione privilegiata in linea con quanto avviene nella normativa europea dove l'art. 8 della Carta dei diritti fondamentali del 2000 assegna alla protezione delle informazioni personali il carattere di diritto fondamentale indipendente[51]. La Legge, ritenuta fondamentale (基本法*jīběnfǎ*) appena al di sotto della Costituzione, deve rispettare le disposzioni del Cod. civ. cin. con cui deve necessariamente coordinarsi.
L'art. 69 della Legge pone un rinvio al Codice:

---

[49] Sul tema di interessse le considerazioni in L. Wang – B. Xiong, *Personality Rights in China's New Civil Code: A Response to Increasing Awareness of Rights in an Era of Evolving Technology*, in *Modern China*, 47(6), 2021, 703 ss.

[50] W. Liming, *On China's Civil Law Codification and the Development of China's Civil Law Scholarship*, in *Contemporary Social Sciences*, 3, 2020, 99 ss. , spec. 103 ss.:« […] *the codification improved the value system of civil law. From the perspective of comparative law, after the enactment of the civil code, the changes of the social, political, and cultural backgrounds and the economic conditions will cause scholars to re-examine and discuss the value and rationality of corresponding regulations. Alan Watson pointed out that the value rationality of the civil code is the ultimate concern for people (Watson, 2005, 269). In essence, civil law is the law for people, and strengthening the concern for humanism is an important trend in contemporary civil law. China's civil legislation reflects the concern for humanism and the innovation of ideas. Traditional civil law is concerned only with abstract individuals, not with the interests of special groups (Radbruch, 1997, 66). From an abstract concept to a specific person, "it is closer to the essence of private law to improve the status of the weak in the market and enhance their ability to realize their will." The concern of humanism has been sufficiently demonstrated in China's civil code*».

[51] Art. 8 Carta dei diritti fondamentali dell'Unione europea: «Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.
2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.
3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

> «Qualora il trattamento delle informazioni personali leda i diritti e gli interessi in materia di informazioni personali e causi un danno, il responsabile del trattamento delle informazioni personali, se non può dimostrare di non avere colpa, è considerato responsabile per i danni e per le altre violazioni responsabili.
> La responsabilità per i danni precedentemente indicati è determinata sulla base delle perdite così subite dall'interessato o dei benefici così ottenuti dal gestore del trattamento; se le perdite così subite dall'interessato o i benefici così ottenuti dal gestore del trattamento delle informazioni sono difficili da determinare, l'importo dei danni deve essere determinato in base alle circostanze effettive»,

laddove, accanto alla presunzione di colpa quale principio di imputazione vi è un rimando alle disposizioni del Codice civile sulla responsabilità civile con esplicito riferimento alla responsabilità per fatto illecito.
A dimostrazione di questa ampia coesistenza a livello sistemico interno, ora tra Legge e Codice penale, è di ausilio l'art. 71 della Legge:

> «Qualora la violazione delle presenti disposizioni costituisca violazione dell'amministrazione di pubblica sicurezza, si applica la sanzione amministrativa di pubblica sicurezza a norma di legge e, se si configura reato, la responsabilità penale è accertata a norma di legge».

Entriamo più nel dettaglio con alcuni esempi. Per quanto riguarda la nozione di informazione personale questa è prevista sia dall'art. 1034, c. 2, del Cod. civ. cin.:

> «Le informazioni personali sono quelle registrate elettronicamente o in altri modi che possano essere utilizzate, da sole o in combinazione con altre, per identificare una persona fisica, inclusi nome, data di nascita, numero di carta di identità, informazioni biometriche, indirizzo di residenza, numero di telefono, indirizzo email, informazioni sanitarie, ubicazione e simili della persona»,

sia dall'art. 4, c. 2, della Legge:

> «Per informazione personale si intende ogni tipo di informazione relativa a persone fisiche identificate o identificabili registrata con mezzi elettronici o con altri mezzi, escluse le informazioni trattate in forma anonima».

Quest'ultima disposizione è certamente più concisa e diverso ne è l'ambito di applicazione escludendo esplicitamente le informazioni anonimizzate che in tal modo non rientrano più nell'ambito delle informazioni personali escludendo l'applicabilità della Legge. Ulteriore esempio riguarda i diritti conferiti sulle proprie informazioni personali normativa fissata sia dall'art.1037 del Cod. civ. cin.:

> «Una persona fisica può consultare o fare copie delle sue informazioni personali

presso il responsabile del trattamento delle informazioni in conformità con la legge. Se la persona riscontra che le informazioni sono errate ha diritto di sollevare un'obiezione e chiederne rettifica o altre misure necessarie da adottare in modo tempestivo.
Se una persona fisica rilevi che un responsabile del trattamento delle informazioni ha violato le diposizioni di leggi o regolamenti amministrativi o l'accordo tra le parti durante l'elaborazione delle sue informazioni personali, ha diritto di chiedere al responsabile del trattamento delle informazioni di cancellarle in modo tempestivo».

