RIVISTA DI
DIRITTI COMPARATI

La legge cinese sulla protezione delle informazioni personali: un GDPR con caratteristiche cinesi?*

*Davide Clementi***

SOMMARIO: 1. Introduzione – 2. Cenni sul riconoscimento giuridico del diritto alla privacy nel diritto cinese – 3. Sistema "duale" di tutela della privacy fra codice civile e PIPL – 4. Ambito di applicazione e problematiche definitorie – 5. Fra consenso (granulare) e dati sensibili: i diritti degli interessati dal trattamento – 6. Obblighi e responsabilità dei *data controller* cinesi – 7. Il cross-border delle informazioni personali: gestori stranieri e grandi gestori alla prova della tutela dei dati – 8. Prime considerazioni conclusive: tutela del singolo nel quadro delle "caratteristiche cinesi"?

1. Introduzione

A partire dall'ottobre del 2020 il governo cinese ha avviato una intensa attività di regolamentazione e controllo del settore privato, in special modo di quelle industrie tecnologiche ad alto valore aggiunto (*hi tech*)[1] che rappresentano il fiore all'occhiello della moderna struttura economica della Repubblica

* Il contributo è stato sottoposto, in conformità al *Regolamento della Rivista,* a *double-blind peer review.*

** Il saggio è realizzato nell'ambito del dottorato di ricerca programma PON "Ricerca e innovazione" 2014-2020 con riferimento all'Azione IV.5 "Dottorati su tematiche green", progetto in Diritto privato comparato – IUS02 dal titolo "L'implementazione delle Innovation technologies nell'industria creativa e culturale italiana alla prova degli ordinamenti e dei mercati dei paesi asiatici".

[1] Questa ondata regolatoria è stata innescata, almeno a livello temporale, da un discorso pronunciato da Jack Ma, fondatore del gruppo Alibaba, al Summit finanziario del Bund di Shanghai. Ma, che il 1° ottobre dello stesso anno si era dimesso dal consiglio di amministrazione del gruppo da lui fondato, critica in quell'occasione il sistema di supervisione dello Stato cinese, molto buono nella gestione *("management")* ma "gravemente carente" per quanto concerne il controllo, rimasto sostanzialmente ai livelli qualitativi di una "stazione dei treni" quando si sta in realtà governando – metaforicamente – un aeroporto. Cfr. Jack Ma, *Jack Ma's Bund Finance Summit Speech*, tradotto da Kevin Xu, disponibile al sito web: https://interconnected.blog/jack-ma-bund-finance-summit-speech/.

popolare. Nell'ambito di quello che è stato definito "Red New Deal"[2], lo stop all'offerta pubblica iniziale di Ant[3], controllata del gruppo Alibaba, ha simboleggiato l'inizio di una stretta – anche giuridica – a settori in rapidissima espansione, come quello del commercio elettronico[4], dei social network, della *gig economy*, etc.

In questa ottica di progressivo rafforzamento della cyber-sovranità, vista in Cina come "naturale estensione della sovranità nazionale nell'ambiente cibernetico"[5], si posiziona a pieno titolo l'approvazione in via definitiva della

[2] Con tale espressione si vuole sottolineare lo sforzo governativo di "ridurre la disuguaglianza e rendere migliore la vita delle persone normali" attraverso "azioni che hanno una logica comunista vecchio stile, ma anche perché le aziende che intralciano il governo perderanno sangue" v. Kaiser Kuo et al., *China's Red New Deal: Tracking all the different crackdowns on companies going on right now*, disponibile al sito web: https://supchina.com/2021/09/09/chinas-red-new-deal-a-guide-to-all-the-different-crackdowns-on-companies-going-on-right-now/.

[3] Il giorno prima della sospensione, Jack Ma era stato convocato dalle autorità della Banca del popolo cinese, la banca centrale della Repubblica popolare cinese che, oltre a esercitare la politica monetaria, gode di ampi poteri di ispezione e controllo degli strumenti e mercati finanziari. In base a quanto riferito in una nota del gruppo Ant, la discussione è consistita in uno scambio di visioni sul tema della "salute e [del]la stabilità del settore finanziario". Cfr. Jing Yang, *Chinese Regulators Summon Ant Leaders Ahead of Gigantic IPO*, consultabile al sito internet https://www.wsj.com/articles/chinese-regulators-summon-ant-leaders-amid-record-ipo-11604327306?mod=article_inline.

[4] Allo stop dell'offerta pubblica iniziale di Ant è seguito l'intervento dell'autorità amministrativa di controllo del mercato – l'Amministrazione Statale per la Regolazione del Mercato ("SAMR") – che con un breve comunicato sul proprio sito web [http://www.samr.gov.cn/xw/zj/202012/t20201224_324638.html] ha annunciato l'apertura di indagini per condotte monopolistiche proprio contro il gruppo Alibaba, accusato di praticare il c.d. *"er xuan yi"* ("fra due, scegline (solo) uno"), ossia quella strategia di business che obbliga i consumatori o le imprese (specie le piccole e medie imprese) a scegliere esclusivamente una e una sola piattaforma di commercio elettronico con i servizi a essa annessi e non quelli dei concorrenti. L'indagine della SAMR si è conclusa con l'adozione della Decisione n. 28 del 10 aprile 2021: in questo provvedimento amministrativo sanzionatorio l'autorità regolatoria del mercato cinese, oltre a comminare al gruppo Alibaba una multa da circa 2 miliardi e 315 milioni di euro, corrispondenti al 4% delle vendite nel 2019 sul territorio cinese del gruppo, ha allegato una "lettera di orientamento amministrativo", nella quale ha altresì ordinato che agli operatori (*vendors*) nelle piattaforme e-commerce di Alibaba non sia impedito di operare in ogni modo anche su altre piattaforme. Il provvedimento è in controtendenza rispetto a pronunce giurisprudenziali, anche di rilievo costituzionale [cfr. *Qihoo 360 v. Tencent*, dove la Corte Suprema del Popolo aveva riconosciuto che la pratica del *"er xuan yi"* non costituisse abuso della posizione dominante. L'analisi del caso è disponibile in China Institute Of Applied Jurisprudence, *Selected Cases from the Supreme People's Court of the People's Republic of China, Volume 1*, Pechino (PRC) e Singapore, 2020, pp. 325-341].

[5] Il concetto di "cyber-sovranità" (网络主权) appare sul Quotidiano del Popolo, organo ufficiale del Partito comunista cinese, dove viene indicato come una "questione inevitabile per l'affermazione stessa della sovranità nazionale nell'era di Internet" [cfr. Wang Yuan, Xin Qiang,

Legge sulla protezione delle informazioni personali (o "PIPL"), adottata il 20 agosto 2021 dal Comitato permanente del Congresso nazionale del popolo in terza lettura e promulgata lo stesso giorno con ordine del Presidente della Repubblica n. 91[6] ed entrata in vigore il 1° novembre 2021. La legge, composta da 74 articoli, si pone l'obiettivo di proteggere i diritti e gli interessi legati alle informazioni personali, standardizzandone le attività di trattamento e promuovendo un uso razionale degli stessi[7].

Nelle seguenti note s'intende ripercorrere brevemente lo sviluppo della tutela giuridica della privacy all'interno del diritto cinese, proponendo poi una analisi comparata fra la regolamentazione della Repubblica popolare cinese in materia di protezione delle informazioni personali e la disciplina europea presa a modello dal legislatore cinese.

2. Cenni sul riconoscimento giuridico del diritto alla privacy nel diritto cinese

Nonostante sia invalsa l'idea che la cultura e la società cinese, specie anticamente, non solo mal sopportassero l'idea di riservatezza[8], ma che non fosse

La sovranità di Internet, una questione inevitabile, in *Quotidiano del Popolo*, 23° ed., 23/4/2014]. Va segnalata la pubblicazione sul sito internet ufficiale della Cyberspace Administration of China di un documento dal titolo "Cyber-sovranità: Teoria e pratica (versione 2.0)", scritto in collaborazione con l'Università di Wuhan, il China Institute of Modern International Relations e l'Accademia delle scienze sociali di Shanghai in cui, oltre a ribadire la definizione suindicata di cyber-sovranità, ne vengono delineate caratteristiche e principi: centrale nella presente analisi è la giurisdizione dello stato sovrano nello spazio digitale, che ricomprende anche "i dati e le informazioni di rete all'interno dei propri confini in conformità con la legge", verso cui gli Stati hanno dei "doveri di prudenza e di prevenzione" onde evitare che Paesi terzi mettano a repentaglio la sicurezza e gli interessi nazionali [cfr. UNIVERSITÀ DI WUHAN ET AL., *Cyber Sovranità: Teoria e Pratica (Versione 2.0)*, pubblicato il 25/11/2020 sul sito web della Cyberspace Administration of China, accessibile al link http://www.cac.gov.cn/2020-11/25/c_1607869924931855.htm].

[6] Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa (中华人民共和国个人信息保护法) [Legge sulla protezione delle informazioni personali della Repubblica Popolare Cinese] (adottata alla 30° riunione del Comitato permanente del 13° Congresso nazionale del popolo e promulgata con ordine del Presidente della Repubblica n. 91/2021). In avanti si adotterà per ragioni di sinteticità l'acronimo inglese "PIPL".

[7] Art. 1, PIPL.

[8] La civiltà cinese, tuttora profondamente influenzata dai principi del confucianesimo e del taoismo, viene vista da parte della letteratura come mancante di un "concetto perfettamente parallelo" a quello di privacy nelle forme che assume nel pensiero occidentale. Per riferimenti al pensiero cinese antico sulla riservatezza cfr. C.B. Whitman, *Privacy in Confucian and Taoist*

contenuta neppure nel vocabolario mandarino prima di un *legal transplant* da Occidente[9], la Repubblica popolare, con l'avvicinarsi agli standard delle moderne economie di mercato e con l'ingresso nell'Organizzazione mondiale del commercio, ha accelerato la propria marcia sulla strada della protezione giuridica delle informazioni personali sia nel mondo fisico tradizionale che nel cyberspazio.

