《高大法學論叢》

第 15 卷第 2 期（3/2020），頁 39-72

數位化、大數據和人工智慧對刑事訴訟的衝擊

葛祥林*

摘要

數位化、大數據和人工智慧等概念，雖然經常在媒體和專業文章等都被提起，但多數人並不理解，這些概念真正的涵義是什麼？其技術上與傳統分析方法究竟有何不同？然而，一旦不理解這些新的基本概念，就更不得理解，其對於刑事訴訟法的真正衝擊何在。因此，本文先行指出數位化、大數據和人工智慧的簡短定義，並且說明其如何能夠經由新的運算方法（類神經網絡等）及新的分析模式（數據剖析）在法學領域加以利用。具體言之，本文解釋為何運用傳統邏輯運算的網格式偵查（Rasterfahndung（數據對比））以及運用類神經網絡的數據剖析（profiling）形成截然不同的分析結果，使得兩者對數據的利用以及在證明上具

*德國奧斯納布呂克（Osnabrück）大學法學院教授，國立台灣大學法學博士。

投稿日期：08/07/2019；接受刊登日期：12/13/2019
責任校對：趙雨柔、李睿祥

有十分不同特徵。同時，本文追蹤相關技術如何導致刑事訴訟的基本概念轉變，乃至刑事訴訟的自我定位發生非常大的、現今逐一實現的變化。依此，歐盟法的相關法規（歐盟綱領（EU）2016/680）已經將刑事實體法的犯罪預防（Prävention）目的納入刑事訴訟法範圍，甚至將之納入偵查階段，使其在尚未進行刑事訴訟意義下的偵查之前，都已經與警察法中的風險控管概念出現。相對於此，德國刑事訴訟法仍然堅持刑事訴訟法的傳統定位，即堅持以事後壓抑（Repression）先前已發生刑事犯罪為基本立場。基於此，德國法必須調整警察法，藉此將預防風險的利益納入一個由警察法及刑事訴訟法所共建的偵查體系。

The Impact of Digitalization, Big Data and AI on Criminal Procedure

Georg Gesk **

Abstract

Although digitalization and big data are notions that are rather familiar terms in our public debate, but most people don't really understand the difference between these new techniques and more traditional ways of analysis. Therefore, it is often not clear what differences occur when these new analytical tools are applied to criminal procedure law. Therefore, this article first gives some short definitions for digitalization and big data before explaining how they can be analyzed in the realm of criminal procedure law with previously unseen tools such as neuronal networks or profiling. In concrete terms, this contribution compares investigative methods that make use of traditional logic, such as large scale data comparison （Rasterfahndung） and profiling, which makes use of techniques such as artificial neuronal networks. Due to the specifics of analytical methods applied, both utilize data in very different ways and produce very different results, lending them different potential within investigation and evidential value. This leads to changes in the possibilities and aims of criminal procedure law, thus redefining

** Professor, Department of law, University of Osnabrück. Ph.D. in Law, National Taiwan University.

scope and aims of investigation. Due to these changes, EU law （guideline（EU）2016/680） integrates prevention of crimes into the realm of criminal procedure, it even introduces prevention as a goal for investigation. On the other side, we can see how i.e. German criminal procedure law keeps up with the basic concept of repression as core value of criminal law, thus not allowing for investigation prior to the suspicion that a crime already happened. Therefore German law takes another path and combines police law and criminal procedure law in a very new fashion, allowing both laws to form a common investigative cluster.

數位化、大數據和人工智慧對刑事訴訟的衝擊

葛祥林

目錄

關鍵字：類神經網絡、數據剖析、歐盟法規範、警察法、刑事訴訟法、偵查犯罪

Keywords: Artificial neuronal network, profiling, EU law, police law, criminal procedure law, investigation of crime

壹、引言

從適應自己的環境到塑造自己的環境，人類經過很多的發明。其中，尤其以文字及機械等二者，使得人與其環境發生根本性的變化。文字導致人的主觀意思可以獨立存在，即可以恆久存在於人間，不受人生命消逝的影響，使得人的集體記憶以客觀的方式存在與發展。機械導致人的力量超越個人的力量，使得人類能夠經由能源及物質之使喚，而徹底地改變自己於環境中的處境。

經由記號而傳達某種意思，在過去幾十年又進入了新的紀元：經過數位化及類神經網絡（künstliches neuronales Netz）[1]等一系列的發明，人工智慧取得自行學習的能力[2]。若結合近幾年人工智慧以及機械等不同層次的進步，就可以想像，未來人類能夠處理的問題以及能夠製造的產品，又出現一個前所未有的空間[3]。甚至人要全面掌控生物的基因，並且依此知識創造新的生物，或改變自己的生物未來，都有可能。

在此不知是禍是福的轉折點上，我們已經可以看到，新的技術層次不僅衝擊自然科學或哲學等領域，同時也改變整體社會的全面運轉。隨著此社會運轉的變遷，規範該社會運轉的法律也不

[1] 雖然 künstliches neuronales Netz 一概念，原則上以神經系統為理念源頭（即以神經細胞與神經細胞間的連接方式為最初模型），但不管是中國大陸或台灣，多數文獻以人工神經網絡（大陸）或類神經網絡為譯稱，並且依此表現其與自然界神經系統的差異性。本文所採取的譯稱為類神經網絡。

[2] 參看 Rudolf Kruse et. al., COMPUTATIONAL INTELLIGENCE,157-160 (2nd ed. 2016).

[3] 參看 Klaus Mainzer, Künstliche Intelligenz – Wann übernehmen die Maschinen?, 2. Aufl., 2019, S. 163 ff.

可能置身事外，反而處處受到來自相關變遷的壓力與牽動。因此，本文希望指出在刑事訴訟領域，現行法已出現何種變化，數位化、大數據及類神經網絡等技術對刑事訴訟的衝擊何在。為此，以下簡短指出，本文對相關技術的工作定義，之後以歐盟刑事訴訟中個資保護綱領（（EU）2016/680）及德國刑事訴訟法近幾年之相應（不予）修正加以說明，刑事訴訟法已採納哪些變遷。同時指出哪些變遷，雖然在現實中已發生，但目前僅出現於警察法，且由此牽動刑事訴訟要否進行偵查的決議，卻未出現於刑事訴訟法本身。

貳、數位化、大數據與類神經網絡的工作定義

人類在過去幾千年多次創造可表達特定意思的符號系統，如文字、音訊等。然而，人類於二十世紀才發展出以數位化為基礎的符號系統，即開始運用一個可同步以電子處理器等工具和技術來處理任何訊號。為此，所謂類比訊號（analoges Signal）必須轉換成以零（0）和一（I）為基本單元的電子二元訊號（binäres Signal）。後者可輸入電腦等處理系統，並且藉此進行特殊運算過程。當然，由於人類無法直接理解二元訊號，所以經常預設雙向轉換訊號類別的系統，即一邊使類比式訊號轉變成二元訊號，使之可輸入符合形式邏輯等的運算系統，另一邊使電子的二元訊號可「還原」成類比式訊號[4]。依此，本文所指的數位化（Digitalisierung）概念，係指此類比式訊號轉換成二元訊號的過程。當然，將不同範疇、不同性質的訊號能夠轉換成一個符合相同格式及相同分析模式的二元訊號，是後續進一步處理的十分重

[4] 參看 Eckart Zitzler, Dem Computer ins Hirn geschaut, 1. Aufl., 2017, S.155.