sia dagli artt. 45, 46, c. 1 e c. 2, 47 e 48:

«Un individuo ha il diritto di consultare o copiare le proprie informazioni dal responsabile del trattamento dei dati personali, salvo che per le circostanze previste dall'art. 18 comma 1, e 35.
Qualora un individuo richieda di consultare o copiare le proprie informazioni, il responsabile del trattamento delle informazioni personali fornisce tali informazioni tempestivamente.
Qualora un individuo richieda di trasferire le proprie informazioni a un responsabile del trattamento dei dati personali da lui designato, il quale soddisfi le condizioni indicate dall'Amministrazione per la sicurezza del ciberspazio, il gestore delle informazioni personali fornisce indicazioni per il trasferimento»;

«Qualora un individuo ritenga che le proprie informazioni personali siano imprecise o incomplete, ha diritto di richiedere al responsabile delle informazioni personali di apportare correzioni o integrazioni.
Qualora un individuo richieda correzioni o integrazioni alle proprie personali, il responsabile del trattamento verifica e corregge o integra tempestivamente tali informazioni»;

«In una delle seguenti circostanze, un responsabile del trattamento delle informazioni personali assume l'iniziativa di cancellare le informazioni personali; qualora ometta di cancellarle, l'interessato ha il diritto di richiedere la cancellazione di tali informazioni:
(i) se la finalità del trattamento è stata raggiunta, è impossibile raggiungere tale obiettivo o non è più necessario raggiungerlo;
(ii) se il responsabile del trattamento delle informazioni personali cessa di fornire prodotti o servizi o il periodo di conservazione è scaduto;
(iii) se l'individuo ritira il proprio consenso;
(iv) se il responsabile del trattamento delle informazioni personali elabora informazioni personali in violazione della legge, regolamenti amministrativi o accordi;
(V) altre circostanze stabilite dalla legge o dai regolamenti amministrativi.
Se il periodo di conservazione previsto dalle leggi e dai regolamenti amministrativi non scade, o la cancellazione dei dati personali è difficile da realizzare tecnicamen-

te, il responsabile del trattamento dei dati personali interrompe il trattamento, oltre all'archiviazione e alle necessarie misure di protezione della sicurezza»;

«Gli individui hanno diritto a richiedere a un responsabile dei dati personali di indicare le proprie regole di processazione delle informazioni personali».

È evidente come la normativa fissata dalla Legge sia più dettagliata rispetto a quella fissata dal Cod. civ. cin. con cui ha continui rimandi ed integrazioni, modalità tipica del diritto cinese in continuo assestamento. Il legislatore, pertanto, è partito dal presupposto che la Legge debba coesistere con il previgente diritto civile e penale ma nel medesimo tempo arricchisca la normativa o resti silente laddove questa abbia già provveduto.

6. Diritto alla riservatezza e tutela delle informazioni personali

Il rapporto tra riservatezza ed informazioni personali è stato a lungo discusso in dottrina e concettualizzato in una solida tripartizione: quello alla protezione delle informazioni personali e quello alla riservatezza sono diritti distinti ma complementari; la protezione delle informazioni personali è un sottoinsieme del diritto alla riservatezza; il diritto alla tutela delle informazioni personali ha carattere indipendente e serve una moltitudine di funzioni, tra cui, ma non solo, la protezione dei dati personali. Accanto alla riservatezza ed alle informazioni personali, assumono caratteri precipui le informazioni sensibili.
Il diritto alla riservatezza trova una prima sistemazione, seguendo il criterio cronologico, negli artt. 38 e 40 della Cost.:

«La dignità personale dei cittadini della Repubblica Popolare Cinese è inviolabile».

«La libertà e la segretezza (秘密*mìmì)* della corrispondenza dei cittadini della Repubblica Popolare Cinese sono tutelate dalla legge. Nessuna organizzazione o individuo può, per nessun motivo, violare la libertà e la segretezza della corrispondenza dei cittadini, tranne nei casi in cui, per soddisfare le esigenze di sicurezza dello Stato o di indagini su reati penali, gli organi di pubblica sicurezza o procuratori sono autorizzati a censurare la corrispondenza secondo le procedure previste dalla legge».

e negli artt. 110, c. 1, e 1032 del Cod. civ. cin.:

«La persona fisica ha diritto alla vita, all'integrità del corpo, alla salute, al nome, all'immagine, alla reputazione, all'onore, alla riservatezza e all'autonomia coniugale».
«Ogni persona fisica ha diritto alla riservatezza. Nessuna organizza-

> zione o individuo può ledere l'altrui diritto alla riservatezza attraverso l'indagine, l'intromissione, la divulgazione o la pubblicizzazione e simili. La riservatezza consiste nella serenità della vita privata di una persona fisica e della sua sfera intima, delle sue attività private e nelle sue informazioni private che non vuole siano rese note ad altri».

