大數據背景下個人信息保護新問題研究

趙　威*

摘　要　在大數據時代，信息傳播在速度、範圍和滲透程度等方面均有質的飛躍，使得數據在流動中創造出了巨大的商業價值的同時，也將個人信息置於了更危險的環境之中。本文在厘清個人信息保護內涵，明晰個人信息與個人隱私、個人數據之間的關係的基礎上，探析個人信息保護中的利益平衡問題，具體包括個人信息保護與信息流通利用的平衡、個人信息保護與社會公共利益的平衡以及信息主體個人信息權益與企業數據財產權的平衡，另外本文也對個人信息可識別性的認定標準不明、告知同意規則失靈、自動化決策帶來隱私泄露風險等問題進行探討，並針對性地提出對策建議，以期在保障個人信息安全的同時促進數據的有效利用。

關鍵詞　個人數據　個人信息　告知同意規則　自動化決策法

一、個人信息保護的法理基礎

（一）個人信息的內涵

個人信息是指能夠單獨或與其他信息結合識別特定自然人的各種信息，但不包括經處理後喪失可識別性且無法復原的信息，即匿名化信息。由此可見，可識別性是區分個人信息的關鍵。個人信息保護以自然人的人格利益為法益，一直以來被各國立法視為隱私和個人自由的象征。[1]近年來，隨著互聯網技術的迭代升級，信息傳播在速度、範圍和滲透程度方面提質增效，也給個人信息帶來更多風險，使得大數據背景下的個人信息保護成為了各國立法研究的熱點。從權屬地位上看，《個人信息保護法》第2條規定，自然的個人信息權益受法律保護。可以發現，我國並未將其上升至民事權利的地位，而是視為一種受法律保護的民事權益。從權益內容來看，其具有弱支配性，[2]因此信息處理者處理個人信息應取得信息主體的授權同意。在完成授權後，信息主體仍有權撤回同意，或請

*　趙威，中國政法大學國際法學院教授、博士生導師。

［1］ Bo Qu, Changxu Huo, Privacy, National Security, and Internet Economy: An Explanation of China's Personal Information Protection Legislation. Frontiers L. China 15, 2020, p.342.

［2］ 參見申衛星：《數字權利體系再造：邁向隱私、信息與數據的差序格局》，載《政法論壇》2022年第3期，第98頁。

求信息處理者對其個人信息予以刪除、屏蔽，也有權保護其個人信息的真實性和完整性。但同意並不是絕對的，若符合《個人信息保護法》第13條第2項至第7項，則無須取得個人同意，原因在於信息主體所享有的該種弱支配性無法對抗涉及公共利益或為履行義務所必需的情形。

（二）個人信息與隱私權的關係

隱私權是一項國際公認的基本人權，旨在保障自然人的私人生活安寧，免受政府、公眾和其他個人的不當干預。早在1361年，英國就起草了世界上第一部隱私權法案，自此之後，隱私權在各國逐漸以法典化的形式被固定下來。而個人信息的概念則肇始於20世紀70年代，伴隨信息技術和互聯網的發展，數據在高效利用的同時也對個人隱私帶來侵犯風險，個人信息權益應運而生，旨在保障信息流通的同時保護信息主體的個人隱私不受侵犯。可以發現，個人信息的概念是IT行業蓬勃發展的產物。從這個意義上來說，隱私權比個人信息權益要古老得多。[3] 而從設立目的來看，個人信息保護從設立之初就以服務“隱私”作為主要目標，將隱私保護擴展到了個人信息處理方面，因此在很長的一段時間裏被認為是個人隱私權的一部分。[4] 但從權利本質出發，個人隱私以“私”為核心，旨在構建私人領域，主要包括私人生活安寧、私密空間、私密活動和私密信息，其並不以信息形式為必要外在要件。而個人信息以“可識別性”為核心，只要該信息能識別出特定自然人，則該信息就屬於個人信息，但不一定涉及該自然人的私密利益。由此可知，個人隱私和個人信息屬於交叉關係，而重合部分即為那些以信息形式存在的，涉及自然人私密利益的私密信息。因此，二者應采用不同的路徑進行區分保護。這種區分保護的邏輯鮮明地體現在我國的相關立法之上。具體而言，內地《民法典》首次明確地將個人信息權益視為一種法律保護的民事權益，將其與個人隱私權在權利屬性上區分開來。隨後，《個人信息保護法》也以單行法的形式擺脫了司法實踐中隱私權“包打天下”的誤區。而私密信息作為二者的交叉部分，根據內地《民法典》第1034條第2款的規定，應優先適用較高標準的隱私權的相關規定，沒有規定的，適用個人信息保護的規定，以提高對私密信息的保護力度。