La Legge sulla protezione delle informazioni personali non giunge inaspettata. Se già nella Costituzione del 1982 avevano trovato espressione i più

Thought, in *Individualism and Holism: Studies in Confucian and Taoist Values*, 1980, p. 85-100, dove si segnala che a un primo sguardo confucianesimo e taoismo dei primordi avessero concetti avvicinabili alla moderna privacy, come l'amicizia, il rispetto dei legami familiari, la non-interferenza, la crescita personale, l'abbandono della società, l'eremitaggio, l'introspezione. In realtà, una analisi più accurata di queste filosofie suggerisce che i suindicati concetti fossero assimilabili a dispositivi politici di controllo e persuasione in favore della onnipresente società per i confuciani, e della ricerca personale non gerarchizzata di ciò che era comune agli uomini per i taoisti. Contro tale ricostruzione cfr. B.S. McDougall, *Privacy in Modern China*, in *History Compass*, vol. 2(1), 2004, p. 1-8, ove si contesta l'idea, ampiamente diffusa in Occidente già negli anni Trenta, della assenza totale della privacy in Cina. Al contrario, l'a. afferma non solo che la privacy nella Cina tradizionale fosse presente primariamente nell'"esistenza di reami privati per individui, coppie, e piccoli gruppi non familiari", ma che, nonostante la contrapposizione confuciana fra 私 (*si*, privato) e 共 (*gong*, pubblico), la Cina sia arrivata autonomamente al conio di una parola, 隐私 (*yinsi*), per definire ciò che in inglese la civiltà occidentale definisce con "privacy". Si veda per una comparazione culturale fra individualismo e collettivismo G. Hofstede et al., *Cultures and Organizations: software of the Mind: intercultural Cooperation and Its Importance for Survival*, 2010, p. 125 ss., ma anche Xiaogang Chen – Yuhui Zhang, *The construct of information privacy concerns in the Chinese cultural setting*, in *Nankai Business Review International*, vol. 12(1) [anno?], p. 42-55, dove si accetta l'idea che nel complesso la società cinese, a differenza di quella occidentale, sia una società altamente collettivistica, ove l'individuo è fortemente connotato dalle sue affiliazioni di gruppo e la sua unicità-personalità abbia una priorità inferiore rispetto alle norme sociali e ai ruoli di gruppo.

[9] Cfr. E. Poon Wai Yee, *The Cultural Transfer in Legal Translation*, in *International Journal for the Semiotics of Law*, vol. 18, 2005, p. 307-323, in cui si compie un'analisi semiotica e comparata della traduzione giuridica. L'a. giunge alla conclusione che "nessuna cultura o lingua sia superiore alle altre nel descrivere l'universo" e che, durante il processo traduttivo, la lingua cinese deve per forza di cose "cambiare a volte il suo lessico e la struttura grammaticale a causa dell'influenza dell'inglese legale, senza perciò perdere la sua tipicità". Sul tema più specifico dei trapianti linguistico-giuridici da Occidente verso la Cina è ottimamente affrontato in M. Timoteo, *Il diritto nelle parole: aspetti linguistici del diritto cinese contemporaneo*, in E. Calzolaio – R. Torino – L. Vagni (a cura di), *Liber Amicorum Luigi Moccia*, Roma, 2021, p. 643-655, ove l'A. segnala come, a seguito anche delle conquiste imperialiste occidentali nel fu Impero del Centro, arrivarono in Cina "tassonomie, costrutti normativi, concetti, termini dei diritti occidentali, del tutto estranei alla storia locale [...] creando un codice espressivo destinato a sostenere il processo di modernizzazione".

elementari corollari del più ampio diritto alla privacy[10], anche norme di livello primario precedenti alla PIPL cercavano di fornire una prima ma limitata tutela al bene della riservatezza. Si veda la Legge sul servizio postale, promulgata nel 1986 ed emendata l'ultima volta nel 2015, che già nel testo originario si poneva "nell'ottica di proteggere la libertà e la confidenzialità della corrispondenza"[11]. Poco dopo, sulla base dei "Principi generali del diritto civile" del 1988, la Corte Suprema del popolo ha fornito una Interpretazione legale giuridicamente vincolante per le corti d'ogni livello ove si esplicitava che l'esposizione di segreti di una persona al pubblico dovesse essere considerata come violazione del diritto alla reputazione e pertanto perseguita in sede civile[12]. Proprio le disposizioni sulla riservatezza della corrispondenza hanno fornito in combinazione ad altre la base giuridica per pronunce su casi controversi e dall'ampia eco nel discorso giuridico e nell'opinione pubblica ove si è fornita tutela anche al diritto alla privacy[13].

[10] Varie disposizioni della Costituzione del 1982, giunta al suo quinto emendamento nel 2018, proteggono in vario modo la riservatezza dei cittadini: l'art. 38 stabilisce che la "dignità personale dei cittadini della Repubblica popolare cinese è inviolabile" contro ogni forma di "insulto, diffamazione, falsa accusa o macchinazione, con ogni mezzo condotti", mentre l'art. 40 tutela esplicitamente e garantisce – almeno teoricamente – il diritto alla riservatezza nella corrispondenza e il dovere da parte di ogni cittadino od organizzazione di inviolabilità, salva per gli organi statali di pubblica sicurezza la possibilità di investigare illeciti penalmente rilevanti e di censurare la corrispondenza in conformità alla legge.

[11] Zhongua Renmin Gongheguo You Zheng Fa (**中华人民共和国邮政法**) [Legge sul servizio postale della Repubblica popolare cinese] (adottata alla 18° riunione del Comitato permanente del 6° Congresso nazionale del popolo e promulgata con ordine del Presidente della Repubblica n. 47/1986, 3° emendamento in vigore dal 24 aprile 2015), art. 1, che utilizza la parola "segretezza" (*mimi* **秘密**), di frequente resa in inglese e in italiano come privacy. Già l'art. 4 nella versione del 1986 (oggi art. 3) si forniva tutela a favore della "libertà e della segretezza della corrispondenza" contro ogni organizzazione o individuo che la violasse "per ogni ragione", salvo i casi in accordo con le procedure legali da parte della forza pubblica.

[12] Zuigao Renmin Fayuan Guanyu Guanche Zhixing "Zhonghua Renmin Gongheguo Min Fa Tongze" Ruogan Wenti de Yijian (Shixing) (**最高人民法院关于**贯彻执行《**中华人民共和国民法通则**》**若干**问题**的意**见 (试**行**)) (**法**[办]发[1988]6**号** [Pareri n. 6/1988 della Corte Suprema del Popolo su diversi problemi concernenti l'applicazione dei Principi generali del diritto civile (per l'attuazione del processo)] (adottato il 26 gennaio 1988 e in vigore dal 4 aprile 1988), art. 140 [trad. inglese a cura di W. Gray – H.R. Zheng, in *Law& Contemp. Probs.*, vol.52, 1989. p. 59-87].

[13] Qui ci si riferisce in particolare al caso-guida *Zhongmao Sungari International Auction Co., Ltd., contro Yang Jikang (nome d'arte Yang Jiang), et al.* < (2014)**高民终字第**1152**号** >, in cui la nota scrittrice Yang Jiang (al secolo Yang Jikang) lamentava la lesione dei diritti di copyright e alla privacy subita da lei, dal marito e dalla figlia – entrambi deceduti – per via della riproduzione e diffusione della corrispondenza privata fra di essi e l'amico di famiglia Li Guoqiang, che aveva consegnato i manoscritti alla casa d'aste Zhongmao Shengjia, la quale aveva provveduto a interrompere l'asta a seguito di istanza pregiudiziale della parte attrice. La medesima parte attrice

A distanza di un secolo dal seminale articolo di Warren e Brandeis sul diritto alla privacy[14], anche la dottrina cinese ha cominciato a individuare nel diritto alla privacy un certo grado di autonomia, distinguendolo e allo stesso tempo ricomprendendolo fra i diritti di personalità[15]. Tale incompiuta autonomia rilevata dai giuristi cinesi è stata infine sanata con la promulgazione della Legge sulla responsabilità civile del 2009, ove il diritto alla privacy trova espresso riconoscimento quale diritto civile, autonomo e distinto dagli altri[16].

3. Sistema "duale" di tutela della privacy fra codice civile e PIPL

Dalla legge sulla responsabilità civile in avanti la Cina ha preferito adottare un sistema unitario (o "statunitense") di privacy, proteggendo congiuntamente sotto il *genus* della tutela della riservatezza la *species* della protezione delle informazioni e dei dati personali[17]. Tale sistema monistico di tutela è entrato in crisi ovvero ha subìto uno sdoppiamento con l'emersione e la diffusione delle tecnologie dell'informazione. La Cina è infatti rapidamente diventata una delle superpotenze globali nell'uso di Internet e delle tecnologie digitali e ciò ha reso

ha comunque agito giudizialmente per chiedere il risarcimento del danno per la perdita economica causata, la violazione del copyright e i "danni mentali" cagionati. L'Alta Corte del popolo di Pechino, pur riducendo la quantificazione del danno, ha accolto le ragioni dell'attore, condannando congiuntamente la casa d'aste e Li Guoqiang e confermando la pronuncia del giudice di prime cure. La sentenza, definitiva e passata in giudicato, è disponibile al sito web http://ipr.cupl.edu.cn/info/1740/11067.htm.

[14] S. D. Warren – L.D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, 1890, vol. 4(5), p. 193-220, che segna appunto la comparsa ufficiale nella moderna cultura giuridica *latu sensu* occidentale (e *stricto sensu* di *common law*) del diritto alla privacy. Due anni dopo il caso *Pavesich v. New England Life Insurance Co. [1905] 122 G.A.* 190 aprirà l'epoca della tutela giurisdizionale del diritto alla privacy,

[15] Si accenna qui a Tong Ruo et al., Zhongguo Minfa (*Chinese Civil Law*), Pechino, 1990, p. 487, citato in Zhu Guobin, *The Right to Privacy: An Emerging Right in Chinese Law*, in *Statute Law Review*, 1997, vol. 18(3), p. 208-214.

[16] Zhonghua Renmin Gongheguo Qinquan Zeren Fa (中华人民共和国侵权责任法) [Legge sulla responsabilità civile della Repubblica popolare cinese] (adottata alla 12° sessione del Comitato permanente dell'11° Congresso nazionale del popolo e promulgata con decreto del Presidente della Repubblica n. 21/2009), art. 2.

[17] Si rimanda in particolare a Shujie Cui – Peng Qi, *The legal construction of personal information protection and privacy under the Chinese Civil Code*, in *Computer Law & Security Review*, 2021, n. 41, p. 7-8. Contro il tracciamento di una netta "linea di demarcazione" tra diritto alla privacy e diritto alla protezione delle informazioni personali pur distinguendo tra esse, Su Wenwei, *L'impatto della distinzione del codice civile tra privacy e informazioni personali sulla gestione del lavoro aziendale*, 2 giugno 2020, accessibile in lingua cinese al sito web: http://www.dehenglaw.com/CN/tansuocontent/0008/018724/7.aspx?MID=0902&AID=.

necessaria l'adozione di policy autonome volte a regolare il trattamento e la protezione delle informazioni personali condivise ogni secondo su Internet dalla popolazione del gigante asiatico[18]. Cogliendo il ruolo portante dei *big data* e delle informazioni personali nelle economie del XXI secolo, il Comitato centrale del Partito comunista cinese ha anzi riconosciuto con una certa *nuance* marxista i dati come "fattore di produzione" assieme alla terra, al lavoro, al capitale e alla tecnologia[19].