Riguardo all'ambito di tutela, secondo quanto stabilisce l'art. 1032, il diritto alla riservatezza comprende lo spazio privato, le attività private e le informazioni private di una persona fisica che non vuole che altri ne vengano a conoscenza. Le informazioni personali, diversamente, sono informazioni di identificazione personale, tra cui il nome, la data di nascita, il numero del documento d'identità, le informazioni biometriche, l'indirizzo, il numero di telefono, l'indirizzo e-mail, le informazioni sulla salute, gli spostamenti, *et cetera*. Pertanto, come è evidenziato dalla dottrina tra diritto alla riservatezza e tutela delle informazioni personali vi sono alcune differenze: la riservatezza consiste nel diritto di tenere segreti aspetti, comportamenti, atti relativi alla sfera intima della persona, le informazioni personali enfatizzano l'identificazione e l'individuazione personale; il rapporto tra le due, non è di inclusione o esclusione, subordinazione o sovraordinazione, bensì un rapporto trasversale[52]. Certo è, tuttavia, che alcune informazioni personali, soprattutto quelle che riguardano la sfera personale, appartengono all'ambito della riservatezza (ad esempio lo stato civile, la salute fisica, le informazioni creditizie, il luogo in cui ci si trova, *et cetera*) essendo informazioni personali private (个人私密信息, *gèrén sīmì xìnxi*) mentre, di altre informazioni personali è evidente il carattere pubblico, nel senso di pubblicamente reperibili, quali ad esempio il nome, il sesso, il luogo di origine, *et cetera*. Le informazioni personali private rappresentano dunque il punto di intersezione tra riservatezza ed informazioni personali. In generale, è possibile sostenere che costituiscono informazioni personali private tutte le informazioni che un privato non vuole divulgare, non desiderando che altri ne vengano a conoscenza quali ad esempio le condizioni fisiche, lo stato di salute, le informazioni sui beni in proprietà, sulla famiglia, le informazioni genetiche, quelle relative ad esperienze personali e altre informazioni attinenti alla vita personale[53]. A causa di questo ambito di coincidenza, esse vengono tutelate su due diversi fronti.

Il Cod. civ. cin. sceglie di dare priorità alla tutela della riservatezza e la ragione di questa impostazione risiede nel fatto che il diritto alla riservatezza si concentra sulla protezione della dignità umana, mentre il diritto alla tutela delle informazioni personali si concentra sulla protezione dell'identità personale. La protezione della riservatezza, quindi, è più rigorosa e forte rispetto alla protezione delle informazioni personali. In secondo luogo, la materia della divulgazione delle informazioni personali private è soggetta al principio di riserva di legge in quanto nucleo centrale di protezione del diritto alla riservatezza, sebbene il diritto alla riservatezza appartenga ai diritti della personalità,

[52] Z. Xinbao (张新宝), *Raccolta di informazioni personali: i limiti dell'applicazione del principio del consenso informato*, in *Studi di diritto comparato*, 2019, 1 ss. e per ampi profili di comparazione Z. Xinbao, *Protezione giuridica del diritto alla riservatezza* (隐私权的法律保护), in *Mass Publishing House*, 1997.

[53] W. Liming (王利明) – C. Xiao (程啸), *Commentario al Codice civile cinese: diritti della personalità*, Beijing, 2020, 392 ss.

così come il diritto alla vita e alla salute, ma differenza dell'inderogabilità assoluta di questi ultimi, può essere derogato in modo condizionato in base alle esigenze di interesse pubblico o di interessi superiori[54]. Tuttavia, la possibile deroga può avvenire solo per legge, in base all'art. 1033[55] del Cod. civ. cin., quale atto approvato dall'Assemblea Popolare Nazionale[56].

L'art. 1033 del Codice stabilisce le regole e le procedure per il trattamento delle informazioni personali, stabilendo che nessuna organizzazione o individuo può trattare le informazioni private di un'altra persona salvo «diversa disposizione di legge o espresso consenso del titolare del diritto» diverso sia dal «consenso implicito», ma anche dal «semplice consenso». In tal senso, il titolare del diritto deve fornire un'esplicita manifestazione di volontà che deve essere una specifica espressione di consenso a specifiche informazioni private, non una vaga o una generica autorizzazione.