（三）個人信息與個人數據的關係

隨大數據時代的到來，數據成為創造價值的新型“石油”，充實了基本生產要素的範疇。與此同時，有關數據權屬和使用的糾紛也不絕如縷，數據治理已成為網絡治理的重要內容。但實踐中個人數據與個人信息的關係一直處於混亂的狀態，甚至部分法律和部門規章在其文本中將二者進行交替使用。[5] 有學者認為，信息是數據之內在內容，數據是信息之外在形式，個人數據就是個人信息，應擇一使用。[6] 也有學者認為個人信息的範圍小於個人數據，僅包括那些能識別特定個人的數據。[7] 而筆者認為，個人信息與個人數據之間相互依托，但由於二者在權利屬性上存在差異，因此也應在保護路徑上做到彼此區分。具體而言，個人數據是表現個人信息的載體，因此在對個人數據進行利用時必須注意保護其上承載的個人信息。就權利屬性而言，個人信息權屬於人格權的範疇，公民個人信息神聖不可侵犯，對個人信息的保護，要以基於人格尊嚴的人格權路徑進行。而個人數

---

［3］ Zana Pedic, Interconnectivity and Differences of the (Information) Privacy Right and Personal Data Protection Right in the European Union, Review of Comparative Law 30, 2017, p.128.

［4］ Hill, D.G.; Data Protection: Governance, Risk Management and Compliance, CR Press, FL, USA, 2009, Chapter 1, p.1.

［5］ 參見申衛星：《數字權利體系再造：邁向隱私、信息與數據的差序格局》，載《政法論壇》2022年第3期，第92頁。

［6］ 參見程嘯：《論大數據時代的個人數據權利》，載《中國社會科學》2018年第3期，第105頁。

［7］ 參見黃國彬、張莎莎、閆鑫：《個人數據的概念範疇與基本類型研究》，載《圖書情報工作》2017年第5期，第42頁。

據則屬於財產權的客體，屬於信息主體個人所有，信息處理者只有在獲得其有效授權後才能夠處理個人數據，體現的是基於支配和利用的財產權保護路徑。數據企業也可以基於此擁有企業數據用益權，從而打破個人信息人格權益的限制，在一定範圍內對個人數據進行合法合規地有效利用，以挖掘其商業價值，這也是將個人信息和個人數據從權利屬性方面進行區分的重要意義所在。[8]

二、大數據時代個人信息保護下的利益平衡

在大數據時代，數據在承載個人隱私的同時，也通過流通和有效利用創造了不菲的經濟利益，使得個人信息不僅單純包含人格利益，還與商業利益、社會公共利益等密不可分。[9] 因此，如何實現諸多利益之間的平衡，成為了大數據時代個人信息保護的難點。

（一）個人信息保護與信息流通利用的平衡

數據在流動中創造價值，同時也將個人信息置於更危險的環境之中，信息主體和信息處理者的利益訴求也矛盾凸顯。具體而言，在雁過留痕的互聯網時代，信息主體的網絡行為形成海量數據，而“告知同意”規則的固有缺陷使得信息主體在大多數情況下沒有真正了解同意的基本內容就徑直作出授權，從而失去了對其個人信息的控制。而隨互聯網技術的迭代升級，信息傳播水平在速度和滲透程度都顯著增加，個人信息一旦泄露，影響範圍將更廣，後果也將更加嚴重。基於此，信息主體呼籲對其個人信息進行更有力的保護。而另一方面，在大數據時代，數據成為了新型石油，為企業創造了巨大的商業價值，通過收集、分析海量個人數據，其可以直觀了解用戶需求，從而對目標用戶針對性地推送個性化廣告，以提高商業效率。信息處理者也可收集個人信息建立數據庫，並進行增值加工，將數據作為“知識商品”來實現價值變現。[10] 因此，信息處理者則期盼立法能夠順暢數據的流通利用通道。