All'incorporazione della legge sulla responsabilità civile nel primo Codice civile della Repubblica popolare si è avuto il consolidamento di un sistema dualistico, astrattamente annoverabile come "europeo", in cui la tutela della privacy e quella delle informazioni personali si affermano come autonomi diritti (*quanli* 权利) in capo al cittadino. Il Codice civile del 2020, che marcatamente segnala la presenza del diritto cinese nella grande *familia* giuridica romanistica[20], ha visto la gemmazione dal diritto alla privacy, definita quale "[diritto] di una persona fisica [a] una vita privata indisturbata e ad un suo spazio privato, attività private e informazioni private che egli/ella non vuole rendere noti ad altri"[21], della

[18] Il governo cinese con nota n. 50 del 2015 ha predisposto un "Piano d'azione per la promozione dello sviluppo dei big data" (促进大数据发展行动纲要), al fine di promuovere l'industria digitale e innalzando per la prima volta a strategico il ruolo dei big data.

[19] Cfr. Zhonggong Zhongyang Guowuwuan Guangyu Guojian Gengjia Wanshan de Yao Su Shichang Hua Peizhi Tizhi Jizhi de Yijian (中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见) [Pareri del Comitato Centrale del Partito Comunista Cinese e del Consiglio di Stato sulla costruzione di un sistema e un meccanismo più completi per l'allocazione dei fattori basata sul mercato]. A commento dei Pareri, si rimanda a Lilian Li, *Data as a factor of production* (versione ridotta), del 4/11/2021, disponibile al sito web: https://lillianli.substack.com/p/abridged-data-as-a-factor-of-production. Sul tema della qualificazione giuridica dei dati come fattori di produzione, assoggettabili al regime giuridico dei beni, anche la dottrina italiana sta da tempo dibattendo: G. Carullo, *Big Data e pubblica amministrazione nell'era delle banche dati interconnesse*, in *Conc. mer.*, 4 [mi sembra l'issue: in caso, dopo l'anno?], 2016, p. 181; M. Maggiolino, *Big data e prezzi personalizzati*, ivi, 1, 2016, p. 3; G. De Minico, *Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria*, in *Dir. pubbl.*, 1, 2019, p. 89 ss.

[20] Tanto è stato scritto e tanto ancora si potrebbe scrivere sull'argomento. Si rinvia per sinteticità e chiarezza espositiva a R. Cardilli, *Diritto cinese e tradizione romanistica alla luce del nuovo Codice civile della Rpc*, in *Mondo Cinese*, vol. 167, anno XLVII, p. 25-45. Nello stesso numero si segnala M. Timoteo, *Il Codice civile in Cina: oltre i legal transplants?*, p. 13-24. Per un approccio completo al tema, F.R. Antonelli, *Il diritto cinese. Dall'antica alla nuova Via della Seta*, Padova, 2021.

[21] Zhonghua Renmin Gongheguo Minfa Dian (中华人民共和国民法典) [Codice civile della Repubblica popolare cinese] (adottato alla 3° Sessione del 13° Congresso nazionale del popolo e promulgato con ordine del Presidente della Repubblica n. 45/2020), art. 1032, co. 1. Cfr.

distinta protezione delle informazioni personali, obbligando (e dunque facendo sorgere un diritto) ogni organizzazione o individuo "che necessiti di accedere alle informazioni personali altrui" di farlo esclusivamente in "ottemperanza alla legge e garantendo la sicurezza di tali informazioni"[22]. Nella medesima disposizione si trova il divieto di *collection, use, processing, trasmission* ovvero *trading, provision* e *publishing* illegali di informazioni personali[23].

Il libro IV, capo VI disegna dunque "due sistemi (di protezione), due diritti": il primo diritto, quello alla privacy (*yinsi quan*隐私权), visto come diritto "negativo"[24], cioè alla non-intrusione nell'altrui vita privata con ogni mezzo che possa disturbare il "reame privato" di un individuo[25]; il secondo, quello alla protezione delle informazioni personali, diritto "positivo", legato non solo alla personalità della persona fisica ma anche al valore d'uso delle informazioni personali e dunque al diritto di controllare chi fa uso delle proprie informazioni e come viene estratto valore dall'utilizzo delle informazioni personali al fine di obiettare, correggere ovvero chiedere un risarcimento all'autorità giudiziaria[26]. Diversi sono pure i rimedi legali che il Codice civile appresta: da un lato un'azione

---

anche art. 110, dove si riconosce il godimento del diritto alla privacy a ogni persona fisica, distinguendolo esplicitamente da diritti attigui come quello alla reputazione e all'onore; art. 990, che annovera il diritto alla privacy fra i diritti di personalità: l'art. 994, che stabilisce il coniuge, i figli, i genitori o, in mancanza di questi, i parenti più stretti hanno il diritto di azione avverso colui che ha violato la privacy del proprio *de cuius*.

[22] Art. 111 cod. civ. PRC.

[23] *Ibidem.*

[24] Ciò del tutto similmente a quanto è avvenuto nello spazio giuridico europeo. Si veda la ricostruzione compiuta in L. Miglietti, *Profili storico comparativi del diritto alla privacy*, in *questa Rivista*, 2014, accessibile al sito web https://www.dirittocomparati.it/profili-storico-comparativi-del-diritto-alla-privacy.

[25] Cfr. l'elenco piuttosto dettagliato di condotte intrusive indicate all'art. 1033, cod. civ. PRC, nn. 1-6.

[26] Cfr. Wang Liming, *Sulla protezione legale dei diritti sulle informazioni personali,* in 现代法学 (*Modern Law Science*), 2014, n. 4, dove l'autore definisce da un lato la privacy come "diritto passivo e difensivo", mentre quello sulle informazioni personali "diritto attivo, di controllo e di utilizzo" grazie al quale il titolare può chiedere a un soggetto che detiene i suoi dati personali di modificarli o cancellarli anche quando non sono stati violati. Sulla stessa posizione G. Finocchiaro, *La giurisprudenza della Corte di Giustizia in materia di dati personali da* Google Spain *a* Schrems, in *Il diritto dell'informazione e dell'informatica*, Anno XXX, Fasc. 4-5, 2015, p. 118, in cui l'A. sostiene che il "diritto alla protezione dei dati personali deve essere considerato distinto dalla libertà negativa di non subire interferenze nella propria vita privata [...] costituendo invece il fondamento della libertà positiva di esercitare un controllo sul flusso delle proprie informazioni".

per risarcimento dei "danni psichici", dall'altro anche il risarcimento per violazione di una propria proprietà[27].

Il sistema duale cinese è stato ulteriormente perfezionato con l'entrata in vigore della Legge sulla protezione delle informazioni personali, il cui collegamento con la dimensione cibernetica è esplicitato pure nella volontà del legislatore cinese. La "continua e profonda integrazione tra informatizzazione e società economica"[28] hanno reso necessaria una regolamentazione *ad hoc* che integrasse e innalzasse la protezione fornita ai cittadini-utenti dal Codice civile, segnalando al contempo come fino ad ora la tranquillità della vita, la salute e la sicurezza della proprietà di cittadini cinesi sia stata messa a repentaglio proprio da chi, specie fra le aziende e le organizzazioni, ha compiuto atti illegali sulle informazioni personali altrui[29].

Come emergerà di seguito, tale sistema non è *self-sufficient*: esso piuttosto fa parte di un regime giuridico cibernetico che, a partire dall'emanazione della Legge sulla cybersicurezza nel 2017[30] – vera e propria *basic law* delle reti cinesi – , ha visto il fiorire di disposizioni legislative, regolamenti amministrativi, provvedimenti locali e agenzie statali che hanno accresciuto l'influenza dello Stato-partito sulla società. All'interno di tale ordinamento, la PIPL rappresenta forse la legge che, pur fornendo allo Stato-partito nuovi strumenti di controllo special modo sul settore privato, ha allo stesso tempo riconosciuto e garantito ai cittadini l'essenziale diritto alla protezione giuridica delle proprie informazioni personali.

---

[27] Cfr. Shujie Cui – Peng Qi, *op.cit.*, p. 15.

[28] Così Liu Junchen, vicepresidente della Commissione Affari Legislativi del Comitato permanente del Congresso nazionale del popolo nella *Spiegazione alla bozza di Legge sulla protezione delle informazioni personali della Repubblica popolare cinese*, pubblicata a seguito della 22° sessione del Comitato permanente del 13° Congresso nazionale del popolo il 13/10/2020 e disponibile in lingua cinese al sito web http://www.npc.gov.cn/npc/c30834/202108/fbc9ba044c2449c9bc6b6317b94694be.shtml.

[29] *Ibidem*. Si veda il caso del 2018 di un cittadino, William Zhang, subissato di chiamate telefoniche giornaliere da parte di agenti assicuratori nei due mesi che precedevano la scadenza della polizza assicurativa per la propria macchina fra lui e il gruppo Ping An Insurance. Reuters segnala come la vendita online delle informazioni personali fosse (*sia?*) una pratica comune in Cina su piattaforme come QQ o Tieba. Per maggiori informazioni, E. Tham, *Data dump: China sees surge in personal information up for sale*, del 23/08/2018, disponibile al sito web https://www.reuters.com/article/us-china-dataprivacy-idUSKCN1L80IW.

[30] Zhonghua Renmin Gongheguo Wangluo Anquan Fa (中华人民共和国网络安全法) [Legge sulla cybersicurezza della Repubblica popolare cinese] (adottata alla 24° Sessione del Comitato permanente del 12° Congresso nazionale del popolo il 7 novembre 2016 e promulgata con ordine del Presidente della Repubblica n. 53/2016). In avanti si adotterà per ragioni di sinteticità la trad. inglese "*Cybersecurity Law*" oppure l'acronimo inglese "CSL".

4. Ambito di applicazione e problematiche definitorie

Se la *Cybersecurity Law* ha un vasto ambito di applicazione corrispondente alla costruzione, operatività e gestione delle reti, dei servizi digitali e della loro sicurezza all'interno e pure all'esterno della Grande muraglia digitale cinese[31], anche la PIPL ne delimita uno proprio, più ristretto e in rapporto ancillare rispetto alla normativa sulla cybersicurezza. L'art. 3, comma 1 PIPL stabilisce infatti che la legge si applica a tutte "le attività di trattamento delle informazioni personali di persone fisiche (*ziranren* 自然人) dentro i confini della Repubblica popolare cinese"[32], dunque senza distinzioni di sorta tra mondo "tradizionale" e mondo digitale, in modo del tutto simile a quanto disposto all'art. 3, co. 1 GDPR[33].

