出國報告（出國類別：進修）

金融犯罪偵查資源（含金融調查、鑑識會計等）之研究

服務機關：臺灣士林地方檢察署
姓名職稱：林士淳檢察官
派赴國家/地區：英國倫敦
出國期間：民國 107 年 8 月 10 日至 108 年 8 月 9 日
報告日期：民國 108 年 11 月 8 日

摘要

金融業高度依賴信息技術，是典型的數據驅動行業。大數據的應用對於金融行業的發展來說也具有深遠的意義，如建立有效的大數據徵信系統，為網際網路金融解決風險評估問題。而金融犯罪是一個日益嚴重的問題，需要對其進行有效的防範，為了防範金融犯罪，金融機構每天必須處理眾多數據，均仰賴電腦程式演算得出之自動化決定，以發現可疑交易並提報給國家洗錢防制專責單位；另方面而言，個人金融資訊涉及隱私甚鉅。本文著眼於大數據演算下金融犯罪預防與隱私權保障之潛在衝突，從歐盟反洗錢指令與數據保護條例相互交錯之處，分析其等之間相容性，藉以檢討我國洗錢防制法與個人隱私保護法之立法完備性。

目次

壹、概說

近年來大數據分析浪潮席捲全球，海量數據分析廣泛地運用在生活各層面。金融業更是大數據的重要產出者，客戶金融資料、交易、報價、業績報告、消費者研究報告、官方統計數據公報、調查、新聞報導無一不是數據來源，其高度依賴信息分析技術，是典型的數據驅動行業。大數據的應用對於金融業的發展來說也具有深遠的意義，例如建立有效的大數據徵信系統，為網路金融解決風險評估問題。近年來運用大數據進行金融犯罪預防等偵查作為如雨後春筍般展開，以大數據運算強化犯罪偵查能量已然成為當代顯學。分析個人金融數據的目標是察悉可疑金融交易行為報告(Suspicious Activities Reports, 下稱SARs)，從而使演算和自動決策技術得到大量應用。儘管依據反洗錢機制蒐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，以歐盟實務而言，由於日益嚴格的反洗錢合規要求，逐年增加的 SARs 帶給金融機構沈重壓力及負擔，同時間該等 SARs 的內容品質也受到各方極度批判，許多專家學者認為大多數的SARs流於形式，只為了應付反洗錢制度而產生。近一步而言，這些 SARs 都出自於數據主體的金融資料，可以想見大多數的 SARs 是無意義的，卻也高度提升了數據主體的隱私權受侵害的可能性。顯然於強化反洗錢措施之際，如何強化人民隱私權保障是天秤另一端的核心議題。

金融犯罪日益嚴重，為了加以防止，金融機構有義務每天處理大量數據。網路服務、科技和全球化的發展，對金融犯罪產生了影響，這些犯罪變得更加普遍，也更難預防。為了防止網路犯罪，越來越多的數據資料庫需要進行數據蒐集和處理。越來越多的數據處理需要更新版

本的數據保護立法，以協調歐盟成員國之間的進程，於是催生了一般數據保護條例（General Data Protection Regulation,下稱 GDPR）的制定，該條例於 2016 年通過，也被認為是在處理和蒐集私人數據時保護個人權利最有效的數據保護立法之一。另一方面，金融犯罪相關數據可能是敏感的，這也凸顯個人數據保護重要地位，可以預見實務上將發生金融機構處理客戶隱私資訊與數據保護之間的複雜與難以兼具。

洗錢防制工作日趨成為國際共同目標，我國洗錢防制法業於 2016 年 12 月 28 日修正通過，在本次修正中主要參考國際防制洗錢金融行動小組（Financial Action Task Force on Money Laundering, FATF）所制定的四十點建議所為的修正。該次修法擴大了洗錢防制得以監控的範圍，同時強化金融機構（包含虛擬貨幣交易平台） 對於往來交易對象資料之蒐集掌握。換言之，金融體系對抗洗錢犯行的主要武器之一即為大數據資料庫，透過廣泛取得往來交易對象數據資料，進而加以處理、運算、比對，精確掌握客戶及洞悉其是否涉及洗錢犯行。正因為洗錢防制措施刻不容緩，為避免我國於接受亞太防制洗錢組織（APG）第三輪相互評鑑時落入觀察名單，政府及民間金融業者均大力加以推動落實洗錢防制作為。然而，相較於洗錢防制法，我國個人資料保護法自 2015 年底修正後，迄今尚未有大幅度修正，因此，可以想像在強化對於金融體系往來之私人信息數據蒐集之同時，必然衍生對於個人隱私權保障是否充分足夠之疑慮，亦可稱作為洗錢防制與個人隱私保護之兩難局面。本文將一併探究隱私權在我個法律體系中之地位，蓋該等概念並未明文規範於我國憲法條文當中，則應否將個

人資料之隱私保障視為人民基本權？我國洗錢防制法當中相關措施是否有可能與隱私權保護發生衝突？若有，以何者優先？何者必需退讓？以下將逐一進行探討。

貳、金融犯罪關於洗錢防制工作與隱私權之相容性

一、背景介紹

當前生活大小事多都與網路相關聯，在瀏覽新網站時，我們學會了自動接受 cookies。網際網路蒐集個人數據，我們的電腦和手機也蒐集使用者的私人數據，我們把個人信息提供給不同的網頁，往往不加以質疑。在此之前，我們必須親自到銀行去獲取有關我們帳戶的資訊或進行金融行為；今天，我們不必到辦公室去接收信息，只需通過一個應用程序提供指紋或代碼，我們就可以獲得所需的所有數據。然而，如此容易地蒐集和接收所有這些數據信息全然都是優點嗎？直覺來說，國家機關和銀行能蒐集這些數據不是很好嗎？能夠保存和共享數據使當局能夠更好地瞭解其客戶群，由於我們的一切資訊都在網路上，它誘使罪犯發展不同類型的犯罪行為，包括但不限於洗錢和身份犯罪。隨著網路世界的發展，罪犯可以使用匿名賬戶、虛擬專用網等隱藏網絡，通過網路銀行進行資金處理，甚至在國外也不留下處理或資金來源的記錄。如果沒有過程或資金來源的記錄，濫用的風險就會增加。處理金融行為存在一定的風險，許多金融機構利用信用評分將風險因素最小化。因此，如果金融當局能夠相互合作，收集客戶信息，並能夠使用數據資料庫以保護金融安全，那將是一件偉大的事情。有了共

享的數據資料庫，就有可能防止犯罪，而金融機構在取得新客戶關係時也可降低風險[1]。

然而，擁有大數據資料庫會在保存個人數據時產生問題。近年來，數據處理的數量明顯增加，對於客戶和金融機構來說，很難判斷哪些信息是需要蒐集的，哪些信息是不必要的，甚至是有害的。各國在蒐集和使用私人數據時採用了國內立法，這在處理這類信息時造成了國際衝突，故而 2012 年歐盟委員會向一項新的數據保護法規提交了一份提案[2]，該提案旨在建立更新的數據保護條例，使其能夠準確地適用於當前情況。經過多年的工作準備，GDPR[3]在 2016 年 4 月 14 日通過，嗣後於 2018 年 5 月 25 日對歐盟成員國生效[4]。GDPR 是最新的歐洲保護數據立法，影響到歐盟和歐洲經濟區。對於如何處理個人數據，以及在處理個人數據時如何保護個人權利，GDPR給出了更嚴格的規定。自 GDPR 出現以來，金融機構不得不為考慮數據處理的新變化做好準備，其經常被要求適用不同的金融法規，並與不同的金融機構同業合作，這增加了法律數據處理和蒐集私人金融信息的複雜性。GDPR 旨在將處理數據的數量降至最低，這使得監管與金融機構之間的關係變得複雜[5]。

---

[1] Financial Action Task Force, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation' (2018) The FATF Recommendations 9.