La portata del "consenso espresso" del titolare è vincolante per chi lo riceve e la divulgazione di informazioni private deve essere coerente con esso. Per ragioni di efficienza, il "consenso espresso" del titolare del diritto non è limitato alla forma scritta, ma può essere prestato oralmente, salva l'ipotesi prevista dall'art. 15 del Regolamento della Repubblica Popolare Cinese sulla divulgazione di informazioni governative (中华人民共和国政府信息公开条例) pubblicato il 5 aprile 2017 e successivamente emendato il 3 aprile 2019:

> «L'organo amministrativo non deve divulgare informazioni governative che riguardano segreti commerciali, riservatezza personale o altre informazioni la cui divulgazione causerebbe un danno ai legittimi diritti e interessi di terzi. Tuttavia, se i terzi acconsentono alla divulgazione o se l'organo amministrativo ritiene che la mancata divulgazione avrebbe un impatto significativo sull'interesse pubblico, le informazioni devono essere divulgate».

Il riferimento all'interesse pubblico deve essere inteso in senso stretto, a riprova di tale impostazione è l'art. 32 del Regolamento:

> «Qualora la divulgazione di informazioni governative in risposta a una domanda pregiudichi i diritti e gli interessi legittimi di un terzo, l'organo amministrativo chiede

---

[54] Z. Xinbao (张新宝), *Protezione giuridica del diritto alla riservatezza*, cit.

[55] Art. 1033 Cod. civ.cin.: «Salvo diversa disposizione di legge o espresso consenso del titolare del diritto, nessuna organizzazione o individuo deve compiere gli atti di seguito indicati:
(1) intromettersi nella vita privata di un'altra persona tramite telefonate, invio di messaggi di testo, utilizzo di strumenti di messaggistica istantanea, invio di posta elettronica e volantini e simili;
(2) entrare, scattare fotografie o spiare negli spazi privati altrui come la resi- denza o la camera d'albergo di un'altra persona;
(3) scattare fotografie, spiare, intercettare o divulgare le attività private di un'altra persona;
(4) scattare fotografie o spiare le parti intime del corpo di un'altra persona;
(5) elaborare le informazioni private di un'altra persona;
(6) violare la riservatezza di un'altra persona con altri mezzi».
V. anche art. 13 Legge sulla legislazione (立法法, *lìfǎ fǎ*) da ultimo emendata il 13 marzo 2023.

[56] Esempio è costituito dalla Legge sulla sicurezza dello stato (国家安全法*Guójiā ānquán fǎ*) promulgata dall'Assemblea Popolare Nazionale il 1° luglio 2015.

il parere del terzo per iscritto. Il terzo deve presentare il proprio parere entro 15 giorni lavorativi dalla data di ricevimento della richiesta di osservazioni. Se il terzo non presenta il proprio parere entro il termine stabilito, l'organo amministrativo decide se divulgarlo o meno in conformità alle disposizioni del presente Regolamento. Se il terzo non acconsente alla divulgazione e ha ragionevoli motivi per farlo, l'organo amministrativo non divulga le informazioni. Se l'organo amministrativo ritiene che la mancata divulgazione possa avere un impatto significativo sull'interesse pubblico, può decidere di divulgare l'informazione e informare per iscritto il terzo del contenuto e delle ragioni della decisione di divulgare l'informazione governativa».

Certo è che in questo modo è interamente delegata alla discrezionalità dell'autorità amministrativa ogni decisone e valutazione.
Il Codice civile cinese ha elaborato due distinte regole per la tutela della riservatezza e delle informazioni personali ed ha rafforzato la ripartizione tra le loro funzioni a vantaggio della corretta gestione delle controversie nella pratica, dell'equilibrio tra la protezione e l'uso delle informazioni personali e della promozione dello sviluppo economico nell'era digitale. Poiché il diritto alla riservatezza è strettamente connesso alla tutela della dignità umana, qualora si considerassero tutte le informazioni personali come rientranti nell'ambito tutelato dalla riservatezza, dovrebbero al contempo ignorarsi le esigenze della comunicazione interpersonale e le attuali pratiche commerciali, nonché il valore apportato dalla condivisione delle informazioni medesime.

7. Lo specifico ambito delle informazioni personali sensibili

Le informazioni personali sensibili sono definite in termini di informazioni personali che, una volta diffuse o utilizzate illegalmente, possono causare una violazione della dignità personale delle persone fisiche o metterne in pericolo la sicurezza personale e patrimoniale. Se ne menzionano quali esempi, l'art. 6 della Convenzione 108 del Consiglio d'Europa[57]:

«I dati a carattere personale che rivelano l'origine razziale, le opinioni politiche, le convinzioni religiose o altre convinzioni, nonché i dati a carattere personale relati-

[57] La Convenzione di Strasburgo del 1981, o anche Convenzione 108 del Consiglio d'Europa è uno dei più importanti strumenti legali per la protezione delle persone rispetto al trattamento automatizzato dei dati personali e l'unico giuridicamente vincolante a livello internazionale in tale materia, potendo ad essa aderire anche Stati non membri del Consiglio d'Europa. La Convenzione 108 scaturisce dall'esigenza di tutela per le persone a seguito del proliferare di tecnologie dell'informazione e comunicazione a partire dagli anni '60. Riguardo all'ambito, si applica a tutti i trattamenti di dati personali effettuati sia nel settore privato che nel settore pubblico, pertanto anche ai trattamenti compiuti da polizia e autorità giudiziaria. La Convenzione ha la finalità di proteggere gli individui da abusi e regolamentare i flussi transnazionali di dati, e trae diretta vocazione dall'articolo 8 della Convenzione europea dei diritti dell'uomo:«Scopo della presente Convenzione è quello di garantire, sul territorio di ciascuna Parte, ad ogni persona fisica, quali che siano la sua nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano («protezione dei dati»)».