個人信息保護與信息流通利用應如何實現平衡，以歐洲和美國為代表的國家走出了兩條不同的路徑。歐盟一直以來都高度重視數據隱私，側重於保護信息主體對其個人信息的有效控制。因此，GDPR規定了嚴格的個人信息保護規則和處罰措施，並賦予其廣泛的域外效力，同時設立了數據保護官（DPO）對數據交易全過程進行監管，使得GDPR被譽為史上最嚴厲的個人數據保護法案。其帶來的後果是雖然有力保護了信息主體的個人信息自決權，但也為數據控制者和數據處理者施加了沉重的合規義務，導致歐盟在B2C領域喪失國際競爭力。[11] 與歐盟相反，美國的數據保護立法旨在保障交易市場秩序，相比於個人信息自決權，更側重於保障數據的商業利用。美國甚至不存在一部綜合的聯邦隱私立法，個人信息處理也以默示同意為一般規則。其雖然有效喚醒了數據市場的活力，但也引發了大規模的數據泄露事件，激發了美國社會對數據隱私的擔憂。[12] 由此可知，我國立法應兼顧個人信息保護和信息流通，以利益平衡為基本原則，平衡安全和發展需求，在不侵犯個人信息權益

［8］ 參見申衛星：《論數據用益權》，載《中國社會科學》2020年第11期，第128-130頁。

［9］ 參見劉金瑞：《個人信息與權利配置———個人信息自決權的反思和出路》，法律出版社2017年版，第109-119頁。

［10］ 參見範小華、周琳：《基於利益平衡視角的個人信息法律保護探析》，載《行政管理改革》2020年第3期，第75頁。

［11］ 參見方芳：《歐盟個人數據治理進展、困境及啟示》，載《德國研究》2021年第4期，第58頁。

［12］ 參見晉瑞、王玥：《美國隱私立法進展及對我國的啟示 ——以加州隱私立法為例》，載《保密科學技術》2019年第8期，第41頁。

的前提下，暢通信息處理者依法處理個人信息的商業化渠道。[13]

（二）個人信息保護與社會公共利益的平衡

個人信息不僅蘊含著豐富的商業開發價值，還與社會公共利益息息相關。具體而言，對相關的個人信息進行收集匯總能為公共政策的制定提供基礎性數據和信息原材料，從而確保公共政策更加科學精準，以提高最終實施效果。[14] 另一方面，在政府部門之間進行政務信息共享的過程中，也可能會包含公民的個人信息。在上述過程中，由於個人信息兼具私法和公法的雙重屬性，既與個人利益密切相關，又能夠成為為政府所用的信息資源，因此，個人信息保護和社會公共利益之間的矛盾在所難免。具體而言，當政府收集個人信息時，屬於《個人信息保護法》第13條第3款“為履行法定職責或者法定義務所必需”的情形，因此無需征得信息主體同意，但根據《個人信息保護法》第17條，收集個人信息的政府部門仍須對信息主體就個人信息處理事項進行真實、準確、完整地告知。同時，政務信息共享也符合《個人信息保護法》第23條向第三方提供個人信息的情形，在理論上應對信息主體進行單獨告知，但目前的政務信息共享只要求相關部門對共享清單進行公布，並未將其送達給相關信息主體本人，使得大多數信息主體對其個人信息以何種方式收集並以何種方式進行政務共享均不知情。[15] 同時，一些地方的政府數據共享條例要求共享的數據應集中存儲在統一的數據庫或大數據中心，與《個人信息保護法》第19條規定的最短必要期限也未免存在沖突。是否應將政務信息共享作為個人信息保存期限的例外情形，換言之，是否應為政務信息共享情形下個人信息的儲存期限予以一定限制，仍屬於法律空白。