Dal canto suo, la CSL interferisce già fornendo una sua più precisa e soddisfacente definizione di informazioni personali (*geren xinxi* 个人信息) come "tutti i tipi di informazioni, registrate elettronicamente o con altri mezzi, che, da sole o insieme ad altre informazioni, sono sufficienti a identificare l'identità di una persona fisica, compresi, ma non solo, i nomi completi delle persone fisiche, le date di nascita, i numeri di identificazione nazionale, le informazioni biometriche personali, gli indirizzi, i numeri di telefono e così via"[34]. La PIPL compie un passo indietro, preferendo utilizzare una definizione generica di informazione legata alla identificabilità di una persona fisica per mezzo delle stesse tramite mezzi elettronici o di altro tipo, ad esclusione delle informazioni trattate in modo anonimo (anonimizzazione)[35]. Il GDPR europeo, che pure si concentra

[31] Cfr. Art. 2, CSL. Sul tema della territorialità e relativa "territoralizzazione" del cyberspazio v. N. Tsaugourias, *Law borders and the territorialisation of cyberspace*, in *Indonesian Journal of International Law*, 18(4), p. 523-551, dove l'A. contesta l'opinione comune che vede nel cyberspazio in luogo di diritto sprovvisto di confini e di norme giuridiche vincolanti.

[32] Art. 3, comma 1, PIPL.

[33] Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati). In avanti si userà l'ormai noto acronimo "GDPR".

[34] Art. 76, n. 5, CSL.

[35] Art. 4, comma 1, PIPL. Nessuna reale innovazione rispetto alla legislazione di secondo livello finora emanata dal Governo o dalle agenzie governative. Ci si riferisce qui in particolare a Quanguo Renmin Daibiao Dahui Changwu Weiyuanhui <Guanyu Jianqiang Wangluo Xinxi Baohu de Jueding> [Decisione del Comitato permanente del Congresso nazionale del popolo sul *rafforzamento della protezione delle informazioni personali nelle reti*] (adottata il 28/12/2012), che, invece di una definizione di informazione personale, forniva una protezione per le "informazioni elettroniche che possono rivelare le identità personali dei cittadini e coinvolgere la loro privacy personale" (art. 1).

sull'identificabilità, elenca allo stesso tempo una serie non tassativa di identificativi diretti (come il nome o il numero di identificazione) oppure indiretti (come le caratteristiche psico-fisiche di un soggetto o lo stato economico)[36].

Ispirato alla normativa europea di riferimento sembra pure il principio di extraterritorialità, allorquando la PIPL estende il proprio ambito di applicazione territoriale alle attività eseguite al di fuori della RPC, ma che abbiano a oggetto le informazioni personali di personali di cittadini cinesi e a condizione che lo scopo sia fornire un servizio o un prodotto agli stessi ovvero analizzare e valutarne i comportamenti (c.d. *targeting*)[37]. Un'ultima specificazione completa però il quadro sull'applicabilità della PIPL, distanziandosi sensibilmente dal GDPR, ossia la previsione che nuove leggi o regolamenti amministrativi possano richiamare direttamente la PIPL[38]. Quest'ultima specificazione lascerebbe mano libera alla ormai onnipresente Amministrazione cinese del cyberspazio[39] (in inglese *Cyberspace Administration of China*, CAC) di integrare ovvero estendere l'applicabilità della PIPL al di fuori dell'elenco, tutt'altro che tassativo, dell'art. 3, co. 2, nn. 1-2. Ciò che finora è certo è che ai sensi del PIPL, le società straniere – anche senza presenza in Cina – impegnate nel trattamento delle informazioni

[36] Cfr. Art. 4, para 1, n. 1, GDPR. Inoltre il considerando 26 adotta il criterio della "ragionevole probabilità di identificazione", a mente del quale si ha identificabilità allorquando è possibile per il titolare del trattamento ovvero per un terzo identificare una persona fisica servendosi di tutti i mezzi, come l'individuazione, di cui egli può ragionevolmente avvalersi. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si deve prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici. Sul tema, v. C. Irti, *Personal Data, Non-personal Data, Anonymised Data, Pseydonymised Data, De-identified Data*, in R. Senigaglia – C. Irti – A. Bernes (eds.), *Privacy and Data Protection in Software Services*, Singapore, 2022 p. 50-2.

[37] Art. 3, comma 2, PIPL. Allo stesso modo l'art. 3, par. 1 del GDPR reitera il principio di stabilimento già presente nella direttiva 95/46/CE, seppur quest'ultima si soffermava sull'individuazione della legge di attuazione della direttiva applicabile al titolare del trattamento stabilito in un territorio nazionale. Di grande portata innovatrice rispetto alla previgente disciplina è il disposto dell'art. 3, par. 2 del GDPR, da leggersi necessariamente in collegato con il considerando 23, che, ravvisando la difficoltà tecnica nell'accertare la volontà del titolare di offrire beni o servizi data l'ubiqua accessibilità di un sito web, pone in capo al titolare del trattamento un generico obbligo di rendere chiara tale volontà. A conferma di ciò anche la giurisprudenza eurounitaria, in particolare in CGUE, [data?] *Pammer v. Reederei Karl Schlüter GmbH & Co* e *Hotel Alpenhof v. Heller*, cause riunite C-585/08 e C-144/09, dove la CGUE ha elaborato degli indici di massima per la sussistenza della volontà di *targeting*.

[38] Art. 3, co. 2, n. 3 PIPL.

[39] Con decreto n. 33 del 2014, il Consiglio di Stato della Repubblica popolare cinese ha provveduto a riorganizzare i già esistenti uffici con responsabilità legate agli "affari cibernetici", creando un ente governativo unificato sotto il nome di 国家互联网信息办公室 (*Guojia Hulianwang Xinxi Bangongshi*) e nota, anche nella *mainland*, con l'acronimo inglese di CAC.

personali di individui con sede in Cina sono vincolate dalla legge e sono tenute a costituire un'entità dedicata ovvero nominare un agente o un rappresentante designato in Cina per essere responsabili della gestione di questioni che rientrano nell'ambito di applicazione materiale della PIPL.

Le attività di trattamento consistono – ma non si limitano – alla raccolta, conservazione (*storage*), uso, elaborazione, trasmissione, fornitura, pubblicazione e cancellazione *(erasure)* delle informazioni personali[40]. La normativa europea nella lunga rubrica delle definizioni di cui all'art. 4 più diligentemente puntualizza che è trattamento "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali", elencando poi tutta una serie non esclusiva di attività che costituiscono attività di trattamento. Il legislatore cinese non segue tale impostazione, lasciando di fatto all'interprete il compito di definire di volta in volta quali operazioni possano costituire attività di trattamento. La legge impone comunque che le attività di trattamento debbano essere il più limitate possibile, e la raccolta eccessiva di informazioni personali viene proibita. Il trattamento deve dunque avere uno scopo chiaro, ragionevole e diretto unicamente al trattamento con metodi che abbiano la minore influenza sui diritti e gli interessi del singolo[41]. Vanno in ogni caso escluse le attività di persone fisiche nel trattamento di informazioni personali o familiari[42].

La legge cinese definisce in modo inequivoco i gestori del trattamento (*geren xinxi chuli zhe*个人信息处理者) come "organizzazioni o soggetti che, nelle attività di trattamento delle informazioni personali, determinano autonomamente le finalità del trattamento"[43]. L'omologo del gestore per la normativa europea è il titolare (*controller*) del trattamento, cioè "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali"[44]. Più complessa è invece la ricostruzione della figura di un "responsabile del trattamento" all'interno della PIPL: se il GDPR preferisce individuare tale figura con più disposizioni "professionalizzanti"[45], al contrario la PIPL riconosce solo la

[40] Art. 4, comma 2, PIPL.
[41] Art. 6, comma 1, PIPL.
[42] Art. 72, comma 1, PIPL.
[43] Art. 73, n. 1, PIPL.
[44] Art. 4, n. 7, GDPR. Al *considerando n. 74* si specifica la "responsabilità allargata" del titolare del trattamento "per qualsiasi trattamento di dati che quest'ultimo abbia effettuato o che altri abbiano effettuato per suo conto".
[45] Cfr. Art. 4, n. 8 GDPR, ove il responsabile del trattamento (*data processor*) assume una connotazione quasi professionale, dato il combinato disposto dell'art. 4 del GDPR – in cui si afferma che è *data processor* "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento" – e dell'art. 28, per cui

generica possibilità per i gestori del trattamento di stipulare accordi con terzi – definiti "affidatari" (*shoutuoren* 受托人) – al fine di far gestire a questi ultimi il trattamento nei tempi, modi e per le categorie previsti nel detto accordo, specificando misure di protezione, diritti e doveri di entrambe le parti e in ogni caso con l'obbligo per il gestore affidante di supervisionare sulle attività del gestore affidatario. Il gestore affidatario sarà obbligato al trattamento nelle finalità e nei metodi previsti dall'accordo, al termine del quale – o in caso di inottemperanza, nullità o cancellazione dello stesso – dovrà trasferire i dati al gestore affidante, ovvero cancellarli, senza possibilità alcuna di trattenerli. È vietato il trasferimento ad ulteriore gestore da parte dell'affidatario senza il consenso del gestore affidante[46].

La *Personal Information Protection Law* cinese prevede poi all'art. 20 – e similmente compie il GDPR, all'art. 26[47] – la possibilità di contitolarità del trattamento, che si realizza mediante un accordo fra due o più gestori del trattamento che "decidono congiuntamente su finalità e metodo del trattamento [e] sui diritti e obblighi di ciascuno".

5. Fra consenso granulare e dati sensibili: i diritti dei soggetti interessati dal trattamento

Fra gli istituti maggiormente paragonabili presenti tanto nel GDPR quanto nella PIPL spiccano certamente la base legale e il consenso informato. In entrambe le normative l'operatività del trattamento dei dati deve poggiare su una base giuridica che conferisca al trattamento stesso liceità, spesso fornita dal

quando il trattamento debba essere effettuato per conto del titolare del trattamento, questi deve ricorrere a responsabili del trattamento che presentino garanzie sufficienti, ovverosia specifiche competenze tecniche.

[46] Art. 21, PIPL. Si segnala che per la dottrina cinese, rilanciata anche dalle autorità competenti, non vi sarebbero differenze sostanziali fra la legislazione cinese ed europea nel concetto di "responsabile del trattamento" [Cfr. Fang Yu, *La legge sulla protezione delle informazioni personali al fine di risolvere i problemi più diretti e realistici che toccano le grandi massi popolari*, pubblicato sul sito internet della Cyberspace Administration of China il 25/08/2021 e accessibile in lingua cinese al seguente link http://www.cac.gov.cn/2021-08/25/c_1631491549783065.htm].

[47] La disciplina della contitolarità impone ai contitolari del trattamento di definire congiuntamente con un atto giuridico ("accordo interno") le finalità e i mezzi del trattamento, così come le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR e, in particolare, quelli riguardanti l'esercizio dei diritti dell'interessato. Cfr. art. 4, n. 8, art. 26 GDPR.

consenso della persona interessata[48]. Nella normativa europea, il consenso è rappresentato da qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile[49] e può essere espresso per il trattamento dei dati per una o più specifiche finalità[50]. La legge cinese invece non definisce univocamente il consenso, lasciando un vuoto che nei fatti è colmato dal Codice civile[51], dalla *Cybersecurity Law*[52] e dalla prassi giudiziaria, con non poche criticità dal lato dell'utenza[53].

