大數據分析下犯罪預測機制之展望——以歐盟立法例為借鏡

林士淳*

案例一：某甲（夫）與某乙（妻）均為西班牙公民，正進行一趟歐美之旅，其等從巴塞隆納出發前往冰島，在冰島欣賞完極光後，兩人開心地從冰島首都雷克雅維克機場準備搭機前往美國華盛頓特區。怎料準備登機之際，某乙卻被海關人員以進行二次安全檢查為由帶離，僅准許某甲一人登機。約莫二十分鐘後，某甲心急如焚地到處詢問某乙遭查驗理由，但僅得到航站人員表示此為例行性隨機抽樣的安全檢查。所幸最後某乙毫髮無傷歸來。

案例二：某丙為英國愛丁堡地區幫派份子，經常在地方上鬧事，亦成為進出警局常客。警方認為某丙人際交往對象具有納入並建立犯罪資料庫之必要，遂以某丙電話聯絡對象為中心，進而掌握某丙友人某丁、某戊個人資料（惟某戊無任何前科），三年後，終於透過犯罪資料庫分析預測結果，在一次某丙、某丁進行毒品交易時當場加以查獲。

壹、前言

為了提高預防犯罪的效率，近年來世界上大多數國家傾向於大數據收集和分析，試圖讓熱門領域犯罪的高危險對象和目標，並進一步將結果提供給警察和執法機構作為參考，從而達到更好的執法效率。我國自當也不例外，近來運用大數據進行犯罪預防及偵查如雨後春筍般展開，以大數據運算強化犯罪偵查能量已然成為新一代警政目標。分析個人數據的目標是預測未來犯罪發生的地點和時間，從而使演算和自動決策技術得到大量應用。儘管收集和處理這些個人資料的目的是合法的，但同時卻增加了濫用的風險，如何強化人民隱私權保障顯然是天秤另一端的核心議題。上開二案例均為根據真實個案改編，目的在讓本文讀者更容易理解犯罪預測實務，進一步思考人民隱私權保障與犯罪預測議題。以下介紹歐盟關於犯罪相關個人數據搜集及處理立法例，其中特別針對以人工智慧進行大數據運算所得出結論，人民可否請求知悉以及解釋的部分進行討論。

貳、概說

在犯罪日益增多的今天，預防犯罪已成為

*本文作者係臺灣士林地方檢察署肅貪專組檢察官，英國倫敦大學國王學院法學碩士（法務部107年度遴選赴外國進修檢察官）

當今世界最重要的全球性問題之一，同時也受到了加強公共安全的高度重視。政府官員正在努力提高預防犯罪的效率。許多關於這個問題的調查通常使用行為科學和統計學。近年來，數據挖掘（data mining）已被證明是犯罪預測和預防的一種積極的決策支持工具，而這些技術都依賴於人工智能。全球社會正在見證大數據（big data）和人工智能技術（artificial intelligence）的躍進式進步。近年來，機器人和相關軟體取得了意想不到的成果，從人形機器人、自動和護理機器人、自動汽車、機器人保姆和玩具，到用於預測治安維護或醫療診斷等領域。其他人工智能應用的例子，例如個人語音助理、人臉和模式識別或自動分析[1]。在自動運算決策系統（algorithm）中，人工智能在處理和分析個人數據方面的廣泛應用贏得了國家有關部門的青睞，這引發了關於數據資料主體（自然人）是否提供了足夠的保護和公平對待的爭議。因此，法律措施針對自動化個人決策施加了限制，目的在於矯正電腦運算產生偏見的風險。儘管可能部分阻礙人工智能在決策中的未來發展，然而這些對自動運算決策的限制就像是一個強有力的壁壘，能夠保護個人權利，當然也維護人民隱私權。