目前，我國政務信息共享的相關規定仍停留在行政法規層面，且各地在具體實施時差異很大，無法有效保障在政府信息收集中處於劣勢地位的信息主體之權益。因此，建議出台專門的《政務數據共享法》，在法律層面明確規定政務信息收集中相關部門的告知義務、信息披露義務及數據存儲期限，將個人信息保護貫穿至政務信息的收集、匯總、加工、共享、刪除等整個周期之中，形成“全國一盤棋”的局面。另一方面，建議修改《個人信息保護法》的相關規定，在告知義務和信息共享方面為政務數據共享進行特殊規定，從而使《政府數據共享法》與《個人信息保護法》進行完美銜接，避免潛在的法律沖突。[16] 此外，政務數據共享也應建立異議機制，當信息主體發現相關政府部門收集的其個人信息不準確或不完整時，應有暢通的渠道進行申訴和糾正，從而保障信息主體救濟權的實現，這也是與《個人信息保護法》第46條中規定的個人信息更正補充權相對應的。最後，相關部門也應加強信息安全技術投入，確保數據中心或數據庫的穩定性和安全性，並定期進行安全評估，防止數據泄露和安全漏洞。簡言之，應以利益平衡為基本原則處理個人信息保護和社會公共利益的關係，通過立法制定明確的規範對政府部門收集並共享個人數據的行為予以約束，從而在保障個人信息安全的同時滿足政府部門對個人數據的正常合法需求，實現科學高效施政。

（三）信息主體個人信息權益與企業數據財產權的平衡

在大數據時代，數據已成為了新的生產要素，也逐漸開始向財產化路徑靠攏。[17] 內地《民法

---

［13］ 參見苗澤一：《數據交易市場構建背景下的個人信息保護研究》，載《政法論壇》2022年第6期，第61頁。

［14］ 參見王柄鑫、周恒：《我國個人信息保護與公共利益的沖突及其解決路徑》，載《哈爾濱師範大學社會科學學報》2022年第4期，第79頁。

［15］ 參見邢會強：《政務數據共享與個人信息保護》，載《行政法學研究》2023年第2期，第73頁。

［16］ 參見張繼紅：《經設計的個人信息保護機制研究》，載《法律科學》（西北政法大學學報）2022年第3期，第31頁。

［17］ 參見沈健州：《數據財產的權利架構與規則展開》，載《中國法學》2022年第4期，第93頁。

典》第127條明確將數據視為一種民事財產性權益存在，但對於數據財產權益歸屬和具體權益內容均未進行明確規定。而以個人信息作為“加工原料”的企業數據應如何確定初始權益歸屬在實踐中也一直飽受爭議，信息主體的個人信息權益也就與企業的數據財產權發生了沖突。如何平衡二者之間的關係？具體而言，可以根據數據價值的生成機制，將企業數據分為數據集合和數據產品。數據集合由原始個人數據經互聯網企業的收集、分析、加工而得，凝聚了互聯網企業的勞動投入，使得數據集合擁有了商業價值和財產價值，但同時未喪失個人數據的可識別性，其上同時承載著信息主體的人格利益和信息處理者的財產性利益，因此，對數據集合應當采取利益融合的方式進行保護。具體而言，作為數據集合的加工者，信息處理者付出了勞動和智力投入，挖掘出了數據集合的財產性價值，根據洛克的勞動賦權理論，應賦予信息處理者以“有限的財產權”。[18] 這也有利於激勵互聯網企業對數據進行加工與技術資源開發，從而創造出更多的商業價值。[19] 就權益內容而言，信息處理者有權對數據集合進行積極利用或授權他人利用，同時有權排除他人未經許可的不當使用。而這裏的“有限財產權”是指，由於數據集合同時承載著信息主體的人格利益，當個人信息權益與信息處理者的財產權益發生沖突時，應優先保護個人信息權益不受侵犯。