> vi alla salute o alla vita sessuale, non possono essere elaborati automaticamente a meno che il diritto interno preveda delle garanzie appropriate. Lo stesso vale per i dati a carattere personale relativi a condanne penali»;

l'art. 9 del GDPR:

> «È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona»;

la Legge del Brasile sulla protezione dei dati personali (LGPD, *Lei General de Proteção de Dados*) in vigore dal 18 settembre 2020 che può essere considerata la risposta del Brasile al GDPR con cui ha diverse somiglianze e si occupa dei dati sensibili all'art. 5, c. 2:

> «Ai fini della presente legge si considerano […] dati personali sensibili: i dati personali relativi all'origine razziale o etnica, alle convinzioni religiose, alle opinioni politiche, all'appartenenza sindacale o ad un'organizzazione religiosa, filosofica o politica, i dati relativi alla salute o alla vita sessuale, i dati genetici o biometrici, quando collegati a una persona fisica»;

infine, la Legge del Giappone sulla protezione dei dati personali (*Act on the Protection of Personal Information*) promulgata nel 2003 e da ultimo emendata il 1° aprile 2022, all'art. 2, c. 3, dispone:

> «Ai sensi della presente legge, per "dati personali sensibili" si intendono i dati personali relativi alla razza, al credo, allo stato sociale, all'anamnesi, ai precedenti penali, al fatto di aver subito un danno da reato, o ad altri elementi identificativi o equivalenti prescritti da un'ordinanza del Consiglio dei ministri che richiedono particolare attenzione per non causare ingiuste discriminazioni, pregiudizi o altri svantaggi a tale persona[58]».

Gli Stati Uniti, diversamente, non hanno una definizione unica di dati personali sensibili a livello legislativo federale, ma hanno previsto, in distinti testi normativi, disposizioni speciali per alcune specifiche categorie di essi: si pensi ad esempio agli standard relativi alla riservatezza delle informazioni sanitarie formulati dal Dipartimento della salute e dei servizi umani degli Stati Uniti (*United States Department of Health and Human Services*)[59].

[58] この法律において「要配慮個人情報」とは、本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報をいう, disponibile in Japanese Law translation.

[59] Da tale approccio si è di recente distaccato lo Stato della California avviandosi ad introdurre una normativa unitaria della materia.

Sebbene il Cod. civ. cin. non adotti direttamente il concetto di informazioni personali sensibili un riferimento è presente nell'art. 1034, c. 3[60]:

> «[…] Le informazioni personali sono quelle registrate elettronicamente o in altri modi che possano essere utilizzati, da soli o in combinazione con altri, per identificare una persona fisica, inclusi nome, data di nascita, numero di carta di identità, in- formazioni biometriche, indirizzo di residenza, numero di telefono, indirizzo *e-mail*, informazioni sanitarie, ubicazione e simili della persona. Alle informazioni personali sensibili si applicano le disposizioni sul diritto alla riservatezza o, in mancanza, si applicano quelle sulla protezione dei dati personali».

Inoltre, l'art. 1035, c. 1, del Cod. civ. cin. stabilisce che il trattamento delle informazioni personali è soggetto al consenso della persona fisica o del suo tutore, il che rappresenta una protezione speciale dei dati dei minori, pertanto, distinguendo tra diversi tipi di informazioni personali e delegando alla Legge sulla protezione delle informazioni personali ogni maggior dettaglio.
Di ausilio per la maggior comprensione di quanto si sta indagando l'art. 2 delle Disposizioni su diverse questioni riguardanti l'applicazione della legge nelle cause civili relative al trattamento delle informazioni personali mediante la tecnologia di riconoscimento facciale (审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定) pubblicate dalla Corte Suprema del Popolo il 1° agosto 2021 che considera qualsiasi violazione delle norme sul trattamento delle informazioni personali come una violazione dei diritti della personalità e dei legittimi interessi degli individui nell'ambito del diritto civile. Di conseguenza, nella prassi giudiziaria hanno iniziato a comparire espressioni quali «diritto di controllare le informazioni personali» nella prospettiva dei diritti della personalità e «contenuto principale del diritto alle informazioni personali quale ambito di dominio e oggetto di decisione autonoma del suo titolare».
L'art. 28 della Legge definisce le informazioni personali sensibili:

> «Le informazioni personali sensibili si riferiscono alle informazioni che potrebbero ledere la dignità personale di qualsiasi persona fisica, o danneggiare la sua sicurezza personale o patrimoniale una volta divulgate o utilizzate illecitamente, comprese le informazioni quali l'identificazione biometrica, il credo religioso, l'identità specifica, lo stato di salute, i conti finanziari, la posizione e le tracce, nonché i dati personali dei minori di 14 anni».