大數據演算係基於自動運算決策系統而來，對於自動運算依賴程度日益提高的情況下，伴隨而來的是人權遭侵害的憂慮。以英國為例，甫於2108年間發現倫敦警方以非法方式監控幫派組織相關人員[2]，倫敦市警方自2011年以來長期違反數據保護法進行對倫敦市民個人資料監控。除了監控特定族群，例如特定地區的年輕黑人男性，更使用無差別管理個人資料，亦即不區分檢舉人（證人）、被害人以及犯罪嫌疑人，一律使用同一方式在大數據資料庫內管理這些個人資料。並且就算某倫敦市民已經從警方掌握的幫派名單中移除，警方卻未將其從資料庫中移除。此外，倫敦警方在未告知資料主體之下，與其他機構，如地方議會、住房協會和教育當局分享其大數據資料庫內的當事人個人資料，且沒有就如何正當使用這些數據提供足夠說明或指示，在在顯示倫敦警方濫用市民個人資料。

再以美國為例，種族偏見一直是警方實施犯罪預測中相關新聞的焦點，部分美國民眾擔心，犯罪預測透過運算法會鼓勵警察直接巡邏，針對少數族裔社區，歧視少數族裔個人[3]。美國專家以美國邊境安全維護為例。雖然這些運算法有可能提高犯罪判斷準確性和效率，但也有可能降低對於犯嫌的懷疑標準，並以現有法律無法防止的方式增加意外歧視。因此，縱使不應完全禁止使用犯罪預測，

註1：Maja Brkan, Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond, International Journal of Law and Information Technology, 2019, p2.

註2：參見Information Commissioner's Office, 2018a, https://ico.org.uk/about-the-ico/news-and-events/news-and- blogs/2018/11/information-commissioner-s-investigation-into-the-metropolitan-police-service/ 瀏覽日期：2019年8月28日

註3：P. Jeffrey Brantingham, Matthew Valasik & George O. Mohler (2018) Does Predictive Policing Lead to Biased Arrests? Results From a Randomized Controlled Trial, Statistics and Public Policy, p.2.

這些電腦運算的使用仍應該受到法律的嚴格限制，以防止大規模侵犯隱私和公民自由[4]。

回到我國現況，建立偵查用途的大數據資料庫（或稱之為巨量資料庫）已然成為當前顯學，時常可見各警政單位讚揚使用大數據資料庫對於犯罪正面成效的新聞。從警方說明，可以得知其冀望建立一套高偵查效率人工智慧運算系統，其基礎乃係建立於各種大數據資料庫之上，除了提高破案率之外，更能節省警力。此外，該等犯罪資料庫更可進一步與其他政府單位或民間企業相互整合，進行關聯分析以提高破案契機。同時，警方強調導入人工智慧運算系統，可藉由電腦自我學習，判斷、分析情資並加以篩選、整理，最終提供給警員一份優質的分析結果，從而達到提升辦案績效目的[5]。

事實上，我國警方上開願景，就是基於大數據資料庫，透過電腦運算而得出的自動決策系統（automatic decision-making）。從其相關說明中可以發現警方完全忽略了對於人民隱私權保障的配套措施或者預防機制，遑論自動決策系統可能存在的缺失及偏見，如此不免令人擔心未來民眾個人資料隱私與大數據資料庫蒐集、處理之間的緊張關係無法獲得平衡點。既然我國近年來刑事偵查運用大數據演算發展如此蓬勃，多數司法警察單位將建置大數據資料庫視為一次次的里程碑[6]，可以預見未來我國司法警察單位將更加倚重犯罪資料庫，於此同時是否也應該檢視我國法相對應於人民的隱私權保障是否充分足夠？

根據經驗，藉由自動運算決策系統提升犯罪偵查效率，必須同時實施更強而有力的保障人權措施。由於犯罪預測也將使用大量的自動決策(automatic decision-making)，為國家預防犯罪而收集和分析個人資料將會遇到以下問題：第一、資料當事人是否有權要求國家解釋收集資料的理由或產生結論的邏輯？其次，即使數據蒐集具有法律基礎，但是否存在固有的偏見？例如，基於前科或不同背景的歧視？歐盟於2016年4月通過的新個人資料保護框架由《一般數據保護條例》(General Data Protection Regulation，下稱GDPR)，以及《執法指令》(Law Enforcement Directive 2016/680，下稱LED)組成，此二者均業於2018年5月6日生效實施。特別的是，LED乃專門適用於司法、偵查單位處理用於執法目的

註4：Lindsey Barrett, Reasonably Suspicious Algorithms: Predictive Policing at the United States Border, 41 N.Y.U. Rev. L. & Soc. Change 327 (2017), p327.