Il legislatore cinese, similmente a quanto avviene nello spazio giuridico europeo sui dati, adotta lungo tutta la legge il modello "granulare" di consenso: questo dovrà essere nuovamente ottenuto allorquando lo scopo del trattamento, il metodo di trattamento o le categorie di informazioni trattate subiscano mutamenti[54]. Ogni persona ha diritto a revocare il consenso, in ottemperanza del

[48] L'art. 13, nn. 2-6 PIPL è perfettamente sovrapponibile all'art. 6, para. 1, lett. b-e GDPR. La normativa cinese è invece del tutto assente dell'interesse legittimo quale base legale stabilito invece all'art. 6, para. 1. lett. f GDPR. Ciò che invece prevede la PIPL (art. 13, n. 7) è la possibilità di allargare le basi legali con gli emanandi regolamenti amministrativi.

[49] Art. 4, n. 11 GDPR. Come specificato nel *considerando n. 32*, il consenso non sarebbe legittimamente manifestato attraverso il silenzio, l'inattività o la preselezione di caselle. Ciò è stato ribadito in *Orange Romania SA c. ANSPDCP (Causa C-61/19)*, dove la CGUE ha tenuto a precisare che la mancata deselezione di una cartella preselezionata non possa costituire manifestazione del consenso informato dell'utente.

[50] Art. 6, para. 1, lett. a, GDPR.

[51] Artt. 1035-6 cod. civ. PRC. Nel Codice civile il concetto di consenso non ha natura unitaria, v. Lu Qing, *La costruzione normativa della regola del "consenso" nella protezione delle informazioni personali*, in *Journal of Wuhan University (Philosophy and Social Sciences)*, 2019, n. 5, dove l'A. parla correttamente di "consensi" data la diversa efficacia giuridica che tali manifestazioni di volontà hanno, a volte di semplici autorizzazioni, altre di volontà di mutamento di un rapporto giuridico.

[52] Art. 41, CSL, che impone agli operatori di rete di pubblicare le regole per raccogliere e conservare dati, di esplicitarne scopi e mezzi, e di ottenere il consenso delle persone le cui informazioni sono raccolte.

[53] Cfr, Beijing Hulianwang Fayuan, *Huang c. WeChat Reading ("Tencent")*, dove la Corte Internet di Pechino, se da un lato ha riconosciuto una violazione delle informazioni personali dell'attore nei frequenti collegamenti fra la "lista amici" dell'app WeChat e i "suggerimenti di amicizia" nell'app WeChat Reading, definito come un "irragionevole collegamento", dall'altro non ha riconosciuto la violazione della privacy e ha anzi affermato che è del tutto legittimo impedire l'utilizzo di un software allorquando gli utenti scelgano di non fornire i propri dati personali. Su tutta una serie di problematiche emerse in materia, v. Kong Mengna, *ricerche sulla regola del "consenso" nel trattamento delle informazioni personali*, China Court Network del 17/12/2021, accessibile in lingua cinese al sito web: https://www.chinacourt.org/article/detail/2021/12/id/6440753.shtml.

[54] Art. 14, comma 2, PIPL ma cfr. European Data Protection Board, *Linee guida 05/2020 sul "consenso nel reg. 2016/679, versione 1.1"*, adottate il 4/5/2020.

quale i gestori del trattamento debbono provvedere con modalità opportune[55]. Sono fatti salvi gli effetti delle attività di trattamento prima della revoca del consenso[56]. Inoltre, è specificato che, salvo il caso in cui il trattamento dei dati sia necessario per la fornitura di prodotti o servizi, i gestori del trattamento non possono rifiutarsi di fornire i propri prodotti o servizi sulla base del rifiuto della persona interessata[57].

La PIPL ovvero altre leggi o regolamenti amministrativi possono altresì disporre che, oltre al consenso generico al trattamento dei dati personali, siano richiesti ulteriori consensi, distinti e separati da quello originario. Il caso in assoluto più rilevante è quello del trattamento delle informazioni sensibili (*mingan geren xinxi* 敏感个人信息), disciplinate al capo II, sez. II, ove si prevede che per trattare informazioni sensibili vada richiesto il consenso separato dell'individuo, anche in forma scritta se così disposto da altre leggi o regolamenti[58].

Se il GDPR categorizza in modo speciale i "dati particolari", vietandone il trattamento salvo il consenso esplicito dell'interessato[59], in netto contrasto rispetto alla tecnica europea troviamo le omologhe disposizioni cinesi per le quali sono sensibili tutte quelle informazioni che possono, "una volta trapelate o usate illegalmente, causare danno alla dignità della persona fisica e grave danno alla sua sicurezza personale o patrimoniale, includendo in ciò le informazioni su caratteristiche biometriche, sul credo religioso, su status specificamente designati, sulla salute, sui conti finanziari, sulla localizzazione, etc., così come le informazioni di minori di anni 14"[60].

---

[55] Art. 15, comma 1, PIPL.

[56] Art. 15, comma 2, PIPL.

[57] Cfr. art. 16, PIPL ma in modo dissimile si era già pronuncia la Corte Internet di Pechino, nel già ricordato *Huang c. WeChat Reading ("Tencent"), supra.*

[58] Art. 29, PIPL. Il trattamento dei dati sensibili è ammesso solo per scopi specifici e sotto strette misure di protezione. È quindi assai probabile che, oltre a un regolamento che disciplinerà il sistema di licenze previsto dall'art. 32 PIPL che consentirà di trattare tale categoria di informazioni, si assisterà all'emanazione di linee guida in materia, come lasciato intendere da Liu Ying, *Protezione delle informazioni personali sensibili: elementi importanti della nostra legge sulla protezione delle informazioni personali*, pubblicato sul sito web della Cyberspace Administration of China e accessibile in lingua cinese al seguente link http://www.cac.gov.cn/2021-09/08/c_1632692967456129.htm.

[59] Cfr. l'art. 9, GDPR e il relativo *considerando n. 51*, dove si afferma che i dati sensibili meritano di una specifica protezione per via del fatto che il loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali.

[60] Art. 28, PIPL. Va qui riportato che, in caso di trattamento delle informazioni di un minore di 14 anni, il consenso dovrà essere ottenuto da entrambi i genitori o dal tutore (unico caso di *"consenso speciale"*) e i gestori dovranno formulare regole specifiche per il trattamento di tali informazioni a norma dell'art. 31 PIPL. Il GDPR, all'art. 8, stabilisce invece che il trattamento

Nel prestare il consenso, in modo volontario ed esplicito, le persone devono essere messe nella precondizione di avere piena conoscenza del trattamento. Emulando la disciplina europea, la PIPL dispone l'obbligo di informativa per i gestori del trattamento[61]. Salvo altrimenti previsto, ovvero in caso di urgenza, emergenza o necessità[62], i gestori del trattamento hanno l'obbligo di informare in modo pieno, veritiero e accurato i titolari del trattamento (1) del loro nome e della modalità per contattarli; (2) dello scopo del trattamento, dei metodi, delle categorie e del periodo di conservazione dei dati; (3) dei metodi e procedure per esercitare i diritti previsti dalla legge; (4) e di ogni altra informazione prevista dalla legge o dai regolamenti[63]. Si hanno ulteriori obblighi di informativa in tutti gli altri casi espressamente previsti dalla legge[64].

Gli interessati hanno altresì il diritto di conoscere, consultare, ricevere copie e di decidere sui propri dati, così come il diritto di limitare o di rifiutare il loro trattamento salvo che la legge o i regolamenti amministrativi dispongano il contrario[65]. I gestori dovranno fornire spiegazioni agli interessati circa le regole impiegate nel trattamento[66]. In caso di errori o di incompletezza, gli interessati potranno richiedere la correzione ovvero azioni volte a completare i propri dati personali in un tempo opportuno[67].

I soggetti del trattamento hanno il diritto di richiedere la cancellazione (*youquan qingqiu shanchu*有权请求删除) delle informazioni personali raccolte quando (1) lo scopo del trattamento sia stato raggiunto, sia diventato impossibile da raggiungere ovvero non sia più necessario lo *storage* delle informazioni per lo scopo stesso; (2) il gestore del trattamento ha cessato la fornitura di servizi o prodotti, ovvero il periodo di conservazione è scaduto; (3) il soggetto ritira il consenso; (4) il gestore tratta i dati personali in difformità alla legge o ai

per il minore di 16 anni è lecito se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.

[61] Art. 14, comma 1, PIPL.

[62] Art. 18, PIPL.

[63] Art. 17, PIPL.

[64] Si pensi agli obblighi di informativa specifica in caso di trattamento dei dati sensibili (art. 30); in caso di fusione, separazione, scioglimento, dichiarazione di bancarotta e per ogni altra ragione che renda necessario il trasferimento delle informazioni dal gestore originario a terzi (art. 22); quando il gestore fornisce ad altri gestori di informazioni le informazioni che gestisce, fatti salvi i diritti originari dell'interessato verso il gestore terzo (art. 23).

[65] Art. 44 e 45, comma 1, PIPL.

[66] Art. 48, PIPL.

[67] Art. 46, PIPL.

regolamenti amministrativi; (5) in ogni altra circostanza prevista da disposizioni legislative o amministrative[68].

Il decesso del soggetto al trattamento fa sorgere in capo agli eredi il diritto a esercitare tutti i diritti che il *de cuius* avrebbe potuto esercitare, salvo che egli/ella abbia stabilito diversamente prima di morire[69].

Una norma di raccordo fra diritti dell'interessato e doveri del gestore è quella dell'art. 50, in cui si stabilisce che quest'ultimi debbano instituire un meccanismo di risoluzione delle controversie circa i diritti degli interessi. Nel caso di rigetto delle richieste provenienti dall'interessato, i gestori dovranno spiegare le proprie ragioni. È fatto salvo il diritto degli interessati di proporre ordinaria citazione a giudizio nei circuiti giudiziari ordinari[70].

6. Obblighi e responsabilità dei data controller cinesi

I *controller* soggetti alla legge cinese sono in primo luogo gravati da un generico obbligo di salvaguardia dei dati personali che trattano e dalla conseguente responsabilità[71]. Obbligo che da generico diviene specifico allorquando la legge impone a tutti i gestori di svolgere regolarmente verifiche sul trattamento dei dati e sul rispetto delle disposizioni di legge[72]. Essi debbono adottare tutta una serie di accorgimenti (es.: formazione del personale, tecniche avanzate di crittografia, pseudonimizzazione, piani di sicurezza contro *data leak*, etc.) volte a prevenire l'accesso non autorizzato, la diffusione, la distorsione o la perdita di dati[73]. Nel caso di *leakage* – frequenti anche in Cina[74] – i gestori – oltre

[68] Art. 47, comma 1, PIPL. Un tale diritto, che non va confuso con il diritto all'oblio di cui all'art. 17 GDPR, era già previsto dall'art. 1037 cod. civ. PRC.