[2] Presidency of the Council, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach' (2012) Council of the European Union, COM/2012/011.

[3] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (GDPR).

[4] Council Regulation (EC) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Data Protection Directive) [2016] OJ L119/1.

[5] Olly Jackson, 'Many small firms are still unprepared for GDPR' (2018) International Financial Law Review.

金融業對抗洗錢正在發展，私人數據保護也在發展。金融犯罪是社會的一大威脅，如何正確處理金融犯罪數據顯得尤為重要，自 GDPR 實施後，個人資料的蒐集及使用方法有重大改變,本研究主要集中在探討蒐集金融犯罪數據與保護個人數據之間的平衡點,著重分析金融犯罪在洗錢方面的表現。GDPR 就如何處理和保護個人數據制定了一套全新的規範，即使在偵查金融犯罪領域也必須考慮這些問題，反洗錢指令亦包括關於如何處理金融犯罪數據的指導方針。畢竟若監控私人金融數據有助於預防犯罪,那麼在某種程度上是可以被接受的;然而，處理私人數據資料不可能是完全不受到限制的。這就是為什麼所有歐盟公民都透過 GDPR、LED[6]《刑事執法指令》和 ECHR[7]《歐盟基本權利憲章》享有對個人數據和隱私的保護。

二、個人資料以及金融犯罪數據之交錯

這部分將討論什麼是金融犯罪數據？以及如何定義個人數據？任何與辨別自然人有關，或與個人有關的可識別事物均視為個人資料處理。此外，若蒐集在一起的信息足以識別一個人，該等信息亦被認為是數據。個人資料不包括以匿名方式蒐集或提供的資料，亦不屬於受保障資料的範圍。對於歐盟成員國而言,處理個人數據的一致立法是 GDPR[8]。GDPR 對於「個人數據」一詞規範於第 4 條第(1)款，其定義如下：「個人資料」是指任何相關信息確定或可識別的自然人（資料主體）;可

[6] Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, (LED).

[7] 請參考歐盟基本權利憲章第 7 條、第 8 條以及第 52 條

[8] European Commission 'What is Personal Data?' *(EC Europa EU)* <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en> 瀏覽日期：2019.9.2

識別的自然人是可以確定的，直接或間接，特別是透過援用一個標識符號，比如名字、身份證號碼、位置數據，或特定的一個或多個因素的物理、生理、遺傳、心理、經濟、文化或社會身份的自然人[9]。本條所指的自然人是指第 4 條第(1)款所述的具有法人資格的人或個人，任何可以確定其身份的信息，包括數據，均屬於本條的範圍。這意味著即使非個人信息也可以通過與其他信息相結合而變成個人數據信息，前提是此人可以被識別、特定出來。

在法律術語中，「處理」一詞指的是設置執行個人數據的操作，即使該過程是自動化的亦包含在內。GDPR 第 4 條第(2)款明確規定，即使在刪除數據時，對數據的任何處理均屬於本條的範圍[10]。「數據」本身亦屬一個複雜的術語，特別是在 GDPR 中，「數據」一詞主要指電子記錄的信息，有關的個人資料必須包括可識別的資料。可識別信息是指可以直接或間接識別一個人的兩種數據。這類信息可以是姓名、身份證號碼、照片、位置數據或 IP 地址[11]。至於金融犯罪，又稱經濟犯罪，是指個人為獲取經濟利益而實施的犯罪或違法行為，其具有低風險，高利潤之特點[12]。金融犯罪是一種涉及刑法的新型犯罪，90 年代才在大多數國家被定性

為刑事犯罪。惟金融犯罪本身是一個廣義的名詞，在日常用語中，金融犯罪多與洗錢或資助恐怖主義有關，以下本文主要從預防洗錢犯罪的角度研究金融數據處理。洗錢指的是有人試圖隱藏非法資金的來源，

---

[9] Council Regulation (EC) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Data Protection Directive) [2016] OJ L119/1 Article 4 (1).

[10] Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) 10.

[11] Ibid 11.

[12] Europol 'Economic Crime' *(Europol Europa EU)* <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/economic-crime> accessed on 29 March 2019.

使這些資金成為合法財產[13]。對執法機構而言，金融犯罪調查和識別非法交易正變得越來越困難，有能力注意到非法資金流動者，通常需要國家機構進行多年的培訓。由於金融機構位於洗錢犯行的最前線，因此,反洗錢指令將查悉金融犯罪的責任移交給了金融機構。在歐洲，針對金融犯罪的立法是根據反洗錢指令;目前最新的版本是歐盟第五次反洗錢指令[14](5th EU Anti-Money Laundering Directive，下稱AMLD5)。

另一方面，歐盟儲存個人資料的一般規則是，在有關資料不再適用或處理資料的目的不再需要時，應將有關資料刪除。蒐集和保存資料的理由可能是，例如懷疑或與罪行有關，或該等資料可用於調查。金融當局有義務調查和報告金融犯罪，或如果他們懷疑發生的犯罪。金融犯罪數據可以包括防止洗錢的信息、實施金融犯罪的人員和與恐怖主義融資有關的人員。金融機構，如銀行和商業公司，每天都在蒐集和處理這類信息。當個人向銀行申請貸款或銀行進行信用審查時，就會進行所謂的背景審查[15]。

三、歐盟反洗錢制度發展

[13] Jonida Milaj, Carolin Kaiser, 'Retention of data in the new Anti-money Laundering Directive — 'need to know' versus 'nice to know'' (2017) 7(2) International Data Privacy Law <https://doi- org.db.ub.oru.se/10.1093/idpl/ipx002> accessed 2nd May 2019 118.

[14] Ibid 116.

[15] Jonida Milaj, Carolin Kaiser, 'Retention of data in the new Anti-money Laundering Directive — 'need to know' versus 'nice to know'' (2017) 7(2) International Data Privacy Law <https://doi- org.db.ub.oru.se/10.1093/idpl/ipx002>
瀏覽日期：2019/08/30

洗錢是使犯罪活動的利潤顯得合法的過程，例如使從毒品交易或人口販運得來的錢可用於普通和合法的目的[16]，因此，它是許多嚴重和全球性罪行的核心，第一部《反洗錢指令（AMLD）》於 1991 年通過[17]。《反洗錢指令》包含了反洗錢犯罪和反洗錢預防兩方面的內容，因此成為歐盟內部第一個全面的反洗錢框架[18]。自此，歐盟內部的反洗錢立法與國際進展並行，尤其是從金融行動特別工作組(FATF)的角度[19]，FATF 是一個政府間機構，建立改善反洗錢措施，開發了一系列不具約束力的建議以及認可國際標準[20]。 美國發生 911 襲擊後，打擊資助恐怖主義成為一個額外的和同樣重要的 AMLD 立法的目的[21]。這是通過第三次反洗錢指令時所正式引入[22]，該指令還新增了其他重大變化，如風險基礎方法[23]。最新通過的指令是 AMLD5，它修正了 AMLD4，將於 2020 年初實施[24]。此外，只要符合歐盟法律的限制，歐盟成員國有可能實施更嚴格的規則來實現反洗錢指令的目的[25]。

（一）反洗錢指令的目的和應用

16 Article 1.3 of the AMLD4.

17 Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering.

18 Mitsilegas & Gilmore, *The EU legislative Framework against money laundering and terrorist finance: a critical analysis in the light of evolving global standards,* pp 119–120.