註5：警政署資訊室主任蘇清偉表示：「有了豐富的巨量資料庫後，導入人工智慧，將是警政署強化大數據分析戰力的下一步。…路口監視影像是現階段辦案的主要工具，然而動輒數百小時的影片卻是倚賴人工過濾，才能從中提取出有用的資訊;因此，如何應用智慧影像分析提供如視訊濃縮、車牌辨識、物件偵測等智慧化監控，進而結合人工智慧朝向自動化處理判別，方能有效節省員警人力，掌握辦案契機的關鍵。」參見“整合人工智慧與大數據應用警政署提升治安治理能量”，https://www.asmag.com.tw/showpost/11083.aspx，瀏覽日期：2019年9月3日。

註6：參見“警政署首創毒品資料庫──大數據反毒戰”，https://www.chinatimes.com/realtimenews/20160617006536-260402?chdtv，瀏覽日期：2019年9月3日。以及“新北市警察局善用科技建警，大數據可用來辦案還能預防犯罪”，https://www.ithome.com.tw/people/128804，瀏覽日期：2019年9月5日。

之個人數據，更具體地說，是規範為了「預防、調查、發現或起訴刑事犯罪或執行刑事處罰」之目的而進行的大數據自動運算。

關於基於大數據資料庫而由電腦進行自動運算，GDPR第22條以及LED第11條分別有專文加以規範。另外，根據GDPR 第13條(2)(f)、第14條(2)(g)和第15條(1)(h)的規定，資料控管者（data controller）必須向資料主體（data subject）提供「具有邏輯的且有意義的資料」，亦即資料當事人有權利要求瞭解電腦自動運算的邏輯以及為何得出該等結果。論者因此有認為這就代表GDPR賦予資料主體一「解釋權」，但由於法條用語並非直接使用「解釋權」一詞，故此部分仍有爭議[7]，不論如何，目前歐盟成員國內的公民根據上開GDPR規範，擁有請求取得相關訊息的權利。以下將進一步介紹GDPR以及LED對於自動決策的規範及限制。

參、歐盟對於自動決策相關規範

一、GDPR《一般數據保護條例》

自動決策可以定義為在沒有人工干預的情況下做出決策。根據GDPR，「個人化自動決策」是完全基於自動處理的決策[8]。在自動決策過程中，電腦運算（computer algorithm）可以定義為「以一系列步驟去完成任務，且這些步驟的敘述足夠準確讓電腦足以運算[9]」。如今，許多自動決策都是在電腦運算（或稱之電腦演算）的支持下做出的。隨著大數據的使用越來越多，決策變得越來越複雜。如果自動決策對資料當事人沒有任何約束力，亦沒有剝奪該當事人的合法權利，則該決定的影響將會減至最低。但是，當一項決定對個人有約束力並影響到他們的權利時，例如決定是否應該給予顧客信貸、退稅或給予求職者就業機會，法律必須提供充分的保障來保護人民[10]。GDPR第22條規定個人化自動決策規範，該條第1項表示「資料主體應有權不受僅基於自動化處理所做成而對其產生法律效果或類似之重大影響之決策所拘束[11]。」該條第3項則規定「…資料控管者應執行適當保護措施以確保資料主體之權利、自由及正當利益，至少有權對資料控管者部分為人為參與、表達意見以及挑戰該決策。」以上規定主要強調若在沒有人為審查或介入的情形

註7：Maja Brkan, Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond, International Journal of Law and Information Technology, 2019, p1.