要的條件。

經由數位化而形成的個別資訊，或許屬於為特定目的而搜尋的資訊，所以形成一組從一開始就結構化的資訊群或資料庫。然而，尤其是個人在網路上的活動，經常形成非結構化或半結構化的資訊組（information cluster）[5]。此不同性質的資訊組，可以被納入特定數據分析系統的矩陣（matrix），並且同時被分析。依此，數據分析的範疇可大量擴展：分析者能夠經由所謂數據剖析（profiling）加以（1）整合、（2）比對、（3）分析以及（4）重新個別化相關資訊。換言之，媒體上所謂大數據（big data）的概念，其重點並不在數據的靜態收集，反而在大量數據得以動態分析的可能。易言之，大數據的創新與重要性，在於其分析上的價值：大量不同來源及不同性質的資訊被特徵化和分析。相關分析在現代經濟已經無處不在，無論是全球性企業，如谷歌、蘋果或華為，或德國鄉下提升藥物供應和醫療品質的藥房 2.0（Apotheke 2.0）計畫等[6]，無一不適用相關技術，即整合來自不同末端、不同使用者、不同處理系統、具不同結構化程度等基本性質大不相同的資訊，並且分析之以及藉此提出個人使用、個人消費、個人健康等等個別化結論。

人工智慧，尤其是類神經網絡在經由數位化、大數據的數據

[5] Olivier Heuberger-Götsch, Der Wert von Daten aus juristischer Sicht am Beispiel des Profiling, in Fasel/Meier (Hrsg.), Big Data: Grundlagen, Systeme und Nutzungspotentiale, 2016, S. 88 f.

[6] 有關數位化服務對鄉間醫療及藥物等供應之保障與提升,參看例如 Gesundheitsregion EUREGIO, Projektzuschlag Apotheke 2.0: Vor Ort und doch digital? Gesundheitsregion EUREGIO erforscht mit Universität Osnabrück digitale Technologien in Apotheken, abrufbar unter https://www.gesundheitsregion-euregio.eu/apotheke-2-0-vor-ort-und-doch-digital-gesundheitsregion-euregio-erforscht-mit-universitaet-osnabrueck-digitale-technologien-in-apotheken/, （Letzter Abruf: 11/12/2018）.

剖析等之後，不僅可以經由類似於人的神經系統中細胞與細胞之間的互動而剖析特定命題，甚至可以基於機械邏輯而進行學習、推理、預測等[7]。運算系統在此所適用的，並不是單向的傳統形式邏輯，而是大量運用或然率、臆測與自行糾正之前的推測過程等步驟，使相關推算結果以相對高的或然率提供正確的答案。因此，系統可以依過去所搜尋的資訊，獨立學習[8]。假如想理解傳統運算系統與現代類神經網絡等在現實上有何不同，可比較德國聯邦刑警局（Bundeskriminalamt, BKA）在 1970 年代所發展出來的「網格式偵查」（Rasterfahndung）以及漢堡警察（Polizei Hamburg）在 G20 暴動後所運用的數據剖析（profiling）技術等不同偵查方式。就網格式偵查而言，分析者所運用的數據分析方法屬於傳統形式邏輯的單向是非邏輯。換言之，資訊學者在分析前所擬的分析架構全然依程式而運作：其結果之出現與否，屬於一種必然的現象。德國刑事訴訟法第 98a 條關於網格式偵查的規定的立法背景，尤其反應 1970、1980 年代相關數據分析的革新。就數據剖析而言，其在分析上所運用的，大部分屬於類神經網絡或相似運算方式，即大量利用不同程度的或然率。如此的分析所形成的結果，並沒有一種百分之百的必然性，僅在一定機率上屬於正確。至於何訊息究竟在類神經網絡如何被評價，設計該系統者無從得知。相關系統有如美國再犯評估的指南針（Compas）系統[9]；也有如德國刑事訴訟法第 100g 條關於聯絡資訊（Verkehrsdaten）偵查規定的背後操作與分析系統：除非運用

[7] 認為預測屬於類神經網絡典型功能者，參看例如 Andreas Kroll, Computational Intelligence: Eine Einführung in Probleme, Methoden und technische Anwendungen, 1. Aufl., 2013, S. 224 f.

[8] Ebd., S. 273.

[9] 有關指南針系統及該系統對個別因素的評價不明，參看 Brief for the United States as Amicus Curiae, US Supreme Court 16-6387.

相關預測性分析，否則不可能有效達到該條第 1 項所要求的「對犯罪嫌疑人所在地之調查」。為此，系統必須依高度或然率提出相關預測，即不可能提出單一的必然結果。換言之，分析系統似乎必然而運用類神經網絡等的運算方式，否則無法提供如此的預測。若查相關系統起源，則經常看到警務系統為有效分配資源而發展出相關預測性分析軟體[10]。

由此得知，上述三種資訊科學現象的整合（即數位化、結構化與非結構化資訊的整合、經由或然率之運用而預測未來現象）早已變成了現實。個別現象並非相互獨立而存在，反而形成越來越「智慧」（intelligent）的人工智慧系統。當然，究竟何謂「智慧」，在心理學似乎沒有公認的定論[11]。然而，由相關文獻仍可大致獲得智慧此一概念的幾項主要特質。據此，智慧的主要要素包括：（一）基於觀察而針對特定問題決定：何謂正確選擇或何謂正確回應；（二）在具體行為層次，不僅可以挑選正確答案，也可以確實進行相關選擇，並且依據該行為結果評價，原來的行為選擇有無後續最佳化的可能或最佳化的必要。基於此，（三）智慧的系統必然實現某種經驗累積。假如系統得以分享相關經驗累積，則能夠超越個人（或個別系統）的經歷，形成特定群體、學科、社會等的經驗累積，即形成所謂知識與文化認知等。假如挑選問題的框架設好，資訊系統能夠進行大量的、快速的答案篩選，也可以在一定程度反饋，其所挑選的答案有無最佳化可能。惟，由於資訊系統目前無法自行挑選與鎖定特定問題的框架，並對此問題框架發展出正確分析及答覆的模式，所以資訊科學中幾乎沒有人敢概括性論及資訊處理系統具有「智慧」（intelligent）

[10] The Guardian, Predicting Crime – LAPD-Style, 25/06/2014.
[11] Uwe Tewes/ Klaus Wildgrube, Psychologie-Lexikon, 2. Aufl., 2016, S. 180 ff.