19 Mitsilegas & Gilmore, *The EU legislative Framework against money laundering and terrorist finance: a critical analysis in the light of evolving global standards,* p 120.

20 FATF, “About”.

21 Mitsilegas & Gilmore, *The EU legislative Framework against money laundering and terrorist finance: a critical analysis in the light of evolving global standards,* p 125.

22 Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

23 Recital 10 & article 8 of Directive 2005/60/EC.

24 Recital 53 & article 4 of the AMLD5.

25 Article 5 of the AMLD4.

《反洗錢指令》的總體目的是防止歐盟金融系統被用於洗錢和資助恐怖主義[26]。預防措施是刑法發展的重要補充[27]，它不僅能有效地偵查犯罪，而且能起到威懾犯罪的作用[28]，又為保護共同金融制度，必須在歐盟實施積極管制預防性措施[29]。洗錢定義的一部分，亦即收入來自犯罪活動[30]，而「犯罪活動」一詞包括幾項罪行，包括恐怖主義罪行、毒品交易和稅務相關罪行，這些罪行可被拘留一段時間作為懲罰[31]。因此，《反洗錢指令》係針對從上開列舉犯罪型態中獲取的不法利益進行洗錢，其將恐怖融資定義為聚集恐怖主義犯罪資金[32]，其適用於包括信用和金融機構等多個有義務的實體（Obliged Entity）[33]。此外，儘管「反洗錢」是相關指令中唯一明確的政策目標，但也有人認為 AMLD5 中的修訂還指示了其他政策目標，如防制逃漏稅捐，這意味著不僅要針對從逃稅中獲得的收益進行洗錢管制，而且進一步要針對逃稅本身。

（二）一般性義務

[26] Article 1.1 of the AMLD4.

[27] Recital 1 of the AMLD4.

[28] Recital 4 of the AMLD5.

[29] Recital 2 of the AMLD4.

[30] Article 1.3 of the AMLD4.

[31] Article 3.4 of the AMLD4; article 1.2 of the AMLD5.

[32] Article 1.5 of the AMLD4.

[33] Article 2.1 of the AMLD4.

風險基礎方法（risk-based approach）是反洗錢立法的核心[34]。這種方法意味著，有義務的實體應確定其業務中的洗錢風險，同時考慮客戶、地理區域和產品類型等因素。「反洗錢」政策和程序應基於此風險評估[35]。風險基礎方法在一定程度上減輕了可疑交易報告的負擔，另一個原因是賦予有義務的實體處理複雜問題的靈活性[36]。再者，該方法賦予了有義務實體實施最適合其業務的「反洗錢程序」責任。這種責任的轉移顯示了「反洗錢」內部監管職能從公共機構轉向私人金融活動進行者的趨勢，其目的是使民間金融機構更積極地參與預防工作，從而提高預防工作的效率[37]。

另一方面，與某種業務關係相關的風險會影響關於客戶應蒐集的信息的數量和類型，在此過程中稱為客戶盡職調查(Customer Due Diligence, CDD)[38]。CDD 應在建立業務關係時或以電子商務和現金進行一定數額的交易時進行。當風險被認為較低時，可以進行簡化的 CDD，反之亦然[39]，同時禁止使用匿名帳戶[40]。一些必須執行的 CDD 措

---

[34] 在洗錢防制的實務當中，銀行業從業人員在第一線的實際作業參與程度最大，另外其他業別的從業人員因不同目的也有角色不一的參與，例如，法律人就法律條文對銀行高階主管作解讀、金管會作為監理機構影響銀行決策、外部顧問評價銀行作為有效性等。然而，也因為參與者眾，近期從業人員逐漸發覺跨領域下針對反洗錢時務作業的不同問題意識，其中又以「風險基礎方法」（Risk Based Approach，RBA）的實踐問題最具代表性。風險基礎方法（Risk-Based Approach, RBA）為 FATF 於其「40 項建議」當中所明定為「重大基礎」者，且已為各國實務作業所採用。台灣亦於各洗錢防制法律或規範明定洗錢防制作業需以 RBA 為準，足見此法已為實務上之行動基準。參見：反洗錢的法理學基礎：由洗錢防制風險基礎方法實踐的困難談起，Daniel Wang，https://aml.watch/反洗錢的法理學基礎：由洗錢防制風險基礎方法/，瀏覽日期：2019 年 9 月 28 日。

[35] Article 8 of the AMLD4.

[36] FATF 所稱之洗錢防制 RBA 規範乃意欲利用其規範權威之角色，使得洗錢防制從業人員自行評斷各種犯罪孰輕孰重，並以合理邏輯自行判斷阻斷何種犯罪金流應獲得較多資源、較長篇幅規章政策、以及較嚴謹之事後評價。惟在規範層面，RBA 為國際洗錢防制權威機構 FATF 訂定之準則，故其權威性大致為各國政府認可，然而其內涵卻相當弔詭。RBA 作為規則，其大意旨趣在於要求金融業評估洗錢行為的「程度」，並自行彈性決策何種作為係最適洽者，似乎間接鼓勵從業人員尋得規範與效度之間之縫隙，造成該法實踐上之難點。參見：反洗錢的法理學基礎：由洗錢防制風險基礎方法實踐的困難談起，Daniel Wang，https://aml.watch/反洗錢的法理學基礎：由洗錢防制風險基礎方法/，瀏覽日期：2019 年 9 月 28 日。

[37] Ross & Hannan, Money laundering regulation and risk-based decision-making, pp 107–108.

[38] Article 13.2 of the AMLD4.

[39] Articles 15 & 18 of the AMLD4; article 1.10 of the AMLD5.

[40] Article 1.6 of the AMLD5.

施是驗證客戶以及受益人的身份[41],有義務的實體還應監測業務關係,包括交易，以確保這與它們所掌握的有關客戶的資訊相一致[42]。受益人是最終擁有或控制一個法律實體的人,例如通過擁有一定比例的股份或投票權[43]取得某法人控制權。這些資訊很重要，因為它使罪犯更難隱藏在公司結構背後[44]，為進一步提高透明度，有關受益人的資料亦須保存在銀行登記系統內,並在不同程度上向主管當局及公眾開放[45]，CDD 中包含的信息應在業務關係結束後保留 5 年[46]。自第一部《反洗錢指令》以來，該 5 年的保留期一直不變，該指令隨後認為，為了將數據信息用作調查證據，該保留期是必要的[47]。根據 AMLD4，由於數據保護和法律確定性的原因，限制為五年[48]，並在保留期結束後，應刪除該信息[49];但是，若認為有必要，可在第一個保留期限屆滿後再保留最多五年[50]。此外，亦應制定具體的保障措施，以保護數據不被非法獲取，被處理數據的個人也有可能獲得關於他們自己的信息，儘管根據數據保護條例，這可能是有限的與可疑交易有關的信息[51]。既使沒有要求保存相關資訊於銀行登記系統內，蒐集和存儲信息仍是「反洗錢」預防措施的重要組成部分。在銀行登記系統之前，或與該