註8：Art 22(1) GDPR

註9：Thomas H Coormen, Algorithms Unlocked (MIT Press 2013) 1.

註10：Tal Zarsky, 'The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making' (2016) 41 Science, Technology, & Human Values, p120.

註11：惟同條文第2項有例外規定：第1項規定不予適用，如該決策：
(a)係為締結或履行資料主體與控管者間之契約所必要者；
(b)係控管者受拘束之歐盟法或會員國法有明文授權，且定有適當之保護措施以確保資料主體之權利及自由及正當利益者；或
(c)係基於資料主體之明確同意者。

之下，完全由電腦自動決策所產出結果對人民發生一定法律效力並影響人民權利者，歐盟公民可主張不受該自動決策拘束。GDPR第22條規定一方面反映了歐盟立法者對個人化自動決策機制存有疑慮，首先是可能存在偏見；再者，當電腦運算做出錯誤決定時需設法藉由人為力量介入加以導正。另一方面，此條文規定同時保障資料主體擁有介入錯誤個人化自動決策結果的權利，同時減輕人民對於自動化決策的不信任感[12]。

此外，在GDPR舉例說明第71點[13]更進一步闡述，為了確保數據資料經由公平以及透明程序進行處理分析，資料管控者必須使用適當的運算及統計流程進行，並且特別需先行排除某些可能導致自動決策結果不正確的因素，例如種族或民族起源、政治觀點、宗教或信仰、工會會員，遺傳、健康狀況或性取向，方能將誤判的機率降至最低。當歐盟公民欲挑戰個人化自動決策正確性時，法律應保障公民有表達意見，並要求人為方式檢視，以及獲得數據控制者說明的權利。與此相呼應的還有歐盟第29號特別工作組織針對自動決策所提出之指導方針，亦再次強調實施自動決策必須建立適當的防護機制[14]：決策過程必須秉持透明原則：資料控制者提供予資料主體關於自動決策之相關資訊必須是有

註12：Isak Mendoza and Lee A Bygrave, 'The Right not to be Subject to Automated Decisions based on Profiling' University of Oslo Faculty of Law Legal Studies Research Paper Series No 20/2017, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id1?42964855, 瀏覽日期：2019年9月10日。

註13：GDPR Recital 71(節錄)

…In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. …. In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organizational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimized, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject, and prevent, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or processing that results in measures having such an effect.

註14：Article 29 Working Party

If the basis for processing is 22(2)(a) or 22(2)(c), Article 22(3) requires controllers to implement suitable measures to safeguard data subjects' rights freedoms and legitimate interests. Under Article 22(2)(b) the Member or Union State law that authorises the processing must also incorporate appropriate safeguarding measures. Such measures should include as a minimum a way for the data subject to obtain human intervention, express their point of view, and contest the decision.

意義的，並具有邏輯性[15]。簡言之，當人民提出請求希望得到更多關於自動決策結果時，數據管控者必須以簡單易懂的方式，令提出請求者瞭解該結果背後的基本理由或原理，以及做成該決定所仰賴的標準。防護機制意指最低限度的保障措施，資料當事人應至少有權：(1)要求資料管控者對於自動決策結果進行人為干預及檢視(2)表達意見(3)對自動決策結果提出質疑。當資料當事人發表意見，資料管控者在評估檢視自動決定時應考慮到資料當事人的意見，並有義務作出回應[16]。亦即只要容許作出自動決定，就必須向資料當事人提供適當防護。這些措施旨在防止錯誤或歧視性的決定，或不尊重資料當事人權利的決定。

二、LED《執法指令》

LED第11條第1項對個人化自動決策採取了與GDPR類似的立場，規定成員國有義務禁止完全基於自動處理的決策，包括對資料主體產生不利法律或實質性影響的分析，資料主體有權請求人為介入審視自動決策[17]。同法第13條第1項至第2項則分別規定資料主體有權利知悉資料管控者、處理其個人資料的目的、擁有針對該自動決策提出異議權利、進行該次資料分析處理的法律依據、其個人資料遭留存的時間等相關訊息。LED乃涉及執法方面的個人資料數據保護，該規定採取授權歐盟成員國各自以內國法律授權的方式[18]，並責成歐盟各會員國確定人為力量介入自動決策的權利，給予會員國一定的立法自由空間，給予資料主體適當的保障。