的特質。雖然如此，資訊科學仍然在越來越多相關文獻中論及「資訊處理性智慧」（computational intelligence）[12]或「智慧基礎設施」（intelligente Infrastruktur）[13]等辭。意思是說，工程師只要設定好適用範圍有關的參數，系統就可以在此範圍內依所預設參數自行選擇相應操作模式，使該系統呈現進化（論）規則與發展現象。換言之，資訊系統能夠針對特定問題自行「最佳化」（Optimierung）系統本身的相關行為舉止和運算規則。如此的類神經網絡與我們一般所指的智慧概念已相差不遠，並且可預期相關系統在不久後的未來獲得「智慧」累積知識的能力[14]。雖然人工智慧尚未整體超越人本身的思考能力，但相關資訊學者早已提出警告，並且預期大約 2045 年間，類神經網絡等人工智慧將超越人類本身的智慧，即形成人小機器大的局面[15]。甚至已有資訊學者認為，人腦必須與電腦相結合，否則無從繼續同時利用與控制相關人工智慧系統[16]。如此的發展也使得部分刑法學者現今已預測，刑法將來必然需接受電子人格（e-personality）[17]可成為

[12] 依 Rudolf Kruse et. al.所言，人工智慧領域中之「聰明行為舉止」（intelligent behavior）的最根本的要件在於經物理結構而可操作信號（Symbol）及信號結構（Symbolstruktur）的能力；換言之，系統本身不必辨認，何謂信號，但對於已知信號及已知信號結構可進行有效的、有意義的調整；參看 Rudolf Kruse et. al., *supra* note 2, at 8.

[13] Klaus Mainzer, a.a.O.(Fn. 3), S. 169 ff.

[14] 有關系統選擇進化論與最佳化等現象，參看 Rudolf Kruse et. al., *supra* note 2, at 158-161.

[15] Ray Kurzweil, THE SINGULARITY IS NEAR: WHEN HUMANS TRANSCEND BIOLOGY, S. 136, 260, (1st ed. 2005).

[16] 小羿，馬斯克揭秘 Neuralink: 親任 CEO 用腦機防止人類淪為奴隸，https://www.zhihu.com/tardis/sogou/art/26501654,（最後瀏覽日：09/09/2019）.

[17] 歐盟法關於電子人格的現行規範，參看 P8_TA（2017）0051, European Parliament resolution of 16. Feb. 2017 with recommendation to the Commission on Civil Law Rules on Robotics（2015/2103（INL））, 尤其參看第 59 f 條。.

刑事制裁的主體，以免人受罰，但獨立支配資源與實質決定實務發展的資訊系統反而無責任等不合理現象。既然如此的現實都已經局部實現[18]，相關問題並不是「科幻小說」（science fiction），反而有迅速規範的必要。當學者主張，人工智慧系統應被賦予電子人格，並成為（刑）法規範可獨立被制裁的主體，有其合理性以及其必然性[19]。

參、數位化偵查與個資保護的憲法衝突

到目前為止，我們在現行刑事法範圍中尚未看到如此徹底的、牽涉到刑事主體的典範轉換。可是，數位化與大數據等概念早已改變傳統刑事追訴的方法及其相應規範。尤其因為大數據在資訊處理運算中通常不純然由個案出發，反而由大量資訊中尋找其與案情有關的個案資訊，所以調整如「犯罪嫌疑」（Tatverdacht）等基本概念。具體言之，以往的傳統偵查，由個案及與個案證據所形成的個別線索出發，並且依此具體犯罪嫌疑尋找具體的犯罪嫌疑人。雖然如此的方法或許也形成好幾個可能的線索，然後去除被認定不相干的嫌疑人[20]，但其仍然以個別資

[18] 關於工業 4.0 等現代生產模式中，資訊系統如何獨立簽訂契約，並且由此形成何責任歸屬問題，參看例如 Christoph Mehinger, Industrie 4.0 und AGB-Rechte, Vortrag, Osnabrück: CUR-AGB-Recht im unternehmerischen Rechtsverkehr, 30.1.2019.

[19] Janique Brüning, Künstliche Intelligenz und Strafrecht – Zur Strafbarkeit sogenannter elektronischer Personen, in Gesk （Hrsg.）, Digitalisierung und Strafrecht. Rechtsvergleich Deutschland - China , 2020（in print）.

[20] 舉例言之，在 Oetker 的綁架勒贖案件中，偵查單位原先有了高達 1,000 個犯罪線索，但後來認定，其中只有一個嫌疑人是真正的犯罪人，所以起訴之。聯邦憲法法院後來認定，該案未予審理所謂「線索檔案」（Spurenakten），並不違背法院職權調查原則，也不違背憲法中的正當程序原則；參看 BVerfG 2 BvR 864/81 （12/01/1983）.

訊及個別嫌疑人為出發點。大量數據的運用，越來越容易使得分析系統首先讓所有民眾的資訊當作母數，然後在潛在嫌疑人的大眾中找出真正的「嫌疑人」。早在德國極左恐怖主義經常攻擊西德政經界重要人物時，傳統由個別嫌疑出發的模式已出現巨大變化：由於警方不知，犯罪嫌疑人為何人，但似乎敢斷定，犯罪嫌疑人以假名承租某大都市的公寓，所以將該都市中的所有承租人資料與其他官方資料（如出生登記、駕照等）加以對比，且依此去除不可能為嫌疑人的人群。換言之，警方首先以特定嫌疑對特定群體進行偵查。易言之，警方將任何屬於該群體的成員視為「潛在嫌疑人」（potentieller Täter）或為「可能嫌疑人」（möglicher Täter）。若不僅看承租人的群體，同時也看所對比的資料（戶政機關的登記記錄、疾病保險記錄、駕駛執照記錄等等），則看到超越一整個大都市居民的國民都被當作偵查對像。德國刑法學者批評此現象，其中最重要的批判觀點，就是將一般民眾置於「概括嫌疑」（Generalverdacht）的思維，即以一般民眾為偵查對像，所以將一般民眾當成犯罪嫌疑人。此偵查方法後來被稱「負面網格式偵查」（negative Rasterfahndung）[21]。可見，在一定條件之下，德國刑事偵查由此以來就肯定，雖然偵查單位知道，具體犯罪嫌疑人的人數極少，但為了確認該嫌疑人為何人，仍然可以將社會大眾當作非特定嫌疑人的偵查對像。依此，何為犯罪嫌疑？何人的個人資料成為犯罪偵查必然所搜查的客體？諸如此類的問題，都出現非常大的變化。當年的搜查方法還停留在單向設定的形式邏輯層次、甚至部分必須以人工方式加

[21] 德國刑事訴訟法於 1992 年 7 月 15 日經「反組織犯罪法」將網格式偵查手段納入訴訟法的隱藏性偵查（verdeckte Ermittlungen）的強制處分（參看刑事訴訟法第 98a（網格式偵查的方法和要件等規範定義）及 98b（網格式偵查的法定程序）等條）。

以進行，但已經干涉無數非犯罪者的個資[22]。因此，網格式偵查有無侵犯憲法所保障的一般人格權（Persönlichkeitsrecht），尤其有無侵犯資訊自主權（Recht auf informationelle Selbstbestimmung）[23]，部分學者原本就有疑慮。惟，德國聯邦憲法法院（Bundesverfassungsgericht, BVerfG）並沒有宣告德國刑事訴訟法第 98a 條違憲，甚至將該條規定當作審查類似偵查行為合憲性的標準[24]。其中的主要理由在於比例原則的維護：國家干涉個資，以公眾安全等受高度威脅為由。聯邦憲法法院認定，刑事訴訟法的現行規定高度反應此比例原則的考量；反過來講，聯邦憲法法院甚至以刑事訴訟法第 98a 條的基本框架為由而批判過例如北萊恩・威斯法利亞警察法第 31 條的規定，並宣告後者部分違憲。憲法法院在此案件中所批評的是相關規定對危害程度的規範不足[25]，使之無從反應比例原則的考量。由此得知，基本權與運用大數據的數位化偵查方式似乎必然形成憲法上一定程度的衝突面。

---

[22] 德國刑警局如何於 1979 年發展所謂網格式偵查模式，參看德國聯邦刑警局前局長 Horst Herold 的訪問稿，n.a., Die Position der RAF hat sich verbessert, in: Der Spiegel, Nr. 37 （1986）, S. 49. 38-61.

