簡介德國及歐盟關於 Profiling 的法律規範

鍾宏彬*

目錄

個資幾乎已成為現代社會日常便利的通貨，例如使用手機、刷卡消費、搭乘大眾運輸不用投幣買票等等，都必須交出或多或少的個資來交換。政府及企業掌握無數個資，一旦有機會將夠多的個資串聯在一起，加上大數據分析、機器學習、人工智慧等等高效率的電腦分析技術，便可能迅速剖繪出大量個人的個性、偏好、習慣、思維、價值觀及各個面向的能力等等，或者預測個人未來的行為傾向。更進一步，結合心理學技巧，便可能為每個人量身訂做能夠有效率地改變上述各種屬性之方法，例如更加隱微但更有力的消費誘導，這可能是「比較無傷大雅的」用途；「比較邪惡的」用途，則例如極權國家對人民做思想改造，使其打從心底效忠黨及領導人，永世不渝。

上段勾勒的**「剖繪」（Profiling）**，除了是操縱人類（無論個體或群體）的關鍵步驟，剖繪這動作本身也可能讓分析對象產生極大的被侵犯、被監視、被偷窺感或不安感等等。以自由與人權為信仰的民主國家，是否也應該保障人民不被剖繪的自由？若是，國家自我克制就夠了？或者國家也該約束人民（尤其企業）不對人類同胞做剖繪？

本文出發點是簡介德國法關於 Profiling 的規範。但德國《聯邦個人資料保護法》（BDSG）[1] 關於 Profiling 的規範是在《歐盟資料保護基本規則》（DS-GVO）[2] 的框架之內制定，依據《歐洲聯盟運作條約》（AEUV）[3] 第 288 條第 2 項：「規則具有普遍效力。它的所有部分皆有拘束力，且直接適用於會員國內」。所以必須先認識歐盟法已有那些基礎規範，以及歐盟法容許會員國做何等限度的內國調整，才能完整了解德國法關於 Profiling 的規範體系。

壹、歐盟法關於 Profiling

一、定義

《歐盟資料保護基本規則》第 4 條第 4 款：「„Profiling“ 係指以任何形式對個人資料做自動化處理，該處理涉及運用個人資料來評估一位自然人的特定人格面向，尤其是分析或預測這位自然人的工作表現、經濟狀況、健康、個人偏好、興趣、可靠性、行為、位置或移動」。

由上開條款首先可知，Profiling 是資料處理的一種。其次，Profiling 的兩個關鍵要件是「自動化處理」個人資料與「評估人格面向」。所以若是純人工處理個人資料，則就算是用來評估人格面向，亦因不符合「自動化處理」而不適用該條款。另一方面，該條款的「人格面向」實際上包山包海，透過「尤其是」（德文：insbesondere；英文：in particular）一詞，只是例示立法者所設想到需加強注意的面

向，並不排除其他面向。[4]

二、容許要件

（一）與資料處理相同規範

何時可以做 Profiling？《歐盟資料保護基本規則》前言（即立法理由）第 72 點曰：「Profiling 適用本規則有關個人資料處理之規定，例如資料處理的法律基礎及資料保護原則」。

《歐盟資料保護基本規則》第 6 條第 1 項列出資料處理（含 Profiling）的六款法律基礎：(a) 當事人同意；(b) 為了履行與資料當事人間契約之必要，或為了進行資料當事人所要求的締約準備措施之必要；(c) 為了履行法定義務；(d) 為了保護自然人生命利益之必要；(e) 為了公共利益任務或執行受託行使之公權力；以及授權最廣泛的第 (f) 款「為了追求資料控制者或第三人的合法利益，除非要求保護個人資料的資料當事人之利益、基本人權和自由構成優越利益，特別是當資料當事人為兒童時。」

（二）全自動 Profiling：原則禁止

在《歐盟資料保護基本規則》第 6 條為資料處理廣開授權大門之後，第 22 條相反地原則性禁止特定目的且特定方式的資料處理。第 22 條第 1 項曰：「若決策將對當事人產生法律效力或類似的重大影響，當事人有權不受制於基於全自動處理——包含 Profiling——的決策。」該基本規則前言第 71 點為此等決策舉例：「例如自動拒絕線上的信貸申辦，或無人類介入的線上雇傭程序。」