另一方面，與原始數據不同，數據產品通過算法等技術的進一步加工，已進行了匿名化處理，脫離了原始個人數據的可識別性，呈現出數字化、類型化的內容。因此，數據產品作為一種無形財產，其上僅承載著信息處理者的財產性利益，不再涉及個人信息的人格權內容而成為單純的信息，信息處理者對這類非識別性的衍生數據享有完整的排他的財產性權益，有權對數據產品進行控制、利用和處分。若數據產品同時符合著作權或商業秘密的構成要件，則可同時獲得知識產權、反不正當競爭制度的保護，與數據保護制度一起，構成全方位的數據利益保護體系。[20] 但另一方面，這並不意味著數據產品與個人信息毫不相關。個人數據是數據產品的主要生產原料，信息處理者在獲取和收集個人數據時，必須嚴格遵守《個人信息保護法》下的“告知同意”規則，以征得信息主體的有效同意，從而為其後續的信息處理和數據產品的製造行為奠定合法性基礎。

三、大數據時代個人信息保護的新問題

（一）個人信息可識別性的認定難點

個人信息可劃分為能單獨識別特定個人的直接可識別信息和需要與其他信息結合才能識別特定個人的間接可識別信息兩類。在司法實踐中，相較於直接可識別信息，間接可識別信息的認定具有模糊性和不確定性。具體而言，如今分布式和去中心化的計算機系統具有超強的收集、傳播和運算數據的能力，在數據集聚效應的影響下，不同來源的信息相互結合都可能產生新的信息，進而識別出特定的個人，從而使得間接可識別性的範圍變得無比寬泛。[21] 另一方面，在大數據時代，即使是經過匿名化處理的信息仍有可能保留一定的間接可識別性，使得間接可識別性信息的認定難度進一步

［18］ 參見[英]洛克：《政府論》，葉啟芳、瞿菊農譯，商務印書館1964年版，第123頁。

［19］ 參見李永明、戴敏敏：《大數據產品的權利屬性及法律保護研究》，載《浙江大學學報（人文社會科學版）》2020年第2期，第31頁。

［20］ 參見姬蕾蕾：《企業數據保護的司法困境與破局之維：類型化確權之路》，載《法學論壇》2022年第3期，第120頁。

［21］ 參見楊楠：《個人信息“可識別性”擴張之反思與限縮》，載《大連理工大學學報（社會科學版）》2021年第2期，第101頁。

加大。其原因在於我國在對匿名化進行定義時采用了絕對匿名標準，即個人信息經處理後喪失可識別性且無法復原，但該“不可識別、不可復原”的理想狀態在大數據時代的背景下很難實現。[22]目前的匿名化技術主要包括隨機化和一般化兩類。隨機化通過數據遮掩、數據替換等手段直接改變數據的屬性和真實性，從而切斷該數據與特定個人的聯系。一般化則通過大幅改變數據的規模或量級從而進行泛化。[23]而在數據聚合效應的影響下，這些經過隨機化和匿名化的數據大量結合，可以形成大型元數據集，同時在算法和分析技術的加持下很可能重新建立關聯，恢復可識別性。[24]具體而言，針對這些商業性價值較高的匿名化數據，第三方處理者可以通過數據挖掘、數據聚合等手段進行技術破解，從而將其還原為個人信息，即進行去匿名化操作，侵害信息主體個人隱私的風險也就隨之而生。[25]可以發現，在大數據時代，絕對匿名化是無法實現的，立法亟需重構間接可識別性的認定標準，並將這種由匿名化導致的識別風險考慮在內。