肆、資料主體解釋權

學術界關於資料主體是否有權利在GDPR框架下對個人化自動決策結果要求進行解釋，一直存在爭論，但多數認為應肯定該等解釋

註15：Article 29 Working Party
Meaningful information about the ‘logic involved’
The controller should find simple ways to tell the data subject about the rationale behind, or the criteria relied on in reaching the decision. The GDPR requires the controller to provide meaningful information about the logic involved, not necessarily a complex explanation of the algorithms used or disclosure of the full algorithm. The information provided should, however, be sufficiently comprehensive for the data subject to understand the reasons for the decision.

註16：Maja Brkan, Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond, International Journal of Law and Information Technology, 2019, p18

註17：Article 11 LED.

註18：LED係一種『指令（Directive）』並非直接對全部歐盟國家發生效力，仍有待各會員國各自以國內立法方式轉換實施。例如英國已實施之「2018數據保護法（Data Protection Act 2018）」就是將LED轉換其內國法加以繼受。反之，GDPR性質上為『規則（Regulation）』， 經歐盟立法通國實施後，便當然對全體歐盟成員國發生效力。參見The GDPR and LED, YOUR QUESTIONS ANSWERED（March 2018）By Sharper Pritchard Solicitors and Parliamentary Agents.

權。GPDR第13條第2項(f)[19]規定：「2.…控管者於取得個人資料時，應提供資料主體下列必要之進階資訊，以確保公平及透明之處理：…(f)存在第22條第1項及第4項所定自動決策（包括建檔）者，至少在該等情況，為資料主體之處理所涉及的邏輯性有意義資訊，以及重要性與預設結果。」；同法第14條第2項(g)[20]規定：「2.除第一項所定資訊外，控管者應提供資料主體下列必要之進階資訊，以確保對於資料主體為公平及透明之處理：…(g)存在第22條第1項及第4項所定自動決策（包括建檔）者，至少在該等情況，為資料主體之處理所涉及的邏輯性有意義資訊，以及重要性與預設結果。」此二規定可以視為資料主體之「被告知權（Right to be informed）」。除此之外，GDPR第15條第1項(h)[21]規定：「1.資料主體有權向控管者確認其個人資料是否正被處理，於此情形者，資料主體應有權獲取使用其個人資料及下列資訊：…(h)存在第22條第1項及第4項所定自動決策（包括建檔）者，至少在該等情況，為資料主體之處理所涉及的邏輯性有意義資訊，以及重要性與預設結果。」此則為對於其個人資料之「取得使用權（Right of access）」。

Selbst和Powles以及Wachter等學者，認為解釋權應該來自上開GDPR第13條至第15條相關規定[22]；Casey，Farhangi和Vogl等人則聲稱GDPR引入了「明確的」解釋權賦予資料主體[23]；反之，亦有學者認為前揭GDPR第22條以及第13條至第15條僅規範資料管控者「通知義務」以及資料主體對於數據資料之「取得使用權」[24]。事實上，明確命名為「解釋權（Right of explanation）」的權利並沒有在第22條或關於通知義務的GDPR相關條文中出

註19：Art13(2)(f) GDPR:「the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.」

註20：Art14(2)(g) GDPR:「the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.」

註21：Art15(1)(h) GDPR:「the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.」

註22：Andrew D. Selbst and Julia Powles, 'Meaningful information and the right to explanation' (2017) , International Data Privacy Law 4, 237.

註23：Bryan Casey, Ashkon Farhangi and Roland Vogl, 'Rethinking Explainable Machines: The GDPR' s "Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise' Berkeley Technology Law Journal, from https://ssrn.com/abstract1?43143325, accessed at 7 Apr 2019.