[69] Art. 49, PIPL. Similmente cfr. art. 2-terdecies d.lgs. n. 101/2018 ("Codice Privacy"), che prevede che i diritti di cui agli artt. 15-22 GDPR (concernenti il diritto di accesso, rettifica, integrazione, oblio, portabilità) riferiti ai dati personali concernenti persone decedute possano essere esercitati "da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione".

[70] Art. 50, comma 2, PIPL.

[71] Art. 9, PIPL. Va inoltre segnalato che gli obblighi di cui si dirà sono posti, sbrigativamente, a carico anche dei terzi affidatari del trattamento (art. 59 PIPL).

[72] Art. 54, PIPL.

[73] Art. 51, PIPL.

[74] Nel 2011 il database della China Software Developer Network è stato oggetto di quello che è stato definito dagli esperti il più grave *data leak* di utenti della storia cinese, esponendo e diffondendo i dati di più di 6 milioni di utenti [cfr. Xue Yang, *Chinese Internet Suffers the Most Serious User Data Leak in History*, del 26/12/2011 accessibile in lingua inglese al sito web: https://www.forcepoint.com/fr/blog/x-labs/chinese-internet-suffers-most-serious-user-data-leak-history.

a adottare immediate misure di rimedio – dovranno notificare i dipartimenti di sicurezza e gli individui sulle cause e possibili danni causati dalle condotte, sulle misure correttive adottate e su quelle che i singoli individui possono adottare e sulle modalità per contattare il gestore del trattamento[75].

Nel caso in cui i dipartimenti competenti dovessero venire a conoscenza di rischi relativamente seri nelle attività di trattamento delle informazioni personali ovvero in caso di incidenti, essi potranno contattare direttamente il rappresentante legale del gestore o la persona responsabile ovvero potranno richiedere ai gestori di affidare a istituzioni specializzate il compito di condurre controlli di conformità delle loro attività di trattamento, così come l'adozione di misure volte a correggere ed eliminare le vulnerabilità[76].

I dipartimenti competenti dovranno in ogni caso riferire e trasferire immediatamente alle autorità competenti in materia di pubblica sicurezza tutte le informazioni necessarie in caso di attività illecite nel trattamento ovvero di attività che si sospettino essere dei crimini[77].

In modo forse più netto rispetto al GDPR[78], la PIPL prescrive che il periodo di conservazione debba essere "il più breve periodo, necessario alla realizzazione dello scopo del trattamento delle informazioni personali"[79].

L'art. 24 impone ai gestori del trattamento i principii di trasparenza e non discriminazione in caso di utilizzo dei dati raccolti per i processi decisionali automatizzati[80], laddove il GDPR stabilisce per l'interessato (*data subject*) "il diritto di non essere soggetto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo

[75] Art. 57, comma 1, PIPL.
[76] Art. 64, PIPL.
[77] Art. 64, comma 2, PIPL.
[78] Cfr. art. 28, para. 1, GDPR, che prevede che i dati vadano conservati "per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati".
[79] Art. 19, PIPL. Se il periodo di conservazione non è ancora terminato o la cancellazione delle informazioni è difficile da realizzare, i gestori dovranno cessare il trattamento, eccetto per lo *storage* e per le misure di sicurezza a ciò necessarie (art. 47, co. 2, PIPL).
[80] La definizione di "processo decisionale automatizzato" viene data dall'art. 73, n. 2 della legge, cioè "l'attività di usare programmi computerizzati per analizzare o valutare automaticamente i comportamenti personali, le abitudini, gli interessi, gli hobby, ovvero lo status finanziario, di salute, di credito, o altri status, per poi prendere decisioni [basate su quanto raccolto]". La persona, oltre ad avere il diritto di rifiutare il tracciamento in caso di utilizzo di algoritmi decisionali che producano "decisioni con grande influenza" sui suoi diritti e interessi, in caso contrario ha il diritto di chiedere spiegazioni al responsabile del processo automatizzato (art. 24, c. 3). Un *non-targeting right* viene in ogni caso riconosciuto all'interessato sarebbe il *target* di tecniche di *push delivery* ovvero di vendite commerciali attraverso processi decisionali automatizzati (art. 24, co. 2).

riguardano o che incida in modo analogo o significativo sulla sua persona"[81], salvo i casi stabiliti dal GDPR medesimo.

Allorquando trattino dati sensibili, utilizzino algoritmi decisionali, affidino la gestione a un responsabile del trattamento ovvero divulghino informazioni personali, forniscano dati all'estero o svolgano attività di trattamento con grande influenza sui soggetti del trattamento, i gestori del trattamento dovranno svolgere una valutazione d'impatto preventiva sulla protezione delle informazioni personali, oltre che registrare le proprie attività[82]. Tale valutazione riguarda non solo la legalità, legittimità e necessarietà del trattamento ma anche l'influenza sugli individui, i rischi sulla sicurezza e una valutazione ulteriore circa la legittimità e la sostenibilità al rischio delle misure protettive adottate[83]. I report circa le valutazioni sul rischio e i record sullo stato del trattamento andranno conservati per almeno tre anni[84].

In risposta a diverse rimostranze per l'utilizzo di strumenti di riconoscimento facciale[85], la PIPL ha posto alcuni limiti a tali strumentazioni, utilizzabili in luoghi pubblici solo se: (1) sono poste a salvaguardia della sicurezza pubblica; (2) nel rispetto delle normative statali; (3) e installando chiari segnali di indicazione. Le immagini così raccolte non possono essere usate per altri scopi se non per pubblica sicurezza[86].

I "grandi gestori" del trattamento dovranno nominare uno o più *personal information protection officer* (*geren xinxi baohu fuzeren* 个人信息保护负责人). Mentre le omologhe disposizioni europee si dilungano nel descrivere designazione, posizione e compiti del *data protection officer*[87], l'art. 52 della PIPL si limita ad affermare che tale figura è responsabile della supervisione delle attività di trattamento, così come dell'adozione di misure di protezione, oltre che essere il riferimento di ogni eventuale contatto da parte degli interessati[88].

[81] Art. 22, GDPR.
[82] Art. 55, PIPL.
[83] Art. 56, comma 1, PIPL.
[84] Art. 56, comma 2, PIPL.
[85] La città cinese di Hangzhou nella provincia dello Zhejiang è stata la prima città cinese a proibire l'utilizzo obbligatorio di tecnologie biometriche (fra cui il riconoscimento facciale) per l'accesso alle comunità residenziali, v. Wang Qiuyan – Qin Jianhang – M. Walsh, *East China Internet Hub Mulls Ban on Facial Recognition in Residential Areas*, in *Caixin Global*, pubblicato il 29/10/2020 e accessibile in lingua inglese al seguente link: https://www.caixinglobal.com/2020-10-29/east-china-internet-hub-mulls-ban-on-facial-recognition-in-residential-areas-101620299.html.
[86] Art. 26, PIPL.
[87] Cfr. artt. 37-39, GDPR.
[88] Art. 52, comma 2, PIPL.

Similmente ai "grandi gestori", la PIPL prevede una "norma anti-BATX" che ha come target proprio i gestori di informazioni personali che forniscano importanti servizi Internet su piattaforma, i quali abbiano un importante numero di utenti, e i cui modelli di business siano complessi. Questi dovranno rispettare una serie specifica di obbligazioni, la più importante delle quali è l'istituzione di sistemi e strutture di conformità alla protezione dei dati personali e l'istituzione di un organismo indipendente composto principalmente da membri esterni per la supervisione degli impegni sulla protezione dei dati[89]. Inoltre, tali società dovranno "accettare la supervisione della comunità" (*jieshou shehui jiandu* 接受社会监督)

In tema di responsabilità amministrativa, laddove non si ottemperi alle disposizioni della PIPL, i dipartimenti competenti potranno ordinare la correzione delle condotte, confiscare i guadagni illeciti e ordinare la sospensione momentanea o la cessazione della fornitura del servizio dei programmi che gestiscono illecitamente le informazioni personali. Allorquando il gestore rifiuti di ottemperare agli ordini dipartimentali di correzione, sarà imposta una sanzione amministrativa di non più di 1 milione di yuan (ca. 130'000 euro) e la persona direttamente responsabile sarà sanzionata con una cifra che va da 10'000 a 100'000 yuan[90].

Nel caso in cui le condotte siano gravi, il dipartimento provinciale o quello di livello superiore (fino a giungere, ovviamente, alla CAC), potrà imporre, oltre che le succitate misure, una sanzione amministrativa di non più di 50 milioni di yuan (ca. 6'550'000 euro), oppure una sanzione fino al 5% del fatturato annuo. Di maggiore gravità è il potere di ordinare la sospensione delle relative attività economiche o la cessazione delle stesse per scopi di rettifica, così come la comunicazione alle autorità competenti al fine di cancellare la corrispondenza licenza amministrativa se non addirittura della licenza per compiere attività economiche. La persona direttamente responsabile sarà in caso punibile con sanzione amministrativa fino al milione di yuan e con l'interdizione momentanea dagli uffici di direttore, supervisore, manager di alto livello o di *personal information protection officer*[91].

Le condotte illecite del gestore o dei responsabili del trattamento saranno inserite all'interno dei fascicoli creditizi (*xinyong dang'an* 信用档案) così come stabilito da leggi e provvedimenti amministrativi e verranno pubblicizzati[92].

---

[89] Art. 58, n. 1, PIPL.
[90] Art. 66, comma 1, PIPL.
[91] Art. 66, comma 2, PIPL.
[92] Art. 67, PIPL. La legge qui si riferisce agli strumenti di conservazione elettronica che stanno venendo messi a punto nell'ambito del c.d. "Corporate Social Credit System" (*shehui*

Allorquando non sia possibile per il gestore del trattamento dimostrare che egli non sia responsabile della violazione dei diritti e degli interessi, risultante in un danno per la persona fisica soggetta al trattamento, egli sottostarà a una forma di responsabilità oggettiva, dovendo perciò compensare in base al danno emergente per la persona e al lucro derivato per il gestore stesso[93].

È fatto salvo il diritto per più soggetti del trattamento che siano stati cagionati di una lesione ai propri diritti o interessi da una medesima condotta lesiva di adire le Corti del Popolo in base alla legge. Hanno potere d'intervento principale anche le Procure del Popolo, gli organismi dei consumatori designati dagli statui, e le organizzazioni designate dalla CAC[94]. Se dai fatti lesivi delle disposizioni della PIPL dovesse emergere violazione della legge penale o sulla pubblica sicurezza, si applicheranno le disposizioni riguardanti le indagini penali e sulla responsabilità penale[95].

7. Il *cross-border* delle informazioni personali: gestori stranieri e gestori critici alla prova della tutela dei dati

Di fondamentale importanza per gli operatori stranieri è il Capo III della PIPL, dedicato al fenomeno del trasferimento "oltre Grande muraglia digitale" dei dati personali dei cittadini cinesi.