由《歐盟資料保護基本規則》第 22 第 1 項的「受制於」（德文：unterworfen zu werden；英文：subject to；直譯為「臣服於」）一詞可知，立法目的在於避免當事人成為資料處理的客體。若當事人必須承受資料處理的後果，卻無機會得知被處理的資料內容及處理時的評價標準，亦無機會於事後影響決策，則自動化處理程式（或其使用者）在此就如同君王，單方面決定當事人的命運，當事人因此成為資料處理的客體。[5]

理解這個立法目的之後，當能理解為何《歐盟資料保護基本規則》第 22 條第 2 項為第 1 項的原則性禁令開啟下列例外。第 2 項曰：「若決策具有下列情事，則不適用第 1 項：(a) 為了當事人與資料控制者間締結或履行契約之必要，(b) 基於對資料控制者有拘束力的歐盟法或會員國內國法，該決策被允許，且此等法律同時訂有保護當事人權利、自由及合法利益的適當措施，或者 (c) 基於當事人的明示同意。」同條第 3 項並要求：「資料控制者於第 2 項 a 款及 c 款情形，必須採取適當措施以保護當事人權利、自由及合法利益，此等措施至少應包含要求資料控制者以人工介入決策的權利，說明自身立場的權利，以及挑戰決策的權利」。質言之，以當事人的主體性、事前權

利保障和事後救濟可能性，作為例外要件的設計理念。

（三）針對特種個人資料的特別限制

針對一些特別私密或特別敏感的個人資料（「特種個人資料」），資料處理（含 Profiling）再次受到較嚴格的限制。《歐盟資料保護基本規則》第 22 條第 4 項曰：「第 2 項的決策不得以第 9 條第 1 項所稱的特種個人資料作為基礎，除非適用第 9 條第 2 項 a 款或 g 款，且採取適當措施以保護資料當事人權利、自由及合法利益。」

《歐盟資料保護基本規則》第 9 條第 1 項定義「特種個人資料」（德文：besondere Kategorien personenbezogener Daten；英文：special categories of personal data）是「可從中得知當事人之種族出身、民族出身、政治意見、宗教信仰或世界觀信仰、或工會會員身分的資料，…基因資料，生物特徵資料…，健康資料，或關於性生活或性傾向的資料。」第 9 條第 1 項原則上禁止處理這些資料。但同條第 2 項有例外規定：「下列情形不適用第 1 項：(a) 資料當事人針對該個人資料處理之一個或數個既定目的明示同意，除非歐盟法或會員國內國法禁止資料當事人以同意來廢除第 1 項的禁止。… (g) 基於歐盟法或會員國內國法，出於重大公共利益之必要，與所追求目的之間呈適當比例，且法律規定有適當措施以保護資料當事人權利、自由及合法利益。」

應注意的是，依《歐盟資料保護基本規則》第 22 條第 4 項連結第 9 條時，由於第 22 條是關於全自動資料處理（含 Profiling），限制較嚴格，所以在第 9 條第 2 項 a-j 共十款當中，只取用 a、g 兩款當作特種個人資料的例外容許要件。若是非全自動的資料處理（含 Profiling），則可完整適用十款例外。

三、義務

由於 Profiling 適用資料處理的規定，因此凡是資料控制者於資料處理時應履行之義務，從事 Profiling 時亦應遵守。以下舉兩個特別針對 Profiling 而設的義務。

（一）告知義務

資料控制者的告知義務分為被動義務和主動義務。被動義務是在當事人提出要求時履行，主動義務則是資料控制者必須在要件具備時主動履行。

《歐盟資料保護基本規則》針對第 22 條所稱「基於全自動資料處理（含 Profiling）之決策」，同時設有主動和被動告知義務。主動義務的部分：依該基本規則第 13 條第 2 項 f 款、第 14 條第 2 項 g 款及第 3 項，若資料控制者已知將進行上開決策，則應於蒐集資料時主動告知當事人此事，並告知該等全自動資料處理的邏輯、處理範圍和對當事人的影響；若資料是從其他處所蒐集，則應於取得資料後的合理期間

內，最晚不超過一個月，告知當事人上列事項。被動義務的部分：依該基本規則第 15 條第 1 項 h 款，當事人有權要求資料控制者告知是否將或已進行上開決策，若有，後者並應告知上列的邏輯、範圍和影響等事項。

（二）影響評估

《歐盟資料保護基本規則》第 35 條第 1 項規定，若資料處理方式可預見將對任何自然人的權利和自由產生重大風險，資料控制者應預做影響評估。第 2 項規定，並應針對此事諮詢資料保護政務委員（德文：der Datenschutzbeauftragte）。第 3 項 a 款規定，若涉及利用自動化資料處理做系統性且大範圍的人格面向評定——必然符合 Profiling 定義——，且此處理將成為對自然人產生法律效力或類似的重大影響之決策基礎，則第 1 項的影響評估為必須措施。——換言之，此款情形，資料控制者無主觀判斷是否「對自然人的權利和自由產生重大風險」之空間。[6]