註24：Maciej Gawronski, Guide to the GDPR (2019), Kluwer Law International B.V.p.177.

現，資料管控者義務在於提供關於自動化決策背後帶有邏輯性、具有顯著意義的資訊給資料主體[25]。

反觀LED並沒有包含任何類似GDPR的保護措施或權利使資料主體能夠理解自動決策背後的原因。LED第11條所提供的唯一保障是自然人得以干預自動決策的權利；所有其他可能賦予資料主體的額外權利則全數保留給歐盟會員國自行以內國法制訂。考慮到在刑事案件中個人化自動決策對人民的影響，這種限縮LED適用範圍的結果將影響歐盟民眾權利甚鉅。例如，某一位資料主體可能被拒絕登機，因為根據電腦運算法自動決策的結果，此人與恐怖主義活動有關。如果容許作出該項決定的會員國法律只給予該資料主體要求覆核該項拒絕的可能性，則此人永遠不會明白為何作出該項決定。對此，部分歐盟學者擔心LED第11條沒有賦予數據主體挑戰自動決策的明確權利，對公民隱私權保障不若GDPR明確[26]。

伍、結論

當大數據資料庫結合電腦人工智慧運算所作成之犯罪預測日益受到我國司法警察辦案倚重之時，吾人更應謹慎思考如何維護人民隱私權。值得信賴的犯罪預測機制毫無疑問對於打擊犯罪乃一大利器，然而，同時強化犯罪預測過程之「透明度」以及建立適度「監督制度」作為配套亦不可或缺。否則一味吹捧大數據犯罪預測正面積極功能，將使人忽略該制度的負面作用，況且，參酌上開倫敦警方濫用並監控個人資料數據事件，足以佐證如何監控管理「犯罪預測」這隻日漸茁壯的猛獸，將是此刻我國必須正視的重要課題。強化透明度及監控的方式或可參酌歐盟法制，亦即賦予人民請求知悉關於自動決策相關訊息之權利、單純完全經由電腦運算做成之自動化決策必須容許人為介入檢視等。以我國犯罪預測實務為例，數據管控者為司法警察單位，當經由犯罪預測而特定之對象質疑該自動化決策存在瑕疵，而欲請求警方提供說明或相關資料時，依我國現行法律制度，人民並無該等權利。試想於歐盟如此保障隱私權制度下尚且發生倫敦警方濫權事件，實難想像我國未來可以完全避免犯罪預測制度侵害人民隱私權之爭端。

再者，本文認為歐盟LED未有如同GDPR第13條至第15條相關規定應非立法疏漏，而是歐盟立法機關有意將此二者做出區隔，主要在於考量LED適用於犯罪偵防而有其特殊性，若賦予人民過於詳盡的說明請求權，某程度上將導致妨害司法警察進行案件偵查或犯罪預防。即使如此，我國仍應考量針對個人化自動決策增定專門規範於個人資料保護法。此觀之LED第11條以及第13條仍針對自動化決策賦予民眾符合犯罪偵防目的之下的保

註25：唯一明確提到解釋權的為Recital 71。

註26：Maja Brkan, Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond, International Journal of Law and Information Technology, 2019, p29 .

障，包括資料主體有權利提出異議，請求人工方式介入審視自動化決策，以及知悉其個人資料為司法調查單位使用之目的等，相信此立法方式乃系考量平衡不妨害刑事犯罪偵防與保障人民隱私權後之產物。相較前開所介紹歐盟GDPR以及LED等立法例，我國個人資料保護法第8條至第10條，第15條、第16條雖有規範公務機關對於個人資料蒐集處理使用，惟對於個人化自動決策尚未有專屬條文規範，實無法因應新型態的大數據犯罪預測，相較於歐盟立法例，我國法對人民隱私權保障似有所不足。即便不採取類似歐盟GDPR完整保護隱私權機制，建議亦可參酌LED立法例，明文增定個人自動化決策規範，藉以強化保障在這股大數據浪潮下的人民隱私權。