（二）告知同意規則的失靈

告知同意規則是個人信息處理的一般規則，即處理個人信息須獲得該信息主體的同意方可進行，其致力於保障信息主體的個人信息自決權，實現對其個人信息的有效控制。[26]但在信息爆炸的當代，告知同意規則也暴露出了諸多問題，在阻礙數據流通和利用的同時，也難以發揮其應有的制度價值。首先，《個人信息保護法》第17條詳細規定了告知內容的具體要求，實踐中為合規需要，信息處理者提供給信息主體的隱私協議往往篇幅冗長，而在大數據時代，網絡服務種類愈加多樣，信息主體所面對的隱私協議也是數不勝數，且根據《個人信息保護法》第14條的規定，當信息處理的目的、方式或信息種類發生變更時，還需重新取得同意，這些因素疊加起來無疑給信息主體造成了極大的閱讀成本，使其根本不具有足夠精力對隱私協議進行有效閱讀，且隱私協議推送的普遍化和頻繁化也在一定程度上導致信息主體產生“同意遲鈍”，甚至會選擇放棄閱讀隱私協議的具體內容而徑直做出同意與否的決定。[27]可以看出，在現有的“告知同意”規則下，信息主體難以了解其同意的內容，導致“告知同意”規則流於形式。而對信息處理者來說，“告知同意”規則不加區分的明示同意標準在一定程度上也加重了信息處理的合規成本。根據《個人信息保護法》第14條的規定，信息主體的同意應在充分知情的前提下自願、明確作出。可以發現，我國的“告知同意”規則采用的是與歐盟GDPR一致的“明示同意”標準，而不承認默示同意的效力，在所有需要處理個人信息的情形下，同意都必須以作為的方式明確作出。但由於信息主體並不具有充足的辨別風險的能力，可能會動輒對那些對風險性極小的信息處理行為作出拒絕授權的決定，特別是在信息主體是否作出授權與其所享受的服務並不相關時，大多數信息主體就更不會以作為的方式積極作出授權決定，而信息處理者則會基於此而無法有效利用該個人信息，從而對數據的商業價值開發造成阻礙。[28]

---

［22］ 參見鄭佳寧：《數據匿名化的體系規範構建》，載《政法論叢》2022年第4期，第62頁。

［23］ 參見王麗梅：《大數據視角下的個人信息匿名化規則構建》，載《雲南民族大學學報（哲學社會科學版）》2021年第5期，第145頁。

［24］ 參見李潤生：《個人信息匿名化的制度困境與優化路徑——構建“前端寬松+過程控制”規制模式之探討》，載《江淮論壇》2022年第5期，第115頁。

［25］ 參見鄭佳寧：《數據匿名化的體系規範構建》，載《政法論叢》2022年第4期，第62頁。

［26］ 參見齊愛民：《信息法原論》，武漢大學出版社2010年版，第76頁。

［27］ 參見呂炳斌：《個人信息保護的“同意”困境及其出路》，載《法商研究》2021年第2期，第89頁。

［28］ 參見[英]維克托·邁爾·舍恩伯格、[英]肯尼斯·庫克耶：《大數據時代：生活、工作與思維的大變革》，盛楊燕、周濤譯，浙江人民出版社2013年版，第197頁。

（三）自動化決策帶來的隱私泄露風险

大數據挖掘信息能力的進步為自動化決策提供了技術支持，而自動化決策的實施又是以龐大的數據量作為基礎的，這也就催生了個人數據被非法收集的風險。[29]實踐中網絡運營商往往通過置入cookie等手段對消費者的瀏覽記錄、網頁停留時間、搜索內容等信息進行追蹤和收集來進行用戶畫像，以針對性地提供商業營銷廣告。這種收集方式較為隱秘，消費者不易察覺，而大量個人數據的匯集和二次利用可能會導致用戶未披露的隱私信息被深度學習算法推斷並披露出來。具體而言，在某些情形下，信息主體不經意間的授權行為為網絡運營商提供了該信息主體基礎信息，該信息在預測性分析技術下與其他相關信息經過數據聚合和二次加工，可能會分析出該信息主體其他的隱私信息甚至是敏感信息，同時由於該種信息獲取方式是通過第三方計算所得的，因此不需要獲得信息主體同意，從而可能會在其不知情的情況下對其個人隱私造成嚴重侵犯。[30]典型的案例如美國Target案，Target是沃爾瑪旗下的零售百貨公司，其通過對消費者的購買記錄進行分析，預測出了一名未成年消費者懷孕的事實，並向該消費者家中寄送了母嬰用品的廣告和優惠券，從而遭到了該未成年消費者監護人的投訴。在該案中，若該消費者事先知道Target可以從其購買記錄中預測到其懷孕的事實，其可能就不會選擇在Target進行購物，然而事實上消費者對該懷孕預測模型是毫不知情的。因此，由於信息主體在電子商務平台上提供信息時，無法預測到該信息將會被如何分析利用以及未來預測的用途，在某些情況下，信息處理者的自動化算法和用戶畫像可能會脫離信息主體的事先預知，使其隱私信息遭到泄露。[31]然而，針對該問題，目前有關自動化決策的法律規定未能同步跟進，無法對信息主體的隱私進行有效保護。