四、小結

總體觀之，《歐盟資料保護基本規則》關於 Profiling 的規範特徵是層層疊疊的原則－例外結構，第一層原則之下有例外，此例外成為第二層的原則，在它之下又有例外（因此回到第一層原則的效果），以此類推。《歐盟資料保護基本規則》的立法精神是原則上禁止 Profiling，第 6 條第 1 項開啟此原則的例外（=允許），第 22 條第 1 項是第 6 條第 1 項的例外（=禁止），第 22 條第 2 項是同條第 1 項的例外（=允許），同條第 4 項前半句是第 2 項的例外（= 禁止），同條第 4 項後半句是前半句的例外（=允許）；最後這個第 22 條第 4 項後半句連結到第 9 條第 2 項 a 款，而該 a 款後半句又是同款前半句的例外（=禁止）。

一旦容許作資料處理，資料控制者要承擔許多義務。進行 Profiling 者，須負擔比進行其他類型的資料處理時更多之義務。進行全自動 Profiling 者，須負擔比進行一般 Profiling 時更多的義務。

貳、德國法關於 Profiling

在上述《歐盟資料保護基本規則》層層疊疊的原則－例外結構之中，凡提到「會員國內國法」的地方，例如第 22 條第 2 項 b 款，第 9 條第 2 項 a 款和 g 款，即是德國《聯邦個人資料保護法》（BDSG）[7] 可能自訂 Profiling 相關規範的空間。

一、定義

德國《聯邦個人資料保護法》在 2017 年 6 月 30 日通過的全新版之前，並無 “Profiling” 定義。[8] 這版本第 46 條第 4 款的「Profiling」定義幾乎照抄《歐盟資料保護基本規則》第 4 條第 4 款，二者的德文只有不影響文義的微量選詞差異，[9] 翻譯成中文則隻字不差。所以德國法的「Profiling」定義請直接參照《歐盟資料保護基本規則》。

二、保險給付決策使用全自動 Profiling 及特種個人資料

德國《聯邦個人資料保護法》第 37 條第 1 項針對保險契約給付相關且使用全自動資料處理的決策，設有特別規定：在保險給付的決策過程，若 (1) 當事人的給付請求被核准，或 (2) 該決策只是套用有拘束力的醫療給付條款，且資料控制者（通常即保險人）為未依請求額度全額給付的狀況設有《歐盟資料保護基本規則》第 22 條第 3 項所稱的權益保護適當措施——則除了該基本規則第 22 條第 2 項 a 款和 c 款所列例外情形得做成基於全自動資料處理（含 Profiling）的決策，「別無例外」。由形式上看，這固然是德國立法者在填充《歐盟資料保護基本規則》第 22 條第 2 項 b 款授權給會員國自行立法的空間，然而填充的結果實際上是放棄自訂其他規定。

另依德國《聯邦個人資料保護法》第 37 條第 2 項規定，做成上開基於全自動資料處理的保險給付決策時，得處理特種個人資料當中的健康資料；同樣地，資料控制者對此應設置權益保護適當措施。這屬於《歐盟資料保護基本規則》第 22 條第 4 項連結第 9 條第 2 項 g 款，授權給會員國自行立法的範圍。

三、徵信 Profiling

另一種常見的 Profiling 是日常生活中廣泛運用的徵信評分（Scoring）。徵信業者根據委託人之需求，蒐集並運用多種個人資料，計算出特定人未來做出特定行為的機率，例如履約機率，勝任特定工作的機率、瀆職機率或洩漏營業秘密之機率等等，這可能成為授信、勞動契約或經理人契約的重要前提。此等評分無疑屬於《歐盟資料保護基本規則》第 4 條第 4 款所稱的「評估自然人的特定人格面向」，所以只要評分運用到或多或少的自動化個人資料處理，便符合該條款的 Profiling 定義。[10]

依據德國《聯邦個人資料保護法》第 31 條第 1 項：「僅於下列情形容許運用有關自然人未來特定行為的機率值來作成是否與此人締結、履行或結束契約關係之決策（Scoring）：1. 遵守個人資料保護法的規定；2. 依照科學上認可的數學統計方法，可證明機率值計算過程運用的個人資料對於該特定行為機率的計算有重要意義；3. 機率值不是僅使用通訊資料計算而出；(4) 若使用通訊資料，應於機率值計算前告知當事人該資料將被如何運用；該告知應做成書面紀錄。」