41 Article 13 of the AMLD4; article 1.8 of the AMLD5.

42 Article 30.1 of the AMLD4; article 1.15 of the AMLD5.

43 Article 3.6 of the AMLD4; article 1.2 of the AMLD5.

44 Recital 14 of the AMLD4.

45 Recital 14 & article 30.3 of the AMLD4; article 1.15 of the AMLD5.

46 Article 40.1 of the AMLD4; article 1.25 of the AMLD5.

47 Article 4 of Council Directive 91/308/EEC.

48 Recital 44 of the AMLD4.

49 Article 40.1 subpara 2 of the AMLD4.

50 Article 40.1 subpara 2 of the AMLD4.

51 Recital 46 of the AMLD4.

制度雙軌併行，義務實體需將這些信息存儲在其自身公司內[52]，而在某些情況下，他們還必須共享 CDD 的信息。

（三）分享洗錢防制資訊的義務

每個歐盟成員國都應有一個金融情報單位（FIU），負責「預防、發現和有效打擊洗錢和恐怖主義融資」[53]。且 FIU 應在業務上獨立，負責接收和分析與懷疑洗錢有關的資料 。有義務的實體應向 FIU 報告任何可疑金融交易，並在這種情況下直接向FIU提供所有必要信息[54]。有義務的實體不得進行可疑交易，也不得將正在進行的調查通知嫌疑人或第三方[55]；但應告知客戶，其信息將根據《反洗錢指令》進行處理[56]。為了實現其目的，FIU 還應能夠要求任何有義務的實體提供信息，並將信息轉交給其他主管當局[57]。其不需要一份 SAR 來要求提供資料，但向另一個主管當局提出的要求必須根據充分確定的條件[58]，然而這些條件是什麼，在《反洗錢指令》中沒有進一步定義。FIU 還應該能夠在需要防止洗錢、恐怖主義融資或相關犯罪活動時，請求並響應歐盟成員國內其他主管機關提供的信息[59]。在《反洗錢指令》中未定義哪些權限構成主管機關權限，這使得任何將參與履行反洗錢目的之國家機構都有可能請求相關洗錢信息。這是一種可能的法律架構，因為在不同的歐盟國家中，主管機關的設置可能是不同的，就像 FIU

[52] Article 40 of the AMLD4.

[53] Article 32.1 of the AMLD4.

[54] Article 33 of the AMLD4; article 1.21 of the AMLD5.

[55] Articles 35.1 & 39.1 of the AMLD4.

[56] Article 41.3 of the AMLD4.

[57] Article 32.3 of the AMLD4; article 1.18 of the AMLD5.

[58] Recital 17 & article 1.18 of the AMLD5.

[59] Article 32.4 of the AMLD4.

的設置一樣[60]。需要注意的是，主管部門的定義與 GDPR、LED 的定義不同，一個主管機關基本上只能在可能妨礙正在進行的調查的情況下，才可以拒絕與其他主管機關分享資料[61]。在職掌部門方面，AMLD5 似乎特別強調了某部門在反洗錢行動中的作用，那就是稅務機關[62]。至於國家合作，還單獨提到稅務當局，因為稅務主管機關應確保有打擊洗錢和恐怖主義融資的有效機制[63]，此表明立法者對稅務機關在反洗錢中的作用的重視。賦予稅務機關獲取信息的權限，強化了其在反洗錢措施中的作用，但也可能導致與數據保護法的衝突。這一強調也表明瞭前揭所提及逃稅已成為反洗錢本身的政策目標。

在不同的歐盟國家中，各 FIU 之間的合作也很重要，特別是洗錢和恐怖融資是國際犯罪[64]，歐盟各國應確保 FIU 為了反洗錢或相關上游犯罪的目的，在歐盟境內自動或應請求跨國界交換相關信息[65]。收到請求的 FIU 應及時作出反應，如果交換違反已經規定存在之國家基本原則，則可拒絕這種請求[66]。例如某甲 FIU 想在某乙歐盟成員國中向有義務的實體請求信息，他們必須通過該某乙中的 FIU[67]，且某乙會員國可以要求某甲FIU必須遵守該等資訊信息使用上的限制[68]。實際上，由於對稅收犯罪等上游犯罪的定義不同，歐盟各成員國在信息交換方面遇到了一些困難[69]，然而，不同的定義不應限制跨境資訊交流[70]。不

[60] Recital 16 of the AMLD5.

[61] Article 1.32 of the AMLD5.

[62] Recital 44 of the AMLD5.

[63] Article 1.31 of the AMLD5.

[64] Recital 54 of the AMLD4.

[65] Article 53.1 of the AMLD4; article 1.33 of the AMLD5.

[66] Article 53.3 of the AMLD4.

[67] Article 53.2 of the AMLD4; article 1.33 of the AMLD5.

[68] Article 54 of the AMLD4.

[69] Recital 18 of the AMLD5.

同會員國之間信息交換的另一個問題是 FIU 的形式不同。不過，這些分歧不應妨礙信息交流，FIU 仍應盡可能地合作，實際上，FIU 亦可能會遵循不同的數據保護規則[71]。FIU 還應與歐盟以外國家的 FIU 基於歐盟法律（包括歐盟數據保護法）交換信息數據[72]，義務實體、FIU 和主管部門還應擁有向 FIU 和其他主管部門共享信息的安全保密管道[73]。此外，管理系統應要求保障數據的安全，並應確定哪些人、哪些類別的人或當局應享有對數據的專門取得權。根據《反洗錢條例》，其他要求保密的國家法律不應妨礙保密信息的交換[74]，這些保密措施應確保信息被盡可能少的人知悉。

（四）銀行登記系統制度

1.數據資料儲存

AMLD4 和 AMLD5 均明確指出每個歐盟會員國內，必須建置中央自動化機制，例如登記制度（Register）或電子數據檢索系統（Electronic Data Retrieval System ）。該機制應允許識別在歐盟區域內持有或控制付款或銀行帳戶和保管箱的任何自然人或法人。該機制應允許識別在歐盟區域內持有或控制付款或銀行帳戶和保管箱的任何自然人或法人，對於銀行賬戶和支付賬戶 ，登記系統應包括國際銀行賬號（IBAN）、開立和關閉日期、持有人、控制人和受益所有人的姓名以

---

[70] Article 1.36 of the AMLD5.

[71] Mohamed, *Legal Instruments to Combat Money Laundering in the EU Financial Market,* p 72.

[72] Recital 58 of the AMLD4.

[73] Article 42 of the AMLD4; article 1.30.b of the AMLD5.

[74] Article 1.32 of the AMLD5.

及其他身份數據，如個人身份證件號碼。保管箱的登記還必須載明承租人的姓名、身份證號或者類似號碼，並載明租賃期限。

實行銀行登記系統，銀行蒐集到的所有個人金融數據，將可在同一處提供取得，以便對個人的經濟活動進行通盤了解，從隱私權保障的角度來看，存儲個人信息的這種差異可能帶來新的挑戰。其他歐盟會員國認為對履行反洗錢指令之義務至關重要的相關信息，也可列入銀行登記事項[75]，但應只有包括進行這類調查所需的最低限度數據[76]。至於何者被認為屬於「必要的」或「必須的」，則沒有進一步的定義。銀行登記系統中的信息應與義務機構的CDD信息的保存期相同均為5年，在這種情況下，業務關係的結束可能意味著付款帳戶的關閉，以及銀行登記系統中的資料保留期也可以再延長5年。

2.數據資料共享

銀行登記系統內的數據、資訊應「以直接和不經過濾的方式」直接提供給 FIU[77]。這意味 FIU 不再需要向每一個有義務的實體，亦即各金融機構，請求信息並等待他們的回覆，就像他們在沒有銀行登記系統時期時所做的那樣。相反地，他們可以直接取得銀行登記系統中的數據資訊，如此一個有效率的程序是引進銀行登記系統的主要原因，因為過去獲得資料的時間往往拖延或減慢調查的速度[78]。為了突顯有無實施銀行登記系統的差別，以下舉瑞典的情況為例，該國目前還沒有

[75] Article 1.19 of the AMLD5.

[76] Recital 21 of the AMLD5.

[77] Article 1.19 of the AMLD5.