È bene segnalare come l'art. 43 della legge stabilisce il "principio di reciprocità nel trattamento delle informazioni personali": se, infatti, un Paese o una regione adotta politiche discriminatorie, limitazioni o misure simili contro la Cina, la Repubblica popolare si riserva la facoltà di adottare a sua volta misure simili[96]. La Cina si impegna inoltre a rispettare i trattati e gli accordi internazionali che pongano ulteriori condizioni sulla fornitura di dati al di fuori dei confini della

xinyong tixi 社会信用体系), un piano del Governo cinese di uso delle più moderne tecnologie per monitorare e guidare il comportamento degli operatori di mercato. Il "Corporate Social Credit System" si basa su una serie di requisiti fissati dalle autorità governative, sul monitoraggio del settore privato e sull'impiego di algoritmi valutativi tramite i quali vengono stilate delle classifiche di punteggio. All'aumentare o al diminuire del punteggio, corrispondono *bonus* e *malus* per la singola impresa. Per un'analisi del "Corporate Social Credit System" dal punto di vista delle imprese europee, v. European Chamber of Commerce in China – Sinolytics, *The Digital Hand. How China's Corporate Social Credit System Conditions Market Actors*, European Chamber of Commerce in China, 2019.

[93] Art. 69, PIPL.
[94] Art. 70, PIPL.
[95] Art. 71, PIPL.
[96] Art. 42, PIPL.

Repubblica popolare[97]. Da parte cinese si ribadisce l'impegno nel collaborare con le autorità giudiziarie e di polizia straniere per la fornitura di dati personali immagazzinati in Cina a seguito di approvazione delle competenti autorità della *mainland*[98].

Ruolo chiave verrà svolto dalla Cyberspace Administration of China, che dovrà valutare e autorizzare il *cross-border* di dati personali solo se il gestore (1) passerà la valutazione di sicurezza di cui all'art. 40 della PIPL; (2) verrà certificato da un organo specifico sempre interno alla CAC; (3) concluderà un contratto con una parte ricevente straniera in linea con gli standard formulati dalla CAC; e (4) se ottempererà ad altre condizioni previste dalla legge, dai regolamenti amministrativi, o dalla CAC stessa[99]. I gestori cinesi si impegnano affinché i ricettori stranieri di dati personali adottino gli standard di protezione della PIPL nello svolgimento delle attività di trattamento dei dati[100].

Il gestore cinese è gravato da uno specifico obbligo di informare l'interessato di tutte le informazioni personali del ricettore straniero, oltre che dall'obbligo di ricevere il consenso separato dell'interessato per la fornitura transfrontaliera dei suoi dati[101], mentre l'operatore straniero che desidera gestire dati all'interno dei confini della Repubblica popolare dovrà stabilire un organo dedicato o nominare un rappresentante entro i confini della Repubblica popolare per ogni attività riguardante la gestione dei dati[102].

In ottemperanza a quanto previsto dall'art. 38, comma 1, n. 1, l'art. 40 va a porre specifiche disposizioni per gli operatori di infrastrutture informatizzate cruciali (*"Critical information infrastructure operators*, "CIIOs") e per i gestori di dati che raggiungono una certa soglia di immagazzinamento stabilita dalla CAC:

---

[97] Art. 38, comma 2, PIPL. È bene ricordare che la Cina non ha finora siglato alcun trattato internazionale o accordo che abbia a oggetto il trasferimento di dati. Nell'ambito dell'Asia-Pacific Economic Cooperation (APEC) è stato adottato nel 2015 l'*APEC Privacy Framework (2015)*. L'APEC è un organismo di diritto internazionale e non è dotato di personalità giuridica.

[98] Art. 41, PIPL.

[99] Art. 38, comma 1, PIPL. Sono in fase di pubblica revisione le "Misure per la valutazione della sicurezza delle esportazioni di dati", Guojia Hulianwang Xinxi Baogongshi <Shuju Chujing Anquan Pinggu Banfa (Zhengqiu Yijian Gao)> [Cyberspace Administration of China, *Misure per la valutazione della sicurezza delle esportazioni di dati (bozza per commenti)*, pubblicato sul sito web della CAC il 29/10/2021 e accessibile in lingua cinese al seguente link http://www.cac.gov.cn/2021-10/29/c_1637102874600858.htm]. In base alle misure, si imporrà ai CIIOs, ai gestori di informazioni di più di un milione di persone, ai gestori di informazioni sensibili di più di 100.000 persone o di 10.000 persone "all'estero" una serie di obblighi procedurali per la fornitura di dati all'estero (art. 3) sui quali supervisioneranno i competenti uffici provinciali della CAC.

[100] Art. 38, comma 3, PIPL.

[101] Art. 39, PIPL.

[102] Art. 43, PIPL.

in primis, quella che i dati vadano conservati *(storing)* entro i confini della Repubblica popolare cinese. Se i CIIOs e i "grandi gestori" del trattamento hanno la necessità di fornire dati all'estero, dovranno passare una valutazione di sicurezza strutturata dalla CAC, salvo specifiche disposizioni che li sollevino da tale valutazione[103].

8. Prime considerazioni conclusive: tutela del singolo nel quadro delle "caratteristiche cinesi"?

Le disposizioni approvate dal Comitato permanente del CNP ed entrate in vigore il 1° novembre 2021 rappresentano il primo tentativo di regolamentare in maniera olistica il complicato terreno del trattamento dei dati personali nella Repubblica popolare. La PIPL segue di qualche mese un'altra importante legge, la *Data Security Law* (DSL), che ha anch'essa lo scopo di regolare e limitare le operazioni quotidiani che vengono compiute sui dati di cittadini e organizzazioni cinesi, sempre nel framework della *Cybersecurity Law* del 2017.

Rimanendo focalizzati sulla Legge sulla protezione delle informazioni personali, il più alto consesso legislativo cinese ha cercato, anche per una certa comodità nomopoietica, di emulare il *General Data Protection Regulation* europeo. Come si è potuto brevemente constatare, sono diverse le disposizioni nella PIPL che ricalcano, vuoi per definizioni, vuoi per portata normativa, le corrispondenti europee, creando ciò che potrebbe venire sbrigativamente etichettato come un "GDPR con caratteristiche cinesi".

Certamente la PIPL recepisce alcune tendenze emerse non soltanto nella società cinese ma anche nella giurisprudenza a favore della limitazione (se non del bando) delle più moderne tecniche di sorveglianza, tracciamento e regolamentazione degli spazi che fanno uso di dati personali e biometrici, tanto da portare la Corte Suprema del Popolo a emanare una interpretazione giuridica, efficace dal 1° agosto 2021[104], che bandisce l'utilizzo obbligatorio del

[103] Art. 40, secondo e terzo periodo, PIPL. La PIPL qui rimanda alla Legge sulla cybersicurezza e alla categoria di "infrastruttura informatizzata critica", cioè di tutte quelle reti che, se a rischio, possono danneggiare gravemente la sicurezza nazionale. La CSL elenca una serie di infrastrutture critiche, come i servizi informatici e di comunicazioni pubbliche, l'energia, la finanza, i trasporti, la conservazione delle acque, le reti di *e-governance*, etc. (art. 31 CSL). Gli operatori di queste reti, oltre ai generici obblighi previsti dalla CSL per i *network provider*, sono gravati da specifici obblighi e sanzioni.

[104] Zuigao Renmin Fayuan <Guanyu shenli shiyong ren lian shibie jishu chuli geren xinxi xiangguan minshi anjian shiyong falü ruogan wenti de guiding> Fashi [2021] 15, <<关于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>>, 法释 [2021] 15号

riconoscimento facciale sulla base di una lettura restrittiva del Codice civile. Tutti i cittadini avranno progressivamente esteso il diritto di optare (*opt-out right*) fra il riconoscimento facciale ed altre modalità obbligatoriamente fornite dalle compagnie di gestione e app[105].

Va segnalato che, a differenza del GDPR[106], la PIPL nulla dice circa il "diritto all'oblio" ("*right to be forgotten*", in cinese *bei yiwang quan* 被遗忘权)[107], confermando la giurisprudenza cinese in materia, che già prima

---

[*Interpretazione circa disposizioni su diverse questioni relative all'applicazione della legge in cause civili riguardanti l'uso in prova della tecnologia di riconoscimento facciale per elaborare informazioni personali*], Interpretazione giuridica n. 15/2021 (adottata nella 1841° riunione della Commissione giudicatrice della Corte Suprema del Popolo dell'8 giugno 2021 ed entrata in vigore il 1° agosto 2021). In base a tali disposizioni, le Corti del popolo dovranno valutare come violazione dei diritti della personalità e degli interessi di una persona fisica allorquando un *service provider* non renda note le regole per il tracciamento delle informazioni facciali; quando non abbia indicato chiaramente lo scopo, il metodo o la portata del trattamento; e quando il trattamento delle informazioni facciali è soggetto al consenso di un individuo e il *service provider* non ottiene il consenso separato della persona fisica o del suo tutore ovvero il consenso scritto in conformità alle leggi e ai regolamenti amministrativi.

[105] Cfr. F. Hersey, *China court interpretation to limit use of facial recognition*, 28/6/2021, disponibile in https://www.biometricupdate.com/202107/china-court-interpretation-to-limit-use-of-facial-recognition.

[106] Art. 17, GDPR. Per un commento sul tema del diritto all'oblio, S. Martinetti, *Diritto all'oblio e motori di ricerca: il bilanciamento tra memoria e oblio in internet e le problematiche poste dalla de-indicizzazione*, in *Dir. inf.*, [vol.?] 2017, p. 566; ma anche G.B. Ferri, *Diritto all'informazione e diritto all'oblio*, in *Riv. dir. civ.*, [vol.?]1990, 808, sul tema delle connessioni fra diritto all'oblio e privacy, dove si rinviene la nota affermazione che "il diritto all'oblio appartiene alle ragioni e alle "regioni" del diritto alla riservatezza". In ordine temporale, sul diritto all'obblio si veda M. Mezzanotte, *Il diritto all'oblio. Contributo allo studio della privacy storica*, Napoli, 2009.; A. Miletti, *La protezione dei dati nella rete tra* cloud computing *e diritto all'oblio: questioni di riservatezza e responsabilità*, in *Corti salernitane*, 2-3, 2012, p. ?; D. Marongiu, *Il diritto all'oblio come diritto all'esclusione dai motori di ricerca. Dalla giurisprudenza europea al diritto amministrativo italiano*, in *Riv. dir. e proc. amm.*, 1 [vol. o issue?], 2015, p. 243-264.