四、債信 Profiling

債信評分，亦即特定人的債務履行機率（或倒債風險），是徵信評分的一種。若此人是自然人，便落於《歐盟資料保護基本規則》第 4 條第 4 款（Profiling 定義）所稱「自然人的…經濟狀況…和可靠性」概念中。因此，只要債信評分過程運用到自動化處理，便屬於該條款定義的 Profiling。[11]

德國《聯邦個人資料保護法》第 31 條第 2 項針對債信評分之運用，做了比其他類型徵信評分更嚴格的限制。依該項規定，徵信機構提供的特定自然人未來支付能力和支付意願之機率值，除了必須符合第 1 項之外，該機率值所參考的債務不履行之基礎債權尚須有下列情形之一，後續始得運用該機率值：1. 依確定判決或具有暫時執行力之判決已確認，或依民事訴訟法第 794 條具有強制執行名義；2. 依破產法第 178 條已確認，且債務人未及時提出異議；3. 債務人已明示承認；4. 已書面催告至少兩次，第一次至少是四週前，第一次催告日起曾警告過債務人會將不履行之事通知徵信機構，且債務人對債權未爭執；或者 5. 基礎契約關係的不履行額度已達可不定期終止契約之數，且有警告過債務人會將不履行之事通知徵信機構。

* 德國柏林洪堡大學（Humboldt-Universität zu Berlin）法學院博士候選人；中央研究院法律學研究所研究助理；法務部司法官學院犯罪防治研究中心兼任研究員。

1 Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), zuletzt geändert Artikel 12 des Gesetzes vom 20. November 2019 (BGBl. I S. 1626)（縮寫為 BDSG）。引用德國法律時，中譯的「條」指德文的「§」符號，「項」為德文的括號阿拉伯數字（例如 (1) = 第 1 項），「款」為德文的無括號但有附點的阿拉伯數字（例如 1. = 第 1 款）。

2 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. L 119/1. 此規則的官方德文短名為 Datenschutz-Grundverordnung（縮寫 DS-GVO），官方英文短名為 General Data Protection Regulation（縮寫 GDPR）。引用歐盟條約和法規時，中譯的「條」係指德文「Artikel」，英文「Article」。

3 Vertrag über die Arbeitsweise der Europäischen Union, ABl. C 326 vom 26.10.2012, S. 47–390.

4 *Benedikt Buchner,* Grundsätze des Datenschutzrechts, in: Tinnefeld/Buchner/Petri/Hof, Einführung in das Datenschutzrecht, 7. Aufl. 2019, S. 220 (272); *Maximilian Hermann/Rolf Schwartzmann*, Art. 4, in: DS-GVO/BDSG, 2018, Rn. 54.

5 Vgl. *Jürgen Kühling/Manuel Klar/Florian Sackmann*, Datenschutzrecht, 4. Aufl., 2018, S. 190 f.

6 *Maximilian Hermann/Rolf Schwartzmann*, Art. 4, in: DS-GVO/BDSG, 2018, Rn. 61.

7 Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), das durch Artikel 12 des Gesetzes vom 20. November 2019 (BGBl. I S. 1626) geändert worden ist.

8 Vgl. §§ 3 und 46 des Bundesdatenschutzgesetzes vom 20. Dezember 1990 (BGBl. I S. 2954).

9 《歐盟資料保護基本規則》第 4 條第 4 款：「„Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, ... 」；德國《聯邦個人資料保護法》第 46 條第 4 款：「„ Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, bei der diese Daten verwendet werden, …」。底線的幾個字是僅有差異。

10 *Benedikt Buchner*, Grundsätze des Datenschutzrechts, in: Tinnefeld/Buchner/Petri/Hof, Einführung in das Datenschutzrecht, 7. Aufl. 2019, S. 220 (272 f.); *Maximilian Hermann/Rolf Schwartzmann*, Art. 4, in: DS-GVO/BDSG, 2018, Rn. 58; *Ralf B. Abel*, Datenschutz im Credit Management, in: Behling/Abel (Hrsg.), Praxishandbuch Datenschutz im Unternehmen, 2014, S. 571 (581 f.).

11 *Benedikt Buchner*, Grundsätze des Datenschutzrechts, in: Tinnefeld/Buchner/Petri/Hof, Einführung in das Datenschutzrecht, 7. Aufl. 2019, S. 220 (272);