[78] Recital 20 of the AMLD5.

實施銀行登記制度。所以在瑞典，FIU 必須分別與每家銀行聯繫，以獲取某個人的金融信息，由於 FIU 事先不知道嫌疑人的付款帳戶在哪裡，他們必須分別向每個潛在的金融實體請求信息，這通常是通過「傘狀請求」來完成的，這代表 FIU 向多個金融實體發出一個相同請求[79]，可以想見這個過程將耗時又費錢。對於金融行為執行者（多為金融機構）和 FIU 來說，分別處理這些請求更是一種行政負擔。由於這種負擔考量，FIU 不可能將請求發送給所有的金融行行為執行者，而只能發送給那些更有可能有犯嫌個人帳戶的主要銀行。因此，一些帳戶可能被遺漏，罪犯也很容易通過選擇較小的金融行動者來逃避審查。有了銀行登記系統，FIU 就更容易瞭解某一個人與哪些金融機構有聯繫，以及知道應該向哪一個金融機構索取瞭解更多數據資訊[80]。若沒有銀行登記系統，每個有義務的金融實體都必須處理 FIU 的請求，並對是否提供信息給 FIU 進行審查評估[81]。由於 FIU 現在可以直接、毋庸過濾地直接進入系統，因此在 FIU 內部將嚴謹地審核並作出進入登記系統的決定。但相反地，從隱私權保障的角度來看，過於簡便的數據取得過程卻可能存有疑義。

其他國家主管機關亦可查閱銀行登記系統內的資料，以履行其根據反洗錢指令所承擔的義務[82]。在實施銀行登記系統之前，相關主管機關必須通過 FIU 接收信息。現在，某種程度上它們可以直接進入系統加以檢索，但所有對銀行登記系統的查閱都應以「有必要知悉」為基礎

[79] Promemoria, *Genomförande av 2018 års ändringsdirektiv till EU:s fjärde penningtvättsdirektiv*, p 54.

[80] Promemoria, *Genomförande av 2018 års ändringsdirektiv till EU:s fjärde penningtvättsdirektiv*, p 55.

[81] Article 33.1 of the AMLD4; article 1.21 of the AMLD5.

[82] Article 1.19 of the AMLD5.

[83]。雖然存取系統內資料的方式有所不同，但查閱系統內資料的條件與以前的必要條件並無改變，FIU 還能夠按照共享的一般規則將數據傳遞給其他歐盟成員國家中的 FIU 以及第三方[84]。銀行登記系統在按照一般義務的相同規則共享登記的數據資料時，還必須確保安全性和保密性。在這方面，其設計可能比以前的措施更安全。實際上，AMLD4 已經鼓勵銀行登記系統制度，因為它是向主管當局提供數據資料的一種安全、保密的方式。這樣做的一個原因可能是 FIU 不必與每一個金融實體聯繫[85]，這表示將減少金融實體知情，從而保護了數據主體的隱私。

四、歐盟數據保護發展

（一）概說

歐盟於 1995 年通過其第一個保障個人資料指令，以協調該領域的法例，並使保障個人資料在歐盟諸國中更為平等[86]。然而，該指示 95/46/EC 並沒有涵蓋執法當局處理個人資料的事宜[87]。為了填補此一立法上空白，歐盟通過了理事會第 2008/977/JHA 號決定[88]。這兩項法案都在 2016 年通過一項由 GDPR 和 LED 組成的廣泛改革所取代[89]。2016 年的改革旨在進一步協調個人數據保護和有關數據自由流動的

[83] Recital 21 of the AMLD5.

[84] Article 53 of the AMLD4; articles 1.19 & 1.33 of the AMLD5.

[85] Promemoria, *Genomförande av 2018 års ändringsdirektiv till EU:s fjärde penningtvättsdirektiv*, pp 54–55.

[86] Recitals 7 & 8 of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[87] Article 3.2 of Directive 95/46/EC.

[88] Article 1 of Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

[89] Article 1 of the GDPR; recital 15 of the LED.

規則，GDPR 適用於一般的個人資料處理[90]。如前所述，GDPR 作為一項規定直接適用於所有歐盟成員國，自然人可在其國內法院援引。GDPR 載列處理個人資料的一般規則，而 LED 則明定在執法範圍內處理個人資料的規則[91]。當主管當局為預防、調查或偵查刑事罪行等目的處理數據時，僅適用於被告[92]，在這些情況下，需適用 LED 而不是 GDPR[93]。考慮到執法的特殊性，雖然在很大程度上遵循了 GDPR 的原則，但在處理個人數據方面，LED 允許更多的靈活性。正如前面提到的，歐盟個會員國中，各國 FIU 的設置略有不同，這可能會影響它們彼此共享數據信息的可能性，也會影響到銀行登記中的金融數據資料。這是因為各個 FIU 的性質不同，很難確定是應適用 GDPR 的規則，還是應適用 LED 的規則。換言之，雖然各國的 FIU 追求相同目的，但他們可以按照不同的標準處理信息。由於 GDPR 適用於一般的數據處理，而 LED 只在特定情況下適用，所以 LED 應用的標準決定了應該應用什麼框架。其中一項標準是必須由主管當局進行處理[94]。由於 FIU 在不同國家中的性質不同，它們有時被認為是主管當局，有時則不是[95]。因此，GDPR 和 LED 都有可能應用於處理銀行登記系統中的信息。因此，下文將分析 LED 和 GDPR，並討論它們之間的差異。

（二）個人資料、資料控制者及數據保障原則

[90] Article 1 of the GDPR.

[91] Recital 19 of the GDPR; recital 9 of the LED

[92] Article 1.1 of the LED.

[93] Recital 19 of the GDPR; Quintel, *Follow the money, if you can: Possible solutions for enhanced FIU cooperation under improved data protection rules,* p 36.

[94] Article 1.1 of the LED.

[95] Quintel, Follow the money, if you can: Possible solutions for enhanced FIU cooperation under improved data protection rules, p 36.

個人資料是指與已識別或可識別的自然人有關的任何信息[96]。這一定義在 GDPR、LED 和歐洲人權公約當中都是一樣的。相關數據保護規範所載的個人資料包括:個人的姓名、身份證號或者與個人身份經濟有關的資料[97]，這些資料都需要放在銀行的登記系統當中，將數據登載在銀行登記系統內是為了便於識別[98]。身分辨識是個人資料的核心準則，實現這一定義的結果是，GDPR 和 LED 中的規定將與個人數據信息處理相關[99]，上述資料將稱為個人資料，正在被處理數據的個人則被稱為資料當事人[100]。

數據保護法使數據控制者（Data Controller）和處理者（Data Processor）之間有所區別。數據控制者是決定處理目的和方法的實體[101]，它應負責遵守數據保護原則[102];而數據處理者只是一個代表控制者處理數據的實體[103]。反洗錢指令未指定誰是銀行登記系統的數據控制者或數據處理者，因此，這應該是各個歐盟國家可以自行決定。關於取得數據，自然每個主關權責機關將負責他們自己的資料取得行為，因為他們將決定什麼時候，以及為什麼要處理該等數據，對於數據資料的一般存儲，可能更難確定數據控制者應該是誰。誰是數據控制者可視銀行登記系統的設計而定，AMLD5 允許中央儲存登記和中央數據檢索系統，或者兩者兼備[104]。如果設置的是中央檢索系統，則控制人

[96] Article 4.1 of the GDPR; article 3.1 of the LED; Joined Cases C-92/09 and C-93/09, Volker und Markus Scheke GbR and Hartmut Eifert v. Land Hessen, judgment of 9 November 2010, (Scheke), para

[97] Article 4.1 of the GDPR; article 3.1 of the LED.