[23] 資訊自主權，德國憲法（基本法）無明文規範，但由德國聯邦憲法法院於其有名的「人口普查判決」（Volkszählungsurteil）中（BVerfG 1 BvR 518/02（04/04/2006））肯定資訊自主權以來，德國法學界皆高度肯定此概念，並且由此來批評以大眾為偵查對像的偵查方法；參看 Di Fabio, in Maunz/Dürig, Grundgesetz – Kommentar, 88. Aufl., 2019, Rn. 173.

[24] 德國聯邦憲法法院甚至依刑事訴訟法第 98a 條的實質及程序等要件將其他類似偵查行為加以評價，比較 BVerfG 2 BvR 1372/07, 2 BvR 1745/07 （17/02/2009）.

[25] 依該聯邦憲法法院的裁定，警察所進行的網格式偵查，除非有重大法益受到具體威脅，否則不得為之。法院在此所指出的具體理由，主要基於對該院由基本法第 2 條第 1 項及第 1 條第 1 項所形成的個人資訊自我控制權（Recht auf informationelle Selbstbestimmung）的新興基本權；參看 BVerfG 1 BvR 518/02（04/04/2006）.

此問題不僅是德國立法者應重視的議題，同時也變成歐盟立法所關注的焦點。既然歐盟早已推動刑事偵查趨於統合的情勢，刑事偵查中所干涉的基本權利，也應該獲得不同歐盟國家的相等保護，使訴訟手段可以順利跨境執行，且不會因不同國家對基本權利保護的程度不一而遭受額外障礙[26]。依此，歐盟法及德國刑事訴訟法皆提出相應實質及程序等多面要求。

肆、有關刑事追訴中個資保護的歐盟綱領（EU）2016/680

就歐洲聯盟（Europäische Union，簡稱歐盟 EU）及其前身的歐洲共同體（Europäische Gemeinschaft，簡稱歐體 EG）而言，很早已經開始注意個資在刑事追訴中的重要性以及刑事偵查與人權保障在個資保護範圍中的緊張關係。就人權而言，例如歐盟綱領（EU）2018/680 於立法理由（1）明文指出，「個人資訊在處理中的保護屬於基本權利。依歐盟人權宣言第 8 條第 1 項以及依歐盟運作條約第 16 條第 1 項等定，任何人都享有個人資訊保護的權利」。既然個資保護屬於基本權利，限制該基本權利需經過個人同意，或基於明定的法律依據。後者不僅要法律明定，另還要符合比例原則，以免發生不當擴充等現象。

在此之前，早在歐盟尚未形成時，歐洲共同體於 1995 年 10 月 24 日通過 95/46/EG 的綱領[27]。該綱領原本僅規範歐洲共同體法一般適用範圍中的個資保護；由於刑法本身並不屬於歐體立法

[26] 有關歐洲刑事訴訟統合的跡象，參看 Georg Gesk, Transnationale Strukturen im Strafprozessrecht, in Gesk/ Sinn （Hrsg.）, Organisierte Kriminalität und Terrorismus, Göttingen: Vandenhoek & Ruprecht, 2019, S. 239 ff.

[27] ABl L 281, 23.11.1995, 31.

權限的範圍（即立法範圍），所以相關綱領規範根本不適用於刑事追訴等事項。然而，由於歐盟面臨歐洲漸進統合的現實，同時面臨犯罪的國際化趨勢等，所以不得不應對此一趨勢。因此，刑事訴訟法的各個制度也同樣出現日趨明顯地相互協調與統合的現象[28]。在追求此目標時，歐洲議會及歐盟委員會於 2008 年 11 月 27 日通過框架決議 2008/977/JI（Rahmenbeschluss 2008/977/JI），且依此專門規範警務與刑事司法等機構的跨國互助。該框架決議也部分規範跨境偵查等措施，但在整體上並不符合刑事訴訟的歐洲化和現代資訊社會等多項需求。因此，歐盟於 2016 年 4 月 27 日重新頒布 Richtlinie（EU）2016/680 的綱領[29]，且同時決定取消原來的 2008/977/JI 框架決議。

因（EU）2016/680 僅屬於綱領規範，所以並沒有如同一般性歐盟個資保護令（Verordnung（EU）2018/679 即所謂 Datenschutzgrundverordnung（個資保護基本命令））在各個會員國法規範中的直接拘束力。相反，（EU）2016/680 的綱領需經過歐盟各個會員國的立法，才可能發揮拘束力。依該綱領第 63 條第 1 項，會員國需在 2018 年 5 月 6 日前將該綱領以普通法的方式納入各自的內國法。德國為此內國法化工程也就進行過相應立法；聯邦議會於 2017 年 6 月 30 日通過所謂「資訊保護法因應歐盟命令（EU）2016/679 及歐盟綱領（EU）2016/680 法案」（Gesetz zur Anpassung des Datenschutzrechts an die Verordnung（EU）2016/679 und zur Umsetzung der Richtlinie（EU）

[28] 參看 Georg Gesk, a.a.O.（Fn. 26）, S. 241 ff.

[29] 似乎同時，歐盟以命令的方式頒布 Verordnung（EU）2016/679。對歐盟的各個會員國而言，該命令直接具有拘束力；換言之，一般內國法直接受到歐盟命令的拘束；雖然如此，德國的立法者仍然將該命令內國法化，即依該命令進行對個資保護法等的修正。

2016/680）。之後，德國議會另擬草第二資訊保護法的因應法案；該法案於 2019 年 6 月 27 日由聯邦議會原則通過[30]，惟聯邦參議會（Bundesrat）於 2019 年 08 月 30 日決定許多修正[31]，使整個法案的立法程序尚未完成。

歐盟綱領（EU）2016/680 在第 3 條第 1 款及第 4 款的立法者定義中提出「有關個人的資訊」（personenbezogene Daten）及「數據剖析」（profiling）等概念。在此應注意，既然綱領（EU）2016/680 直接規範動態的個人化數據剖析問題，就沒有必要另行討論靜態的大數據概念。與此類似，該歐盟綱領並不討論概括化的、與刑事訴訟關聯性並不明確的概念，所以不討論例如人工智慧的概念。雖然如此，但綱領仍然討論基於人工智慧運用的具體偵查行為，如綱領第 11 條規範個案中自動化作出決議（automatisierte Entscheidungsfindung im Einzelfall）的問題。換言之，當人工智慧經由個人化數據剖析在刑事偵查中指出行動方案時，則不得由資訊處理系統獨立作出相關決議，而是需偵查機關決定依此數據剖析所得來的具體方案，諸如：刑事司法的公權力機關是否採取行動？應採取何種行動？可見，人工智慧系統可以對既有資訊進行分析，然後預測未來發展，故而提出行動建議。然而，最初架設分析架構以及最後作出行動決議，都不在數

[30] 原草案參看：Gesetzentwurf der Bundesregierung, Beschluss des Bundestages zum Zweiten Gesetz zur Anpassung des Datenschutzrechts an die Verordnung （EU） 2016/679 und zur Umsetzung der Richtlinie （EU） 2016/680, abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2018/dsanpug.pdf?__blob=publicationFile&v=2 (Letzter Abruf: 12/18/2019)；聯邦議會之有關決議參看：Deutscher bundestag, Bundestag stimmt zwei Gesetzen zum Datenschutzrecht zu, abrufbar unter https://www.bundestag.de/dokumente/textarchiv/2019/kw26-de-datenschutz-649218 (Letzter Abruf: 09/06/2019).