四、大數據時代個人信息保護的法律完善路徑

（一）重構個人信息可識別性的解釋路徑

間接可識別信息的認定本身具有模糊性和不確定性，且絕對匿名化的不可實現性再次擴張了間接可識別性的外延。因此，立法不妨在明確間接可識別性內涵的基礎上，同時以信息主體的合理期待作為基本認定原則，並將匿名化信息的再次識別風險考慮在內，從而增加認定標準的全面性與靈活性。具體而言，立法應承認間接可識別性信息的回溯，即若數項信息相結合產生了可以識別出特定個人的信息，則不論是最終產生的該項信息還是在這整個識別過程中發揮作用的所有信息都應被列為個人信息的範圍，這也是對《民法典》第1034條關於間接可識別性內涵進行解釋的應有之義。在司法實踐中，法院在實際認定時，應以信息主體的合理期待為基本原則，即使所涉信息達到了匿名化標準，但只要其與其他信息相結合導致該信息被再次識別的風險超過了信息主體在信息收集階段作出授權同意時的合理預期，則就應將對該信息的處理納入個人信息保護法的調整範圍。[32]合理預

［29］ 參見孫建麗：《算法自動化決策風險的法律規制研究》，載《法治研究》2019年第4期，第110頁。

［30］ 參見徐辰燁：《從個人數據到國家數據：互聯網平台數據安全問題的升級》，載《新聞論壇》2021年第5期，第10頁。

［31］ 參見陸青：《數字時代的身份構建及其法律保障：以個人信息保護為中心的思考》，載《法學研究》2021年第5期，第18頁。

［32］ 參見孫其華：《我國間接識別個人信息規制機制的檢視與完善》，載《上海對外經貿大學學報》2022年第1期，第40頁。

期原則保障了信息主體對其個人信息的有效控制，有利於防止初期同意的後發性風險。其次，針對匿名化信息的“剩餘風險”，信息處理者作為數據紅利的主要享有者，也應對其數據產品進行的定期審查和評估，以防止匿名化數據被再次識別的可能。

（二）修正告知同意規則的制度缺陷

一方面，通過實踐可知，告知同意規則下的明示同意標準在大數據時代無法充分滿足數據流通的需要，也難以發揮保障信息主體同意自決權的應有制度價值。[33] 但另一方面，告知同意規則一直以來均是大多數國家個人信息處理的核心規則，對信息主體的知情權和對個人信息的控制權進行了有力保障，因此，對於“告知同意”規則，我們不應全盤舍棄，而應在制度框架內進行改良與完善。具體而言，可以融合歐盟和美國的實踐經驗，在個人信息處理的一般規則上與歐盟一致，采用明示同意標準，同時針對特定情形為美國式默示同意標準的適用創造條件。這兩種同意標準的適用情形可以根據信息處理行為類型的不同進行劃分，[34] 在不指向特定個人的信息處理場合，可以采用更為寬鬆的默示同意標準，信息處理者充分履行了告知義務之後，除非信息主體明確反對，否則則視為同意處理其個人信息，從而有效提高數據流動的效率；而在諸如用戶畫像等以特定個人為分析對象的信息處理場合以及涉及敏感信息的情形下，則應以保障個人信息合法權益為前提，堅持采用“明示同意”標準，在保障個人信息安全的基礎上促進數據的商業化利用。