[98] Article 1.19 of the AMLD5.

[99] Article 1.1 of the GDPR; article 1.1 of the LED.

[100] Article 4.1 of the GDPR; article 3.1 of the LED.

[101] Article 4.7 of the GDPR; article 3.8 of the LED.

[102] Article 5.2 of the GDPR; article 4.4 of the LED.

[103] Article 4.8 of the GDPR; article 3.9 of the LED.

[104] Article 1.19 of the AMLD5.

可能是負責存儲的實體，而主管當局是控制者，負責其查閱及資訊取得。如果選擇了一個中央儲存系統，那麼應該有一個單獨的控制者來管理這個儲存登記系統，在這種情況下，很難確定誰是最合適的控制者。一種可能性是FIU，因為它們可以不經過濾地取得數據信息原貌，儘管它們必須遵守決定存儲目的之相關法律規定。因此，可以想像關於特定數據控制者的部分，將發生難以識別或確定的問題，因為誰應該為遵守數據保護規則負責變得難以釐清。EDPS（European Data Protection Supervisor）還強調了在其對 AMLD5 的意見中識別數據控制者的重要性[105]。數據保護原則在 GDPR 開始時提出，然後在 GDPR 各章節中加以規定，並給出豁免的條件。數據保護的原則是:合法、公平和透明、用途限制、數據最小化、準確性、存儲限制、完整性和機密性[106]。如前所述，雖然 LED 考慮到執法環境的具體性質，但它在很大程度上是基於這些原則和 GDPR 的定義[107]。

（三）銀行登記系統制度與數據保護規範

1.合法性、公平性以及透明度

也許最基本的原則就是合法性。如果數據的依據為 GDPR 第 6 條或 LED 第 1.1 條，則具有合法性[108]。如上所述，為防制洗錢犯行所作的數據處理應符合 GDPR 認可之公共利益[109]。此外，洗錢防制指令的立法目的亦符合 LED 的目的，亦即在於防範刑事犯罪，故而銀行登記系統制

[105] EDPS Opinion 1/2017, para 66.

[106] Article 5 of the GDPR.

[107] Article 4 of the LED.

[108] Article 8.1 of the LED.

[109] Recital 42 & article 1 of the AMLD4; recital 38 & article 1.26 of the AMLD5.

度也可取得合法性。公平性和透明度涉及資料當事人（或稱之為數據主體，Data Subject）有權知道他們的資料在何時，以及為什麼目的而被處理[110]，有關當局應告知資料當事人該等資料將被處理作為反洗錢用途。由於這應在最初進行數據蒐集時告知，義務實體將在其日常工作中增加金融數據於銀行登記系統中處理的內容[111]。這項原則也包括資料當事人的查閱權，不但可查閱所儲存的實際資料，而且可在資料遭處理時獲得通知[112]，惟如果這種獲取行為可能妨礙正在進行中的調查，則可以限制這種權利[113]。在反洗錢指令中，只有在該等通知不能妨礙調查時，才應通知數據主體[114]。如此一來，資料當事人便有可能根據數據保障規則的規定尋求司法補救[115]。對此，反洗錢指令似與 GDPR 和 LED 一致。就銀行登記系統而言，通知資料當事人有關處理的義務尤其重要，由於當局很容易通過銀行登記簿獲得民眾個人生活的概況，因此，在沒有通知的情況下，資料當事人可能會覺得自己處於不斷的監視之下。同時，若會妨害洗錢調查，則可以不通知數據主體。雖然反洗錢指令在這方面似乎符合 GDPR 和 LED，但此通知流程仍可能與歐盟基本權利憲章相衝突。

2.目的性限制

[110] Recital 39 & articles 5.1.a & 12–15 of the GDPR; article 13 of the LED.

[111] Article 13 of the GDPR.

[112] Article 15 of the GDPR; article 14 of the LED.

[113] Article 23 of the GDPR; article 15 of the LED.

[114] Recital 46 of the AMLD4.

[115] Article 79 of the GDPR; article 54 of the LED; recital 46 of the AMLD4.

在反洗錢指令中處理信息的目的也必須遵循目的限制原則。目的限制是指個人資料的收集應出於「明確、明確和合法」的目的，而不是以與該目的不相容的方式處理 。目的必須明確，以便資料當事人能夠預見他們的資料將在什麼時候和為了什麼而被處理。判例法在確定是否符合可預見原則時是很重要的，當涉及到數據的存儲時，反洗錢指令的目的應被視為相當明確，因為數據存儲在銀行登記系統當中便於當局為打擊犯罪而進行查詢，起初將個人資料保留在銀行登記系統內似乎是為了「反洗錢」目的；但是，後續的使用及處理可能會有更多的問題。當 FIU 進入銀行登記系統加以查詢時，其目的似乎也相當明確，因為該權限是為反洗錢目的而創建的。考慮到它們在不同的歐盟國家中看起來是不同的，它們可能仍然有稍微不同的用途，例如執法、管理，抑或兩者兼具[116]。由於 GDPR 和 LED 的不同，他們在某種程度上考慮了這些差異，但反洗錢指令在不同的 FIU 或其他主管部門之間沒有任何區別。

許多不同的單位可以組成主管當局，但稅務機關尤其重要。由於沒有更詳細地規定稅務機關在多大程度上可以實現反洗錢預防目的，因此不清楚這些機關應在多大程度上能夠為此目的獲取個人數據。例如，預防上游犯罪也是預防洗錢的一部分嗎？雖然不同的權責單位為同一目的使用這些數據，但它們也可能對與這一目的相稱的程度有不同的評估。如前所述，AMLD5 中的一些新措施表明，逃稅本身就是一個政策目標，例如，基於稅務當局現在有更多的機會獲取為反洗錢目的

[116] Mohamed, *Legal Instruments to Combat Money Laundering in the EU Financial Market,* p 72.

而蒐集的數據信息[117]。在這種情況下，銀行登記系統制度相當重要，因為它可以使稅務當局直接獲得有關個人的詳細金融資料，這些資料可能有助於打擊逃稅。但仍有論者認為由於這一目的只是說明，並不明確，因此有可能處理數據的目的不符合目的限制原則[118]。

隨後對存儲在銀行登記系統中的數據查詢，可以在單獨的法律基礎上進行處理，但也可以在與初始處理兼容的基礎上進行處理。當 GDPR 和 LED 進一步定義如何確定後續處理的目的是否與初始處理的目的相一致時，兩者是不同的。在 GDPR 中，有一個應該考慮的因素列表，例如目的之間的聯繫、蒐集數據的環境以及處理的可能結果[119]。而在 LED 中，有關標準的條文規範並不精確，其僅表示如數據控制者獲授權處理該等數據，而該等數據是為完成其他目的而必須且適當的，則該條文只敘明該目的是相容的[120]。與 GDPR 相比，當局似乎有更多的自由裁量權來決定處理是否符合 LED。這在執法中可能是必要的，蓋為了有效地調查犯罪可能需要更大靈活性，此種差異會影響不同 FIU 之間的共享，因為它們會根據不同的標準交換數據信息。

跨國界的信息共享也會使處理目的界線變得模糊。由於適合性（compatibility）可能在某些國家是中根據 GDPR 進行評估，而在另一些國家中則是根據 LED 進行評估，所以被認為達到適合性的標準可能會不同[121]。因為反洗錢指令並未清楚指出何種目的屬於合適，因而

[117] EDPS Opinion 1/2017, para 18.

[118] EDPS Opinion 1/2017, para 31.

[119] Article 5.1.b of the GDPR; article 4.1.b of the LED.