[31] Bundesratsdrucksache 380/19 （30.8.2019）.

據剖析自行處理的範圍內。尤其警察及刑事司法等機構究竟要基於分析結果採取何種行動，不可能也不應該由運算系統以自動化方式來進行。意即整個分析的事先理解、基本分析架構以及後續的具體行動等，皆不可由人工智慧系統來主宰，而需由檢警等權力機關加以決定和具體安排。系統尤其不得單獨決定未來的偵查行動方案。

就數據剖析而言，歐盟綱領（EU）2016/680 原則允許刑事訴訟的偵查機關進行如此的新型偵查措施，僅在特殊情況之下，綱領才例外禁止或限制之。首先，綱領的立法理由（38）主張，當數據剖析使得個人遭到歧視性待遇時，則應依歐洲人權宣言第 21 條及第 52 條加以禁止之。可見，除了一般性資訊自主權之外，尤其數據剖析的資訊技術另牽涉到平等原則，即牽涉到其他基本權利。歐盟立法者不僅理解到此根本性問題，同時也試圖讓若干刑事偵查制度與人權規範相符與相容。

其次，綱領的立法理由（51）又指出，（個人化）數據剖析具有傷害個人權利與自由的風險。雖然該規定僅屬於立法理由，但其仍然構成一個重要的立法定義：依該理由之敘述，由數據剖析所形成的風險與損害，涵蓋三種不同面向，即包括生理上的、物質上的和精神上的損害。顯而易見，由於歐盟綱領需同時符合不同法系的法律體系，所以在損害概念上，不能假設各個會員國有關損害概念的法規範已徹底統合，甚至不能期待各個會員國現行法已具備共同的、明晰的概念。因此，相關概念所涵蓋的範圍有多大，反而需由歐盟的權威機構自行提出明文定義，使該定義得以適用於任何歐盟國家與法系。

雖然歐盟綱領對各個會員國僅發揮間接的拘束力，即必須經各國立法，才可能將該綱領的實質內容納入各國法規範，但在此還需注意綱領內容的二分法：大約一半屬於立法理由，大約另一

半屬於綱領條文本身。應予內國法化的，是狹義的條文。然，立法理由同時減少對抽象條文的理解困難，即協助各國立法者，且使各國司法得以相互一致地解釋相關條文。其次，由於立法理由直接指出綱領與歐盟人權法治的緊張關係，並且要求在此緊張關係中應採取何解釋及制度選擇，所以當然也成為歐洲人權法治的重要參考依據。因此，假如德國聯邦法院的刑事庭必須考慮，德國相應規範有無合乎歐洲（人權）法時，該法院當然需參考相關立法理由。與此相反，假如某會員國不想參考相關制度時，則很可能將來在歐洲人權法院遭到批評。因此，為了避免相關立法將來在歐洲或在各個會員國的層次被宣告違憲，則應該將歐盟綱領於立法理由中所表達的制度考量納入立法，並且依此調整各國的刑事訴訟體系。

伍、資訊保護法因應歐盟命令（EU）2016/679 及歐盟綱領（EU）2016/680 法案

如上文所述，為了因應歐盟命令（EU）2016/679 及歐盟綱領（EU）2016/680 等歐盟層次的法規範，德國聯邦議會於 2017 年 6 月 30 日通過修正法案。該修正法案主要調整原先於 1990 年 12 月 20 日所制定的聯邦資訊保護法（Bundesdatenschutzgesetz, BDSG）。為了因應歐盟綱領（EU）2016/680 的新規定，該法一方面在一般性規定為刑事追訴中的資訊處理設置除外條款（第 1 條第 7、8 項），另一方面增設第三部「依歐盟綱領（EU）2016/680 第 1 條第 1 項之目的而處理資訊的規定」（Bestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 1 Absatz 1 der Richtlinie（EU）2016/680）。其中第一章「有關處理個人資訊的適用範圍、概念認定與基本原則」

（Anwendungsbereich, Begriffsbestimmungen und allgemeine Grundsätze für die Verarbeitung personenbezogener Daten）借用歐盟綱領的相關概念，尤其於第 46 條第 4 款規定，「『數據剖析』係指個人有關資訊的自動化處理，且在此處理中適用個人資訊來評價有關自然人的個人事項，尤其分析和預測其工作表現、經濟狀況、健康、個人喜好、興趣、可信度、行為舉止、所在地、空間移動等」。此定義全然重複歐盟綱領第 3 條第 4 款的定義，使歐盟及德國等規範在這點上完全相符。該定義所指出的個人有關資訊的立法定義，同樣在歐盟綱領第 3 條第 1 款以及在德國資訊保護法第 46 條第 1 款完全一致。德國的資訊保護法在其第 54 條第 3 項也納入綱領中立法理由（38）的人權考量，因而禁止任何具歧視性效果的數據剖析。

不同於歐盟綱領，德國資訊保護法第 70 條要求，任何個資處理行為應予記錄和列冊。相關責任由刑事追訴機關的主管來承擔。依該規定，相關記錄相當詳細，即應指出負責相關處理行為的人員、處理行為的目的、已轉送資訊或即將轉送資訊的對象、受影響人員及所干涉的資訊等；其中，第 1 項第 5 款也明文要求，假如進行數據剖析，則需記錄之。

除此之外，資訊保護法第 71 條另建立起一個新原則：本人建議稱之「資訊極簡原則」（Informationsminimalismusprinzip）。具體言之，設計若干處理資訊系統者，必須在設計中事先考慮，如何經由最少量的個人資訊而達到處理資訊系統所追求的目標；資訊設計者同時必須考慮到，相關處理系統與處理行為對所影響的法益造成多大的風險。依此，具有個人資訊保護義務的人有兩者：資訊處理系統的設計人以及其使用人。其次，系統設計人還需考慮到相關風險本身、實現該風險的機率以及造成此風險的必要性。換言之，在規劃與