Secondo il metodo della sintesi e della enumerazione, da un lato la disposizione ne definisce chiaramente la nozione, dall'altro pone il parametro di valutazione sul quale identificarne nella pratica i diversi tipi: quello cioè della facilità con cui la loro violazione può danneggiare la dignità personale delle persone fisiche o metterne in pericolo la sicurezza personale e patrimoniale. Il parametro fornisce una base fondamentale per identificare con precisione le informazioni personali sensibili nella pratica; al medesimo tempo, la definizione generalizzata è sufficientemente flessibile e aperta ad accogliere

[60] V. art. 76, c. 5, della Legge sulla sicurezza informatica della Repubblica Popolare Cinese.

tipi di informazioni emergenti ed in rapida evoluzione nell'era digitale in connessione alle esigenze dello sviluppo sociale. L'art. 28 vi include i dati biometrici, le credenze religiose, le identità specifiche, l'assistenza medica e sanitaria, i conti finanziari, gli spostamenti e altre informazioni, nonché le informazioni personali dei minori di 14 anni.
La maggior parte degli ordinamenti adotta il metodo dell'enumerazione delle informazioni personali sensibili, senza specificarne le caratteristiche[61]. La Legge sulla protezione delle informazioni personali, diversamente, ne prevede gli elementi fondamentali per la successiva identificazione, fondando il proprio criterio di qualificazione nella eventuale incidenza sulla dignità personale e la sicurezza della vita e della proprietà, determinando un danno alle persone.
Le informazioni personali dei minori di 14 anni sono incluse tra quelle sensibili[62].
Secondo l'art. 31 della Legge sulla protezione dei dati personali:

> «Per operare il trattamento dei dati personali di un minore di età inferiore ai 14 anni, il responsabile del trattamento deve ottenere il consenso dei genitori o di altri tutori del minore.
> Per operare il trattamento dei dati personali dei minori di età inferiore ai 14 anni, il responsabile del trattamento predisporrà regole specifiche per il trattamento dei dati personali».

il trattamento dei dati personali dei minori richiede il consenso dei loro tutori. Quando tratta le informazioni personali di un minore, il responsabile del trattamento dei dati personali deve verificare se la persona che processa i dati è un minore e se la persona che dà il consenso è il tutore del minore. In teoria, questo è il cosiddetto "obbligo di doppia verifica".
Nel valutare le informazioni personali sensibili occorre, innanzitutto, valutarle sia in base ai parametri legali, sia al contesto. Riguardo ai parametri legali questi devono essere determinati in combinazione con le disposizioni di altra normativa, si pensi, ad esempio all'art. 14 del Regolamento sull'amministrazione del settore creditizio che include il gruppo sanguigno nell'ambito dei dati personali sensibili; oppure all' Interpretazione giudiziaria del riconoscimento facciale che protegge le informazioni del volto quali dati personali sensibili.
La dottrina cinese evidenzia come il contesto debba aiutare a qualificare le informazioni come sensibili o meno[63]. Motivo per cui si dovrebbe adottare tale impostazione è che i cambiamenti sociali e la loro portata incerta impongono questo approccio, confermato anche dall'utilizzo della formulazione aperta dell'art. 28 in cui l'elencazione delle informazioni personali sensibili non è limitata a «l'identificazione biometrica, il credo religioso, l'identità specifica, lo stato di salute, i conti finanziari, agli spostamenti». In futuro, con l'ulteriore sviluppo della società, ci saranno nuovi tipi di informazioni per-

[61] Art. 6 del GDPR, l'art. 5 della Legge generale sulla protezione dei dati del Brasile, l'art. 2 della Legge sulla protezione dei dati personali del Giappone, l'art. 23 della Legge coreana sulla protezione dei dati personali.

[62] Art. 9 del GDPR.