[120] Article 4.2 of the LED.

[121] Quintel, Follow the money, if you can: Possible solutions for enhanced FIU cooperation under improved data protection rules, p 46.

無助於不同國家之間相岐異的標準，但這不應妨礙相關數據信息的交換[122]。因此，不同的歐盟國家可能會對稅務犯罪的嚴重性有不同的看法，與目的限制相關的反洗錢指令的問題在於目的不夠具體。這也會影響與數據最小化原則相關的比例性評估。

3.數據最小化原則

在處理個人資料時，亦必須達到上述目的，即公眾利益。只有在用其他方法不能達到目的時，這種處理才是必要的，此一原則被稱為數據最小化（Data Minimisation）。與數據最小化相關的還有存儲限制原則，數據最小化原則在 GDPR 和 LED 中有所不同。LED 不要求數據處理必須與加工目的相關聯，而是要求於目的範圍內進行數據處理[123]，可以說 LED 對於數據處理所需的門檻低於 GDPR。根據數據最小化原則，銀行登記系統中存儲的數據信息應限於必要或不過度者，如前所述，引進銀行登記系統目的是考量偵查和調查犯罪的過程。因此，數據的儲存應與實現這一目標成比例。需要儲存在銀行登記的資料，例如 IBAN 和個人身分證號碼應認為是必須的登記內容，因為它提供了一個對於數據主體的概覽。如前所述，各個歐盟成員國還可以在銀行登記簿中包含他們認為必要的其他數據，然而反洗錢指令並未明確哪些內容應被視為必要，或應如何進行評估。

FIU 和主管當局的權限也應限於必要的範圍，其擁有直接且未經過濾的數據取得權限，而主管當局則擁有履行其在反洗錢指令所規範下取得數據權限之義務。如果取得數據資料之目的不清楚，則很難加以評

[122] Article 1.36 of the AMLD5.

[123] Recital 26 & article 4.1.c of the LED.

斷是否符合上開所述之符合比例的最小化數據要求。銀行登記系統中的信息獲取是基於「需要知道」的基礎，這表明應進行某種比例原則檢驗，但反洗錢法指令並未具體規定應考慮哪些事實。由於有些措施可能與打擊恐怖主義成正比，而與打擊稅務犯罪不成比例，如果這兩者都是反洗錢指令目的，立法者應更清楚指出哪些基於反恐怖主義或者稅務犯罪基礎上是必要的，哪些是不逾越必要手段的。

4.準確性原則

準確性原則是指個人資料必須隨時更新，而不準確的資料必須予以刪除或更正[124]，蓋若數據的準確性受到資料當事人的質疑，處理工作也會受到限制[125]。在反洗錢指令中似乎沒有任何規則與數據保護法中的這一義務相衝突，為了進行有效的調查，銀行登記系統上的資料必須是最新並正確的。

5.儲存的限制

GDPR 和 LED 都規定了數據存儲限制的原則[126]。這部分的「刪除權」是指當收集個人資料的目的不再需要時，有關的個人資料必須被刪除或匿名，數據控制者必須根據 GDPR 以及 LED，規劃定期覆核及清除的時限[127]。如前所述，處理銀行登記系統內的資料須有五年時限，也有可能再延長五年；反觀反洗錢指令並未規定任何延展數據保留時限的標準，其規定無庸視個案情形決定數據保留時限是否展延，因此展延

[124] Article 5.1.d of the GDPR; article 4.1.d of the LED.

[125] Article 18.1.a of the GDPR; article 16.3.a of the LED.

[126] Article 5.1.e of the GDPR; article 4.1.e of the LED.

[127] Recital 39 of the GDPR; recital 26 & article 5 of the LED.

似乎可以是一般通用的，無需考慮在個案單獨的情況下需要什麼[128]。從而，反洗錢指令和數據保護法之間可能產生衝突，因為後者要求數據的保存時間不得超過必要時間。如果在每種情況下都沒有對「保存必要性」進行評估，就不可能知道在這種情況下擴展實際上是否有其必要。在這種情況下，還有一個衝突，即最初的五年保留期是出於對數據保護的考慮而選擇的。法律應規定延長保留期間的一般依據，因此可以認為，立法者應考慮到在不同情況下的需要。然而，反洗錢法指令似乎並未要求法律應考慮哪些參數是必要的，而只是簡單地規定了一般應延長保留期限。

LED 規定有時數據資料可能會受到限制而非刪除，例如個人資料必須保存作為證據之用[129]，然而這一規則在 GDPR 中則沒有相應的規定，這表明 LED 基於執法特殊性而作出不同的立法考量。儘管反洗錢指令並未聲明任何與延長數據保存期限相關的限制，在此背景下，似乎銀行登記系統的保留期設置可能與 GDPR 和 LED 的存儲限制原則存在潛在衝突。

6. 完整性和機密性

完整性和保密性的原則也被納入數據保護法[130]。在實施這些措施時，數據控制者應考慮某些方面，如數據的性質和不同的風險[131]。雖然須實施的安全措施有所不同，但在這方面，GDPR 與 LED 並無顯著差異。

---

[128] Recital 21 of the AMLD5.

[129] Article 16.3.b of the LED.

[130] Recital 39 & article 5.1.f of the GDPR; recital 28 & article 4.1.f. of the LED.

[131] Article 32 of the GDPR; article 29 of the LED.

反洗錢指令中規定了一些安全措施，如保密措施以及應制定數據的其他安全措施。這些措施未作進一步規定，但由於反洗錢指令也應符合數據保護法律，歐盟各國在引入銀行登記系統制度時必須遵循 GDPR 和 LED 中的標準。因此在現階段，數據保護法中的規定與反洗錢指令中的規定似乎並無任何衝突

五、我國洗錢防制法與隱私權之衝突與調和

如同本文上開所述，我們已經發現了銀行登記系統與 GDPR 和 LED 之間的一些潛在問題。其中之一是對保留期限的延長沒有明確的規定。另一個是某些處理的目的不明確，這也會影響對特定情況下的處理是否成比例的評估。此外，關於誰是數據控制者還是存有不確定性，因此很難認定誰應對遵守數據保護法負責。反觀關於合法、公平和透明以及誠實和保密的原則部分似乎沒有衝突發生的疑慮。

（一）我國洗錢防制法新增部分

我國洗錢防制法於 2016 年 12 月 28 日修正通 過，在本次修正中主要參考國際防制洗錢金融行動小組(Financial Action Task Force on Money Laundering, FATF)所制定的四十點建 議所為的修正。以下對於本次新修正後的洗錢防制法相關重點，如下加以簡要說明:

一、在立法目的上增加「促進金流之透明，強化國際合作」，其顯然擴大打擊面，並與稅捐稽徵法第五條之一，未來可能導入的國際

稅務資訊「共同申報準則」(Common Reporting Standard, CRS)的稅務資訊透明相呼應。

二、本次修法中擴大「洗錢」行為的定 義，其包含下列三種行為類型:∶(一)意圖掩飾或隱匿特定犯罪所得 來源，或使他人逃避刑事追訴，而移轉或變更特定犯罪所得。 (二)掩飾或隱匿特定犯罪所得之本 質、來源、去向、所在、所有 權、處分權或其他權益者。 (三)收受、持有或使用他人之特定犯罪所得。

三、降低對於「犯罪」的定義，包含最輕本刑為六月以上有期徒刑以上之罪，同時並擴及商標法、廢棄物清理法、 稅捐稽徵法、電子支付機構管理條例 的相關刑事責任規定。另外，對於犯 罪所得的門檻規定亦予以刪除。