設計若干系統時，系統設計人應予注意的事項超越一般公法上的比例原則，因為其應注意事項不僅限於實質的有利與不利影響，同時也包括由此所形成的潛在利益與不利益，即其中的機會與風險。德國的司法將來如何審查該注意義務？是否會因設計人未注意風險，或因注意風險不當而認定相關系統不合資訊時代的比例原則？此種種問題，目前尚無明確的答案，且資訊學者私底下認為，此原則不可能予以貫徹。因此，司法有無可能將來依此標準加以審查相關系統，並且依此認定系統設計者侵犯資訊背後主體的人格，目前言之過早。唯一可以肯定的，就是資訊保護法出現如此的概念和訴求，所以形成一種完全新的發展框架。

由於人工智慧系統不僅分析過去所發生的事宜，同時有預測未來事宜的功能，所以資訊保護法第 72 條所列舉的受影響人明顯超乎傳統刑事訴訟的範圍：該規定區分五種受個人資訊處理影響的人：

（1）具過去犯罪之具體嫌疑的人；
（2）具未來犯罪之具體嫌疑的人；
（3）受有罪判決的人；
（4）犯罪被害人或因具體事項指向特定人為犯罪被害人；
（5）其他人，如證人或與（1）至（4）的人有接觸或有關係的人。

我們在此可目睹，德國（及歐盟各國）在面臨風險社會時，如何不斷將刑法干涉的時間點向前推，即不斷朝向刑法前置（Vorverlagerung des Strafrechts）[32]而發展。惟，由於相關規範

[32] 簡而言之，所謂刑法前置，係指核心法益以外建構邊陲的法益，使構成要件所保護的法益前置；亦或指部分行為階段轉變成獨立罪行，使原先不罰的準備行為轉變成單獨的罪名。兩種現象導致應刑罰的犯罪行為的前置現象。關於此

屬於程序法規範，所以和以往所觀察的實體法罪名前置的現象確實不一。雖然刑事偵查的前置有一定界限，但該發展趨勢仍然越來越強。其重要動因之一，來自新型風險：由敘利亞戰爭歸來的「聖戰人員」已高達 1000 人左右。相對於這些極端主義者及恐怖份子，德國警察及刑事司法被逼迫思考，如何有效監督所謂「危險人物」（Gefährder），以免具潛在恐攻傾向者後來真的實現恐怖攻擊。[33]

除此之外，資訊保護法另有許多歐盟綱領以外的制度變遷，諸如資訊處理中應區分事實與評估（第 73 條），傳送資訊的程序（第 74 條），個人資訊的更正、刪除及處理上的限制（第 75 條），自動處理系統之運用記錄（第 76 條）及隱密通報違法事宜的機制（第 77 條）。

雖然歐盟綱領（EU）2016/680 的主要目標在於統合刑事追訴中的個人資訊運用，即指向刑事訴訟，尤其指向刑事偵查等事宜，但德國於 2017 年所立的資訊保護法因應歐盟命令（EU）2016/679 及歐盟綱領（EU）2016/680 法僅修正資訊保護法本身，但未修正刑事實體法及刑事訴訟法。更令人意外的是：聯邦議會正在審合的第二資訊保護法因應歐盟命令（EU）2016/679 及歐盟綱領（EU）2016/680 法案，雖然依目前的規劃將修正總共 154 部法律，但僅修正刑事實體法[34]（以及其他法規），似乎

點，詳看例如 Uriel Möller, Definition und Grenzen der Vorverlagerung von Strafbarkeit: Diskussionsstand, Rechtsgeschichte und kausalitätstheoretische Bezüge, 1. Aufl., 2018, S. 123ff.

[33] 關於此點，參看 Bernhard Kretschmer, Terrorismusverfolgung in Deutschland-tatsächliche und rechtliche Aspekte zum islamistischen Terror, in Gesk/ Sinn（Hrsg.）, Organisierte Kriminalität und Terrorismus, Göttingen: Vandenhoek & Ruprecht, 2019, S. 45 ff.

[34] 該法案擬修正刑法第 355 條第 1 項關於公務員違背職權而侵犯個人資訊；參看

唯一不予修正的相關法規就是刑事訴訟法。可見，歐盟法認定數據剖析屬於刑事偵查的方法之一，但德國立法者並不想要將該制度納入刑事訴訟法，而是一面規避相關問題，一面創造替代方案。

陸、德國現行刑事訴訟法之相應規範

要理解德國如此雙手策略，應先釐清德國相關法規的整體框架。數位化時代早已進入德國刑事訴訟法的具體規範。人類溝通的種種符號系統，一直都有助於人類意識的表現，所以當然也被利用於事後證明特定行為人有無表現與特定犯罪事件有關的意識。因此，例如通信監控與搜索，由德國刑事訴訟法第 100 條（郵件之扣押）加以規範；電話中溝通的音訊及電磁資訊可依德國刑事訴訟法第 100a 條來監控與記錄。然而，現代通訊溝通已不似傳統通信，關於過去沒有加密溝通的傳統電話，現今已經很少見到如此「簡陋」的設備：大部分的智慧型手機、網路電話等，都在發訊端將訊息加密，在收訊端解密。因此，傳統的監控模式已不管用。基於此，德國刑事訴訟法於 2017 年 8 月 17 日增設第 100b 條關於線上搜索的規定。再者，假如偵查單位並不想知道相關溝通內容，但試圖理解嫌疑人或被告之移動模式和交往對象，則可依第 100g 條之規定取得該人之「溝通資訊」（Verkehrsdaten）[35]。除此之外，所謂隱藏性偵查措施還有第

修正草案第 62 條。

[35] 雖然 Verkehrsdaten 一詞似乎係指「交通」資訊，但依德國通訊監控法（TKG）第 3 條第 30 號的定義，此概念所指的是通訊業者所取得、所處理及所適用的資訊；參看例如 Lutz Meyer-Goßner/ Bertram Schmitt, in: StPO-Kommentar, 62. Aufl., 2019, § 100g Rn. 7.

100c 條（住宅之聲音監控）及第 100f 條（住宅以外之聲音監控）。尤其線上搜索及交通資訊之分析等，除非運用最先進資訊技術，否則不可能獲得刑事偵查中可用的證據與信息。相對於此，德國早於 1970/80 年代追訴極左恐怖份子時期，檢警開始適用所謂網格式偵查。此偵查模式，雖然當年有效，但從今日看來，屬於資訊科技相對落伍的技術層面。1979 年，德國警察追捕恐怖份子時，首次適用過該偵查方法[36]，並且藉此也確實逮到犯罪人了。立法者後來於 1992 年 7 月 15 日經反組織犯罪法案（Gesetz gegen die organisierte Kriminalität）將該偵查方法以第 98a 條明文納入刑事訴訟法。當年，檢警僅於案發後來適用網格式偵查的方法。可是，在 911 之後，以及在資訊系統及電腦的處理能力大量升級之後，德國內政部長原先希望以預防為目的而適用該偵查方法。此刑事政策遭到聯邦憲法法院的反對：該法院於 2006 年 4 月 4 日以裁定確認[37]，網格式偵查不得以防範抽象風險為由而使用，僅可針對具體危險而適用之。可見，聯邦憲法法院不願意否定德國自己在國內反恐時期所適用的偵查方法，但並不希望擴大該方法的適用範圍。聯邦憲法法院的裁定明確主張，即便 911 過後，整個西方社會都面臨恐攻風險，但除非已經出現重大法益受具體侵害之危險（具體危險 konkrete Gefahr），否則不得以抽象危險或風險為由而進行網格式偵查。由此得知，聯邦憲法法院在此似乎採取折衷意見[38]：雖然該法院並不允許侵犯基本法第 2 條第 1 項及第 1 條等規定之一般人格權（allgemeines Persönlichkeitsrecht），但仍然在比例原則的具體運用之下，犧

[36] Jürgen Simon/ Jürgen Taeger, Rasterfahndung : Entwicklung, Inhalt und Grenzen einer riminalpolizeilichen Fahndungsmethode, 1. Aufl., 1981, S. 11 ff.
[37] 1 BvR 518/02.
[38] 參看 Lutz Meyer-Goßner/ Bertram Schmitt, a.a.O. （Fn. 35.）, § 98a Rn. 1.