[107] Il tema suscita comunque l'interesse della dottrina cinese più attenta, che ha esaminato, proprio a partire dal celebre caso *Google Spain c. AEPD (C-131/12)*, le problematiche di natura etica e politica che sorgono attorno al problema del *right to be forgotten*. In particolare, Liu Zegang, *La protezione del diritto all'oblio e il costo per la libertà nell'Era dell'Iper-connessione*, in (当代法学) *Contemporary Law Review*, 2019, vol. 1, p. 91-100, ove l'A., inquadrando prima la natura giuridica del diritto all'oblio nello spazio giuridico europeo, ha rilevato la "tensione" tra libertà e diritto all'oblio, avvertendo del "rischio di una lesione della libertà" se si addiviene ad un compiuto riconoscimento del diritto all'oblio, e preferendo dunque lo *status quo* cinese sul tema, ove esisterebbero autonomi "diritti alla cancellazione" di determinate informazioni. A favore dell'introduzione del diritto all'oblio, specie nell'"era dei *big data*", valutando positivamente l'impatto che ciò avrebbe sullo sviluppo della "tutela della privacy personale nella nuova era e nello sviluppo dell'e-commerce", v. Zhang Jianwen, *The Field Thinking of Right to be Forgotten and the Relationship with Privacy Right and Right of Individual Information*, in *Journal of*

dell'emanazione della PIPL e della Cybersecurity Law aveva negato che nell'ordinamento cinese esistesse un tale diritto[108].

Un'area dove la Cina ha seguito l'esempio europeo è la limitazione nell'utilizzo di algoritmi decisionali, compresi quelli basati sul *profiling*: in entrambe le legislazioni il soggetto del trattamento ha "il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato" (art. 22, comma 1, GDPR) ovvero "il diritto di rifiutare che i gestori del trattamento compiano decisioni esclusivamente sulla base di metodi automatizzati di decisione" (art. 24, comma 3, PIPL).

Se vanno lodate le accresciute tutele del singolo in un ordinamento giuridico e in una cultura che spesso sacrificano la riservatezza e le informazioni personali sull'altare del controllo collettivo[109], non bisogna dimenticare le "caratteristiche cinesi" (*Zhongguo tese* 中国特色) di cui la legge è disseminata, a partire dal fatto che questa non pone gli stessi obblighi ai quali devono sottostare i gestori del trattamento anche in capo alle autorità statali[110].

Chongqing University of Posts and Telecommunications (Social Science Edition), 2017, 29(1), p. 24-30; per una posizione mediana e mediata ma pur sempre favorevole all'introduzione del diritto all'oblio nel diritto cinese per "tornare al punto di partenza etico della natura umana", cfr. Li Lifeng, *Il "diritto all'oblio" nei contesti locali: una costruzione procedurale del diritto alle informazioni personali*, in *Journal of Wuhan University (Philosophy and Social Sciences)*, 2019, n. 3, p. 145 ss.

[108] Cfr. Sentenza del Primo Tribunale Intermedio del Popolo di Pechino, *Ren Jiayu v. Beijing Baidu Netcom Technology Co., Ltd. (2015), Zhongmin Zhongzi n. 09558* in cui la parte attorea affermava di godere del "diritto all'oblio" delle informazioni su un rapporto di lavoro pregresso – reputato poco edificante per la sua immagine – e che pertanto tali informazioni dovessero essere cancellate dal motore di ricerca Baidu, controllato dalla società convenuta in giudizio. La Corte, oltre a rubricare l'oggetto del caso come afferente ai "diritti alla reputazione", ha rigettato la richiesta dell'attore, statuendo oltretutto che la descrizione oggettiva del precedente lavoro non richiedeva alcun tipo di protezione speciale.

[109] Il fenomeno più incisivo e di massa a cui si fa riferimento nell'era digitale è certamente quello dei "motori di ricerca di carne umana" (*renrou sousuo yinqing* 人肉搜索引擎). Paragonabile all'inglese *doxing*, il termine indica quel fenomeno, cominciato dai primi anni 2000, in cui i *netizen* cinesi si riunivano in forum o community per cercare e mettere insieme informazioni private su singoli individui. Il fenomeno è stato descritto sia nelle arti [v. il film "*Caught in the Web*" (2012), regia di Chen Kaige] e nel diritto, v. Dai Jitao, *Internet Mass Hunting: una protezione equilibrata della privacy e della libertà di parola*, in 法学 (*Legal Studies*), 2008, n. 11, p. ?.

[110] Il Capo II, Sez. III della PIPL pone alcune disposizioni specifiche che si applicano agli organi di Stato, i quali, nel trattamento delle informazioni personali, non devono comunque eccedere gli scopi necessari al raggiungimento dei loro doveri e responsabilità previste dalle leggi (art. 34). Salvo in caso di urgenza, necessità o emergenza, gli organi statali debbono notificare all'interessato scopi e responsabilità del trattamento (art. 35). La legge inoltre specifica che i dati gestiti dallo Stato (o da altre organizzazioni autorizzate alla gestione per conto dello Stato) in

Anzi, gli accresciuti poteri della Cyberspace Administration of China – da una parte produttore attivo di disposizioni e controllore dell'applicazione delle stesse – fanno sì che questa agenzia governativa, creata nel 2016, assurga al ruolo di *dominus* non solo del cyberspazio cinese, ma anche del controllo e del trattamento dei dati e dei gestori di dati che desiderano operare in Cina. Sarà CAC l'ente che coordinerà gli altri dipartimenti nella formulazione di regole e standard di protezione delle informazioni personali, anche per gestori di piccole dimensioni e per l'impiego di nuove tecnologie che facciano impiego di informazioni sensibili (es. riconoscimento facciale, intelligenza artificiale), anche a scopo di propaganda[111]. Sempre la CAC supporterà la ricerca, lo sviluppo e l'adozione diffusa di tecnologie e servizi pubblici di autenticazione dell'identità elettronica, anche online[112].

Inoltre, il livello delle sanzioni previste in caso di violazione delle disposizioni si pongono in linea con quel *leitmotiv* cominciato con l'indagine su Alibaba condotta della State Administration for Market Regulation, l'antitrust cinese, e con tutta quella serie di multe e condanne che hanno raggiunto le big tech del Paese asiatico e di cui si accennava nelle introduzioni.

È bene quindi ricordare il costante accenno che la legge compie non soltanto al ruolo delle agenzie governative – in un sistema politico-istituzionale in cui queste sono tutt'altro che indipendenti – ma anche alla *governance* statale sui dati personali del singolo: se l'art. 10 vieta infatti ogni attività di trattamento che metta a repentaglio la sicurezza nazionale (*guojia anquan* 国家安全) e l'interesse pubblico (*gonggong liyi* 公共利益), gli artt. 11 e 12 sanciscono il ruolo attivo del Governo centrale, che istituisce una struttura di protezione dei dati personali con la partecipazione degli organi di governo, delle imprese, di organizzazioni sociali rilevanti e della popolazione, il tutto in un quadro di "vigorosa partecipazione" dello Stato nella formulazione di *best practices* a livello internazionale per il trattamento dei dati e per la cooperazione fra Stati.

---

attività di trattamento sono oggetto di *storage* nel territorio della *mainland* cinese, salvo sia assolutamente necessario fornirli al di fuori di esso (art. 37). Il capo VI enuncia in maniera limitata i doveri e le responsabilità dei dipartimenti di Stato – in particolare CAC e MIIT – nella pianificazione, coordinazione, gestione, protezione dei dati personali (art.60, co. 1). Saranno le pertinenti disposizioni statali a determinare i dipartimenti competenti in materia a livello di contea e superiore (art. 64).

[111] Cfr. art. 62, nn. 1-2, PIPL. I dipartimenti a ogni livello incaricati della protezione dovranno condurre attività di educazione e propaganda in materia di protezione delle informazioni personali, accettare e gestire reclami e report, effettuare valutazioni, produrre e pubblicare report e risultati delle valutazioni, condurre investigazioni in caso di attività illecite, etc. (art. 61).

[112] Art. 62, n. 3, PIPL.

Come alcuni commentatori hanno notato, l'emanazione della PIPL può peraltro rappresentare un punto di riferimento sul tema del trattamento dei dati per i Paesi dell'Asia-Pacifico ovvero per regimi politici autocratici e illiberali, portando – dopo oltre un secolo di "importazioni legali" – a una "esportazione legale" e quindi nel caso di specie alla diffusione del modello di controllo cinese sui dati[113]. Allo stesso tempo, come nota la Camera di commercio europea in Cina, il combinato della PIPL e della DSL, produrrà, al netto dei "significativi sviluppi nel regime della sicurezza digitale", anche un "impatto estremamente negativo sulle operazioni finanziarie"[114].

***

ABSTRACT: The essay, following a brief outline of the legal evolution of the implementation of the right to privacy in the Chinese legal culture, focuses on the analysis of the Personal Information Protection Law (PIPL) of the People's Republic of China, by comparing it with the General Data Protection Regulation (GDPR) of the European Union.

The provisions of the new information protection law will be analysed, in order to prove the evolution of the Chinese legal system from a monistic scheme of privacy protection to a dualistic protection of both privacy and personal information, and to assess the recognition of certain individual rights within the framework of the "rule of law with Chinese characteristics".

[113] Invero, seppur con eco ridotta rispetto alle spesso decantate o temute implicazioni economiche e finanziarie, la "Belt and Road Iniatitive" sta già influenzando soprattutto i Paesi in via di sviluppo. Cfr. F.R. Antonelli, *Gli aspetti giuridici della Belt and Road Initiative*, in *Mondo Cinese*, vol. 165.168, 2018, p. 121-135, ove l'autore sostiene come "il basso livello di istituzionalizzazione e l'uso della *soft law*" stiano favorendo il diffondersi nei Paesi africani e asiatici dei modelli e principi giuridici della Repubblica popolare attraverso l'arrivo dei finanziamenti e dei progetti legati alla BRI. In particolare poi l'a. fa riferimento al "Forum on the Belt and Road Legal Cooperation", tenutosi a Pechino il 2 luglio 2018 sotto l'egida del Ministero degli affari esteri e dalla China Law Society, visto come un tentativo di *moral suation* giuridica.

Si veda anche P. Swabey, *Here's what 'China's GDPR' means for international businesses*, del 27/8/2021, accessibile al sito web https://techmonitor.ai/policy/heres-what-pipl-china-gdpr-means-for-international-businesses, dove l'A. riporta che la "PIPL rappresenta il livello massimo degli obblighi di conformità alla privacy dei dati nella regione [nda. dell'Asia-Pacifico], e stiamo vedendo sempre più organizzazioni adottare un approccio regionale alla conformità dei dati".

[114] EUROPEAN CHAMBER OF COMMERCE IN CHINA, *European Chamber Stance On China's Data Security Law And Personal Information Protection Law*, 25/8/2021, in: https://www.europeanchamber.com.cn/en/press-releases/3367#.

KEYWORDS: China – privacy – personal information protection – data

***

Davide Clementi – Dottorando in diritto privato comparato, Università di Macerata (d.clementi1@unimc.it)