[63] H. Nissenbaum, *Privacy as Contextual Integrity* , in *Washington Law Review*, 2004, 119 ss.

sonali sensibili, quale risultato inevitabile dello sviluppo della scienza e della tecnologia che i giudici saranno chiamati a valutare.
A definire l'ambito di trattamento delle informazioni sensibili interviene l'art. 28, c. 2:

> «Solo per specifiche finalità e sufficienti necessità, e qualora siano state adottate rigorose misure di protezione, il responsabile del trattamento può trattare dati sensibili».

in cui sono fissate condizioni dettagliate riguardo al trattamento dei dati sensibili: in primo luogo, uno scopo specifico; in secondo luogo, una necessità suficiente; in terzo luogo, l'adozione di misure di protezione rigorose. Il principale riferimento tra questi elementi sembra essere la finalità specifica: solo in presenza di una finalità specifica le informazioni personali sensibili possono essere trattate secondo la legge. Tuttavia quello di "specifica finalità" è un concetto incerto e la sua semantica ha un ampio spazio interpretativo per cui è necessario definire ulteriormente ed effettuare una ulteriore analisi. Di aiuto è l'art. 6 della Legge che fissa il principio della limitazione delle finalità del trattamento, vale a dire che qualsiasi trattamento delle informazioni personali deve avere una finalità chiara e ragionevole e il criterio si applica anche alle informazioni sensibili. Tuttavia, vi sono alcune differenze tra le due disposizioni, e lo standard della finalità specifica è più elevato di quello della finalità chiara e ragionevole. Emerge quindi che: i) la finalità specifica nel trattamento delle informazioni personali sensibili debba essere intesa quale finalità specifica e chiara, non una finalità generale; ii) la finalità specifica può essere quella esplicitamente fissata dal legislatore e dalle forze dell'ordine; iii) in base alla finalità fissata dal legislatore, il responsabile del trattamento delle informazioni può trattare le informazioni sensibili in conformità alla legge; iv) il giudizio sulla specificità della finalità non può essere generalizzato. Nel giudicare una finalità specifica, occorre considerare anche l'occupazione e la natura delle attività del responsabile del trattamento e se il trattamento dei dati personali sensibili sia finalizzato a fronteggiare emergenze ed a realizzare interessi pubblici. Naturalmente, anche in queste circostanze, il responsabile del trattamento deve trattare le informazioni sensibili dell'individuo entro i limiti necessari, configurandosi diversamente una condotta illecita, impostazione adottata anche dall' art. 9 del GDPR.
Un ultimo rilievo riguarda il consenso separato. La differenza tra il trattamento delle informazioni personali sensibili e quello delle informazioni personali generali risiede nel fatto che, nel caso in cui si risponda a una finalità specifica, è necessario ottenere anche il consenso e l'autorizzazione individuale dell'interessato, mentre non è previsto il consenso tramite autorizzazione implicita. Le norme generali sul trattamento delle informazioni personali si basano sul consenso dell'interessato, mentre il trattamento delle informazioni personali sensibili prevede che «solo in presenza di uno scopo specifico e di una necessità sufficiente e con l'adozione di rigorose misure di protezione, il responsabile del trattamento dei dati personali possa trattare le informazioni personali sensibili». Inoltre, la Legge sulla protezione delle informazioni personali ha introdotto disposizioni più severe sul consenso e sulla divulgazione delle informazioni personali sensibili, richiedendo che il trattamento di queste sia conforme alle norme separate sul

consenso. Le ragioni di questa disposizione sono che, da un lato, i requisiti di obbligo per i responsabili del trattamento delle informazioni sono stati ulteriormente innalzati e la raccolta di informazioni personali sensibili è stata rigorosamente limitata mediante un'autorizzazione separata per prevenire la violazione delle informazioni personali sensibili. Dall'altro, per l'interessato, la modalità di autorizzazione individuale può anche renderlo consapevole dei rischi causati dall'autorizzazione, in modo da agire con cautela e rafforzare la consapevolezza della tutela dei diritti.
L'art. 29 della Legge migliora i requisiti del principio del consenso informato nella protezione delle informazioni personali. Secondo questa disposizione, il consenso per il trattamento delle informazioni personali sensibili deve essere individuale secondo questi tre aspetti: il consenso deve essere separato, pertanto è vietata una autorizzazione generalizzata; la regola del consenso separato richiede che il responsabile del trattamento abbia un chiaro obbligo di informazione; la regola del consenso separato dovrebbe implementare la regola della restrizione del rifiuto di fornire servizi.

8. Privacy con caratteristiche cinesi

Lo studio della materia, i principi, i requisiti ed i contenuti delle disposizioni della normativa della Repubblica Popolare Cinese mostrano come si sia attinto a modelli preesistenti. Tuttavia, alcuni profili della Legge, tra cui quello della localizzazione dei dati, sono tra i caratteri maggiormente distintivi della impostazione adottata dalla Cina, ambito in cui la normativa mostra la maggior parte della propria specificità. L'approccio del modello degli Stati Uniti, tra i più forti oppositori alla localizzazione dei dati, percepita come una barriera commerciale, risulta essere il più semplice, in quanto non esistono requisiti specifici per il trasferimento di informazioni personali ad un Paese terzo. L'approccio del modello dell'Unione europea seppur maggiormente restrittivo, non prevede l'obbligo di localizzazione dei dati, i trasferimenti transfrontalieri di dati potendo avvenire, infatti, solo qualora rispettino il livello di protezione stabilito dal GDPR, quindi, verso Paesi terzi con un livello di protezione dei dati che la Commissione europea riconosce come equivalente a quello dell'Unione europea, o utilizzando garanzie appropriate quali clausole contrattuali standard o attraverso le *binding corporate rules*. La Cina, attraverso una lettura di insieme della normativa, ma in modo particolare degli artt. 1 e 37 della Legge sulla sicurezza della rete imposta il proprio modello:

> «La presente legge è elaborata al fine di garantire la sicurezza informatica, di proteggere la sovranità del ciberspazio, la sicurezza nazionale e l'interesse pubblico, di salvaguardare i legittimi diritti ed interessi dei cittadini, delle persone giuridiche e delle altre organizzazioni e di promuovere un sano sviluppo dell'informatizzazione dell'economia e della società».
> «Gli operatori di infrastrutture di informazioni essenziali che raccolgono e generano o producono informazioni personali e dati sensibili all'interno della Repubblica Popolare Cinese devono assicurarne l'archiviazione e la memorizzazione all'interno della Repubblica Popolare Cinese. Se per concrete esigenze commerciali, è

> necessario fornirli o trasmetterli al di fuori dei confini nazionali è richiesta un'opportuna valutazione sulla sicurezza dell'operazione, effettuata secondo le modalità formulate congiuntamente dall' Amministrazione per la sicurezza del ciberspazio e dal dipartimento competente del Consiglio degli Affari di Stato. Nel caso leggi o regolamenti amministrativi dovessero prescrivere diversamente, si applicheranno questi ultimi».

L'impostazione prescelta non è presente né nella normativa della Unione europea né in quella degli Stati Uniti ma diversamente in quella Russa – riferimento strico del legislatore cinese in particolare in alcune fasi di costruzione dell'ordinamento giuridico - specificatamente nella Legge federale Russa n. 242 FZ, in vigore dal 1° settembre 2015, successivamente emendata il 2 dicembre 2019 ed in vigore dal 13 dicembre 2019. La posizione proclamata dal legislatore cinese sulla localizzazione dei dati è che essa protegge la privacy delle persone ma al medesimo tempo la propria sovranità, lo sviluppo economico della Cina e riduce al minimo la sua esposizione a fattori esterni. Tratto saliente è, tuttavia, la disuguaglianza tra il rafforzamento della protezione delle informazioni personali rispetto ad azioni di entità private e il contestuale e parallelo aumento dell'intromissione da parte del governo. Mentre il diritto alla riservatezza e alla tutela delle informazioni personali è stato oggetto di una evoluzione a favore dei singoli e dei consumatori, criticità e fragilità persistono nel rapporto cittadino - governo[64]: la normativa tutela sempre più i diritti delle persone contro le entità private che detengono i loro dati e ne garantisce un maggiore controllo ma i benefici derivanti da questi progressivi miglioramenti sono attenuati dall'accresciuto accesso del governo ai dati dei singoli, impostazione confermata dall'art. 28 della Legge sulla sicurezza della rete, art. 28:

> «Gli operatori di rete devono fornire supporto tecnico e assistenza alle autorità di pubblica sicurezza e alle autorità di sicurezza nazionale che, in conformità della legge, operano a salvaguardia della sicurezza della nazione e che indagano sulle attività criminali».

La *ratio* alla base della normativa cinese è diversa da quella dei due modelli dell'Unione europea e degli Stati Uniti: la prima obbligata ad adottare un elevato livello di protezione dei dati, tutela garantita quale diritto fondamentale sia verso entità private sia verso il governo; negli Stati Uniti la protezione della privacy, diversamente, è concepita prima di tutto, quale protezione verso le attività governative, verso il potere dello Stato, ancor prima che verso le entità private. Quello che emerge è il diverso concepimento in Cina dei diritti dei singoli in cui il riconoscimento di questi ultimi è comunque superato dall'interesse superiore dello Stato. La Cina, anche in questo settore del diritto, ha varato una propria normativa con "caratteristiche cinesi". I macro poli che hanno orientato il legislatore sono, come di consueto i due sistemi di Civil law e Common law,

[64] Sul diritto amministrativo cinese di interesse le relazioni di studiosi cinesi contenute in E. Toti, *Leggi tradotte della Repubblica Popolare Cinese, XIII, Legge sul processo amministrativo, Legge sulle sanzioni amministrative, Legge sul riesame amministrativo*, Milano, 2021.

nello specifico ambito rappresentati da Europa e Stati Uniti da cui si è attinto, sempre in modo selettivo e ragionato, al fine di varare un proprio modello in grado di mantenere bilanciati i diversi interessi coinvolti in questo complesso macrosistema.