牲該法院在其他案件中所創造的資訊自主權（Recht auf informationelle Selbstbestimmung）的一部分[39]。換言之，基本權利的保護，雖然在其核心享受絕對保護，但在其邊陲仍可依比例原則以及重大公共利益的考量而限制之。

雖然部分德國刑事訴訟法學者在非正式溝通中猜測，要在刑事訴訟法範圍內適用數據剖析時，或許可準用網格式偵查的訴訟法規定，但此觀點僅注意到兩者之間的相似性，卻忽略網格式偵查與數據剖析在概念定義上的重要差異。依德國刑事訴訟法第 98a 條之規定，網格式偵查原則上將個人資訊或個人可能所具備的資訊與其他資訊以自動化（德語原文使用「機械式」maschinell 一辭）的方法加以對查。藉此，排除部分犯罪嫌疑人，或發現犯罪嫌疑人的其他特徵。前者稱消極的網格式偵查，後者則稱積極的網格式偵查。舉例言之，德國警方於 1979 年首次使用該方法時，僅推定恐怖份子在法蘭克福以假身份租用公寓，因此對查租用公寓者名單與任何含有合法姓名資料的目錄，如戶政事務所資料、監理單位有關駕照的資料庫、退休保險之參與者名單等等。最後查出大約 10 個人，其姓名與任何資料庫中的實名不相符，即查出具高度嫌疑的對象。若將該方法與數據剖析加以比較，則可以看到幾個重要的差異：（一）數據剖析未必事先正面定義其所對查的參數。由於系統本身具自主學習能力，且不需要事先已結構化數據，反而可自行將未結構化數據納入其分析的數據矩陣（data matrix），所以能夠更加靈活運用。（二）對查的公式未必是機械式的，即未必是一時不變的，反而很有可能是一組自動學習的運算方式（Algorithmus），即屬於類神經網絡。依此，數據剖析未必從一開始具有傳統明確的特徵，

[39] 1 BvR 209/83, 15/12/1983.

也提不出一個無庸置疑的單一結果，反而運用一些在運算上說不出其被評價的比例的相對模糊分析的方法，且依此提出具高度或然率的結論。數據剖析在德國刑事偵查中目前較明顯被運用的例子，應該是偵查漢堡舉行 G20 會議時所發生的暴動及其中的嫌疑人[40]。當年有了不少來自不同國家、具有不同背景的人來漢堡，他們一邊示威遊行，一邊破壞無辜者的車輛、店舖等等。德國檢警事後扣留所有公車、地鐵、車站等記錄資料、民眾所提供的手機錄影、警察自己所拍到的照片等，並且由此先行確認，什麼人在哪裡進行破壞行動，然後經由影片比對而搜尋其間無法辨認的嫌疑人真正長相？利用什麼交通工具？幾號到達漢堡以及幾時離開等等。

恰好因為上述自動比對犯罪嫌疑人的面孔與各式各樣的錄影錄像等資料，所以警方後來確實偵查有功，並且導致部分被告被判處 3 至 4 年有期徒刑[41]；相關偵查方式也引起注意與爭論[42]。原因在資訊錄製與資訊運用等目的相互脫節：相關錄影錄像資料原來的製作目的在確保公車上安全、地鐵上安全、火車站安全等等；現今所進行的自動比對面孔的目的，反而用於確認當日在公

[40] 漢堡 G20 高峰會於 2017 年 7 月 7 至 8 日舉行。因反全球化團體（Globalisierungsgegner）認為，G20 高峰會不僅為全球化象徵，同時為日後的全球化發展過程創造更多的政治途徑與社會空間，所以號昭反全球化人士來漢堡,並且組織大型示威遊行活動。雖然大多數示威者採取和平行動，但另有數百名自稱「獨立左派」（unabhängige Linke）、「自主左派者」（autonome Linke）、「黑色方塊」（schwarzer Block）等人認為，應經由暴動而增強抗爭力度。因此，尤其 7/7 晚上在部分市區發生嚴重暴動事件，不僅路邊車輛被燒毀，店舖也先被搶劫，後被燒，警察成集體攻擊的目標；參看例如 https://www.ndr.de/nachrichten/hamburg/G20-Gipfel-in-Hamburg,gipfeltreffen264.html (Letzter Abruf: 21/12/2018)

[41] Gericht verhängt bislang höchste Strafe gegen G20-Randalierer, Zeit, 9.1.2018; Zeit Online (Letzter Abruf: 09/09/2019)

[42] 參看 G20: Streit um biometrische Erfassung （AFP, dpa）, NOZ, 19/12/2018, S. 5.

車、地鐵、火車以外的地方進行破壞行動的嫌疑人為何？顯然，相關錄影錄像的製作目的與其現今的使用目的並不相符。因此，漢堡市的資訊保護官要求刪除相關錄影錄像，檢警反而認為，相關資料對比符合漢堡警察處理資訊法[43]第 22、23、27 條。可是，依該法第 22 條之規定，為防止具體危險或因足以證明特定事實，有預防性防治未來嚴重犯罪的必要[44]，警察得以對比相關個人資訊與警察手上的資料庫或其他來源的資訊。顯然，警察在此所比對的目的，不在防治未來風險，而在偵查過去犯罪。又，依第 23 條，警察得以要求其他單位傳送含有個人資訊的檔案，並且以自動化方式進行檔案比對。依第 23 條第 2 項，比對之主要特徵需事先以書面方式加以記載。雖然這些規定不再要求進行機械式比對，所以原先可允許現代數據剖析，但因為進行偵查者需事先以書面方式指出，其所比對的特徵為何，所以在相當程度無從利用數據剖析的優勢：自動學習的系統不能基於數據剖析而自行指出其中的重要參數，更不能事先指出相關特徵。因此，除非警察僅籠統指出行為人參與特定時間及特定地點的暴動，否則無從適用本條規定。其次，由於漢堡警察處理資訊法僅容許偵查單位以預防目的而進行資料自動比對，所以當然難以合理化事後的偵查。可見，唯一沒有提起危險防範（預防）目的的條文係漢堡的警察處理資訊法第 27 條有關自動化檔案（automatisierte Dateien）的規定。該條並沒有提出未來風險防範的限制，僅要求設置自動化〔處理和運算特定事項的〕檔案的利益要大於被干涉者值得保護的利益，即具體運用狹義的比例原則。依此，或許

[43] Gesetz über die Datenverarbeitung der Polizei, Hamburg, 最初立法 02/05/1991，最近一次修正 08/12/2016, letzter Abruf 15/09/2019.