（三）完善算法自動化決策的法律規制

由於算法具有較強的專業性和技術性，針對自動化決策帶來的隱私泄露風險，建議成立專門的算法安全委員會進行算法使用前的審查與風險評估和算法使用過程中的監督，從而全過程抑制隱私泄露等風險發生的可能。同時，網信部門也應根據算法的具體應用情形、使用範圍及可能對信息主體產生的影響等風險因素制定詳細的風險評估標準，在促使互聯網企業合規的同時，也有利於增加算法安全委員會評估活動的穩定性和規範性。[35] 此外，當自動化決策已造成實際侵權時，個人隱私受侵犯的信息主體也可以尋求算法安全委員會的幫助，由算法委員會代表受害群體統一接受設計者對算法的解釋和驗證，以明晰算法設計者的責任，及時保障信息主體的合法權益不受侵犯。[36] 另一方面，由於自動化決策受制於算法機器邏輯的影響，忽視了現實的人的主觀感受和主體地位，具有侵犯人格尊嚴的風險，因此，《個人信息保護法》第24條第3款就賦予了信息主體拒絕對其個人權益有重大影響的自動化決策的權利，但何為“重大影響”則缺少具體的判斷標準。未來，立法應對信息主體有權拒絕自動化決策的情形進行進一步細化，可以以“平衡論”為基本原則，予以有梯度的分級保護。具體而言，立法可以明確規定對信息主體生命權、自由權、人格權等基本權利或對社會公共利益造成影響的事項不得使用自動化決策。而針對可能會對信息主體權利產生消極影響或機會喪失的自動化決策，則應獲得信息主體的明確同意。至於那些不涉及價值判斷的事實性問題，由於其本身不具有侵權風險，則可以徑直適用自動化決策，而無需獲得信息主體同意，以提高信息處理的效率。[37]

---

［33］ 參見馮愷：《個人信息“選擇退出”機制的檢視和反思》，載《環球評論》2020年第4期，第151頁。

［34］ 參見呂炳斌：《個人信息權作為民事權利之證成：以知識產權為參照》，載《中國法學》2019年第4期，第61頁。

［35］ 參見宋華健：《反思與重塑：個人信息算法自動化決策的規制邏輯》，載《西北民族大學學報（哲學社會科學版）》2021年第6期，第104頁。

［36］ 參見孫建麗：《算法自動化決策風險的法律規制研究》，載《法治研究》2019年第4期，第116頁。

［37］ 參見鄭智航：《平衡論視角下個人免受自動化決策的法律保護》，載《政法論叢》2022年第4期，第102頁。

結語

作為大數據時代的新型石油，數據在流動中創造商業價值，同時也為個人信息帶來了更多風險。與以“私”為核心的個人隱私不同，個人信息的核心特征在於“可識別性”，但二者之間也存在交叉部分，即私密信息。與個人數據相比，個人信息權屬於人格權的範疇，要以基於人格尊嚴的人格權路徑進行保護，而對個人數據的保護則應采用基於支配和利用的財產權保護路徑。同時也應注意，在大數據時代，個人信息不僅單純包含人格利益，還與商業利益、社會公共利益等密不可分，應以利益權衡為原則，平衡個人信息安全和數據流通的發展需求，同時完善政務信息共享的相關立法，在保障個人信息安全的同時滿足政府部門對個人數據的正常合法需求，促使政府部門依法依規收集個人信息，以實現科學施政。另一方面，也應根據數據價值的生成機制明晰企業數據的權益歸屬，以平衡信息主體的個人信息權益與企業數據財產權的關係。同時，針對大數據時代個人信息保護出現的間接可識別性認定標準不明、告知同意規則流於形式、自動化決策帶來隱私泄露風險等新問題，立法首先應重構個人信息可識別性的解釋路徑，以信息主體的合理期待為基本原則，重視匿名化信息的剩餘風險。其次，應采用有梯度的同意標準，以提高告知同意規則的靈活性。最後，建議成立專門的算法安全委員會對自動化決策進行全程監管，同時完善信息主體對自動化決策的拒絕權，以減少隱私泄露風險。

Abstract: In the era of big data, the level of information dissemination has increased significantly in terms of speed, scope and penetration, making the flow of data create great commercial value, but also placing personal information in a more dangerous environment. On the basis of clarifying the connotation of personal information protection and the relationship between personal information, personal privacy and personal data, this paper explores the balance of interests in personal information protection, including the balance of personal information protection and information circulation and utilization, the balance of personal information protection and social public interest, and the balance of personal information rights of information subjects and data property rights of enterprises, and at the same time, this paper explores the new problems of personal information protection in the era of big data, including the unclear criteria for identifying personal information, the failure of the inform consent rules, and the risk of privacy disclosure due to automated decision-making, and propose countermeasures in order to promote the effective use of data while safeguarding the security of personal information.

Key words: Personal Data; Personal Information; Inform Consent Rules; Automated Decision-Making

（責任編輯：勾健穎）