[44] Gesetz über die Datenverarbeitung der Polizei, § 6 Nr. 6: "...zur vorbeugenden Bekämpfung von Straftaten mit erheblicher Bedeutung erforderlich...".

可容許漢堡市警局該偵查行為。其中所提到的限制有二：（一）公共利益要大於受影響者之值得保護利益受侵犯的風險，（二）自動化處理不得造成相關事實之不當簡化或不當扭曲。可見，漢堡警察所進行的，就是數據剖析；其進行數據剖析的目的是刑事偵查目的，但其進行數據剖析的法律依據，並不是刑事訴訟法，反而是漢堡市所立的警察處理資訊法。可見，聯邦議會沒有如歐盟綱領所要求的，將數據剖析納入刑事訴訟法，造成實務單位的不方便，也多少造成相關規範不明確的困擾。

柒、結論

如果我們由歐盟綱領（EU）2016/680 關於數據剖析的規定來看漢堡市警局的偵查方法，則看到漢堡的規定符合該綱領。未經檢警以錄影錄像等搜查方式確認行案者，即受影響的無辜民眾，都不可能被起訴，所以也不可能受到歧視性待遇；確實在漢堡進行犯罪者，其在公共空間所享受的隱私權不屬於隱私權的核心領域，所以沒有絕對的保護必要，同時沒有值得保護的其他理由，所以在比例原則的範疇之下，也不可能指出漢堡警察的相關偵查行為違法。可是，以類神經網絡所處理的數據剖析並不提供一個必然正確的判斷結果，僅提供高度或然率的分析結果。換言之，其並不能適用刑事訴訟法第 98a 條的規定。因為後者並不直接涵蓋數據剖析的情形，使得此偵查行為在德國刑事訴訟法中沒有一個明確的法律基礎。警察當然可以依數據剖析回溯找出原來的記錄，然後以目測的方式主張，哪位暴徒是哪位乘客，且依此隱藏其所適用的方法。但此結果另人感到有些不妥當。除非各邦所立的警察法賦予警察相關偵查依據，否則根本沒有什麼合適的規範。可是，由於警察法的目的在於未來風險的防範，所以原本

不應該被當成偵查犯罪的依據。也因為如此，漢堡的警察處理資訊法若干規定也僅模糊論及自動化檔案的對比，但並未說明此自動化檔案的使用是否限於該法第 22、23 條的情況，也沒有另外說明，相關檔案及其比對等使用目的為何？僅提起公共利益需優於受影響者之潛在受害風險，所以留下法規範不明確的困擾。

其次，當聯邦憲法法院審查，偵查措施有無合憲，該法院就有問題意識：所對比的數據庫是單一的，還是複合的？假如所對比的僅屬於單一數據庫，該偵查行為所防範的風險不必很大。所防範的風險越大，可偵查的數據庫的數量也就可隨著增多[45]。由此得知，德國司法很清楚，數據剖析以及其他有關數據分析的偵查方式都一樣：用的數據（庫）越多，對他人隱私的破壞可能性也就越高。國家要干涉基本權利，要干涉的如此深，需以相對重要的、具體的公共利益為前提，否則禁不起比例原則的審核。可惜，德國一般社會以及德國的立法者，似乎沒那麼清楚地理解到，當兩個平行而進行的數據剖析或其他數位化偵查方法被整併，其所形成的新的偵查方式呈現質量上的大幅提升。因此，當立法者於刑事訴訟法規範中未確立綜合分析的規範，就必然形成一個不明確的空間。舉例言之：當偵查部門得以對查犯罪嫌疑人的電話定位記錄時，可否將該定位記錄與犯罪嫌疑人的臉書資料或與其他社群媒體上所「公布」的資料加以對比？可否基於社群媒體上所留下的記錄進行犯罪嫌疑人的心理分析及溝通對象的數據剖析？每一個相應的偵查方法有可能合法存在，但相關綜合分析對被調查者的偵查力度與個別分析大不相同。因此，德國立法者到目前都規避數據剖析在刑事訴訟法中的確立，實屬不當。一方面未予實現歐盟綱領（EU）2016/680 的內國法化義務，另一

[45] 參看 BVerfG 2 BvR 1372/07, 2 BvR 1745/07（17/02/2009）.

方面造成實務單位偵查行為合法性的疑慮。綜而言之，德國的刑事訴訟法，雖然已開始考慮到數位化時代的來臨，但到目前為止，德國的聯邦議會並未納入歐盟法有關數據剖析的規範於德國刑事訴訟法內。

參考文獻

Kroll, Andreas (2013). Computational Intelligence: Eine Einführung in Probleme, Methoden und technische Anwendungen, 1. Aufl., München.

Kretschmer, Bernhard (2019). Terrorismusverfolgung in Deutschland – tatsächliche und rechtliche Aspekte zum islamistischen Terror, in: Gesk/ Sinn (Hrsg.), Organisierte Kriminalität und Terrorismus, Vandenhoek Ruprecht, Göttingen.

Zitzler, Eckart (2017). Dem Computer ins Hirn geschaut, 1. Aufl.,Berlin.

Gesk, Georg (2019). Transnationale Strukturen im Strafprozessrecht, in: Gesk/ Sinn (Hrsg.), Organisierte Kriminalität und Terrorismus, Vandenhoek Ruprecht, Göttingen.

Brüning, Janique. Künstliche Intelligenz und Strafrecht – Zur Strafbarkeit sogenannter elektronischer Personen, in: Georg Gesk (Hrsg.), Digitalisierung und Strafrecht, Göttingen: Vandenhoek Ruprecht, (in print).

Simon, Jürgen/ Taeger, Jürgen (1981). Rasterfahndung – Entwicklung, Inhalt und Grenzen einer kriminalpolizeilichen Fahndungsmethode, 1. Aufl.,Baden-Baden.

Mainzer, Klaus (2019). Künstliche Intelligenz-Wann übernehmen die Maschinen?, 2. Aufl., Berlin.

Maunz, Dürig (2019). Grundgesetz – Kommentar, München: Beck, 82. Aufl..

Meyer-Goßner, Lutz/ Schmitt, BertramMeyer-Goßner (2019). Strafproz essordnung-Kommentar, 62. Aufl.

Heuberger-Götsch, Olivier (2016). Der Wert von Daten aus juristischer

Sicht am Beispiel des Profiling, in: Fasel/ Meier (Hrsg.), Big Data: Grundlagen, Systeme und Nutzungspotentiale, Springer, Wiesbaden.

Kruse, Rudolf et al. (2nd ed. 2016). COMPUTATIONAL INTELLIGENCE. Wiesbaden: Springer.

Kurzweil, Ray (1st ed. 2005). THE SINGULARITY IS NEAR. New York: Viking Books.

Möller, Uriel (2018). Definition und Grenzen der Vorverlagerung von Strafbarkeit: Diskussionsstand, Rechtsgeschichte und kausalitätstheoretische Bezüge, 1. Aufl., Göttingen.

Tewes, Uwe/ Wildgrube, Klaus (2016). Psychologie-Lexikon, 2. Aufl., München.