四、擴大申報義務的規範對象,包含非金 融事業或人員(例如銀樓業、律師、 信託等)，使得規範在主體的打擊面 更為擴張。

五、申報義務人對於其客戶身分的確認， 確認客戶身分程序應以風險為基礎， 並包括實質受益人之審查。同時對於 對現任或曾任國內外政府或國際組織 重要政治性職務之客戶或受益人與其家庭成員及有密切關係之人,亦以風 險為基礎,加強審查程序。

六、交易紀錄的保存，應至少保存五年。

七、增列對於特定前置行為的特殊洗錢罪，有下列特定類型之前置行為之一，而其金流無合理來源，且與收入顯不相當，則其亦受到本法的規範:(一)冒名或以假名向金融機構申請 開立帳戶。(二)以不正方法取得他人向金融機 構申請開立之帳戶。 (三)規避第七條至第十條所定洗錢防制程序。

八、對於疑似犯本法所規定的犯罪(包含特殊洗錢罪)，金融機構及指定之非金融事業或人員，其申報義務人有向法務部調查局申報之義務。

九、對於高風險國家或地區的強化措施如下所列:(一)命金融機構強化相關交易之確 認客戶身分措施。(二)限制或禁止金融機構與洗錢或資恐高風險國家或地區為匯款 或其他交易。(三)採取其他與風險相當且有效之必要防制措施。

十、本法所規定的犯罪，均處罰未遂犯。

十一、關於犯罪所得的沒收規定，其包含 洗錢行為標的之財物或財產上利 益，同時對於集團性或常習性的非 本案其他財物或財產利益，係取自 其他可能違法行為所得者，得擴大 沒收之。

（二）隱私權於我國之法律位階

隱私權雖未明文規範在我國憲法條文中，成為列舉之基本權，但在釋憲實務上，司法院大法官解釋從釋字第 293、509、535、585、603 到 689 號解釋，大法官在釋憲上一再的肯認隱私權為我國憲法保障之基本權之一。該六則大法官解釋大致建構出我國憲法保障下的隱私權範。以下將先為各號解釋內容之介紹後，再為簡單的區分：

1. 司法院大法官釋字第 293 號解釋

（1）銀行法雖有保障隱私權之規定，但有例外：

「銀行法第四十八條第二項規定「銀行對於顧客之存款、放款或匯款等有關資料，除其他法律或中央主管機關另有規定者外，應保守秘密」，旨在保障銀行之一般客戶財產上之秘密及防止

客戶與銀行往來資料之任意公開，以維護人民之隱私權。惟公營銀行之預算、決算依法應受議會之審議，議會因審議上之必要，就公營銀行依規定已屬逾期放款中，除收回無望或已報呆帳部分，仍依現行規定處理外，其餘部分，有相當理由足認其放款顯有不當者，經議會之決議，在銀行不透露個別客戶姓名及議會不公開有關資料之條件下，要求銀行提供該項資料時，為兼顧議會對公營銀行之監督，仍應予以提供。」

2.司法院大法官釋字第509號解釋

（1）言論自由應兼顧隱私權：

「言論自由為人民之基本權利，憲法第十一條有明文保障，國家應給予最大限度之維護，俾其實現自我、溝通意見、追求真理及監督各種政治或社會活動之功能得以發揮。惟為兼顧對個人名譽、隱私及公共利益之保護，法律尚非不得對言論自由依其傳播方式為合理之限制。」

（2）真實者不罰：

「刑法第三百十條第一項及第二項誹謗罪即係保護個人法益而設，為防止妨礙他人之自由權利所必要，符合憲法第二十三條規定之意旨。至刑法同條第三項前段以對誹謗之事，能證明其為真實者不罰，係針對言論內容與事實相符者之保障，並藉以限定刑罰權之範圍，非謂指摘或傳述誹謗事項之行為人，必須自行證明其言論內容確屬真實，始能免於刑責。惟行為人雖不

能證明言論內容為真實，但依其所提證據資料，認為行為人有相當理由確信其為真實者，即不能以誹謗罪之刑責相繩，……」

3. 司法院大法官釋字第 535 號解釋

（1）法律明確性原則：

「執行各種臨檢應恪遵法治國家警察執勤之原則，實施臨檢之要件、程序及對違法臨檢行為之救濟，均應有法律之明確規範，方符憲法保障人民自由權利之意旨。」

（2）臨檢與隱私權之衝突：

「除法律另有規定（諸如刑事訴訟法、行政執行法、社會秩序維護法等）外，警察人員執行場所之臨檢勤務，應限於已發生危害或依客觀、合理判斷易生危害之處所、交通工具或公共場所為之，其中處所為私人居住之空間者，並應受住宅相同之保障；對人實施之臨檢則須以有相當理由足認其行為已構成或即將發生危害者為限，且均應遵守比例原則，不得逾越必要程度，儘量避免造成財物損失、干擾正當營業及生活作息。」

4. 司法院大法官釋字第 585 號解釋

（1）立法院調查權與隱私權之衝突：

立法院調查權之行使，依調查事項及強制方式之不同，可能分別涉及限制多種受憲法保障之人民基本權利，如憲法第八條保障之人身自由、憲法第十一條保障之消極不表意自由（本院釋字第五七七號解釋參照）、憲法第十二條保障之秘密通訊之自

由、憲法第十五條所保障之營業秘密、隱私權……等等。其中隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活秘密空間免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第二十二條所保障（本院釋字第五〇九號、第五三五號解釋參照）。」

5.司法院大法官釋字第 603 號解釋

（1）資訊隱私權：

「維護人性尊嚴與尊重人格自由發展，乃自由民主憲政秩序之核心價值。隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第二十二條所保障（本院釋字第五八五號解釋參照）。其中就個人自主控制個人資料之資訊隱私權而言，乃保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權。惟憲法對資訊隱私權之保障並非絕對，國家得於符合憲法第二十三條規定意旨之範圍內，以法律明確規定對之予以適當之限制。」

（2）指紋乃個人隱私資訊：

「指紋乃重要之個人資訊，個人對其指紋資訊之自主控制，受資訊隱私權之保障。而國民身分證發給與否，則直接影響人民基本

權利之行使。戶籍法第八條第二項規定：依前項請領國民身分證，應捺指紋並錄存。但未滿十四歲請領者，不予捺指紋，俟年滿十四歲時，應補捺指紋並錄存。第三項規定：請領國民身分證，不依前項規定捺指紋者，不予發給。對於未依規定捺指紋者，拒絕發給國民身分證，形同強制按捺並錄存指紋，以作為核發國民身分證之要件，其目的為何，戶籍法未設明文規定，於憲法保障人民資訊隱私權之意旨已有未合。縱用以達到國民身分證之防偽、防止冒領、冒用、辨識路倒病人、迷途失智者、無名屍體等目的而言，亦屬損益失衡、手段過當，不符比例原則之要求。」

6. 司法院大法官釋字第 689 號解釋

（1）隱私權原則應不受侵擾：

「蓋個人之私人生活及社會活動，隨時受他人持續注視、監看、監聽或公開揭露，其言行舉止及人際互動即難自由從事，致影響其人格之自由發展。尤以現今資訊科技高度發展及相關設備之方便取得，個人之私人活動受注視、監看、監聽或公開揭露等侵擾之可能大為增加，個人之私人活動及隱私受保護之需要，亦隨之提升。是個人縱於公共場域中，亦應享有依社會通念得不受他人持續注視、監看、監聽、接近等侵擾之私人活動領域及個人資料自主，而受法律所保護。惟在公共場域中個人所得主張不受此等侵擾之自由，以得合理期待於他人者為限，亦即不僅其不受侵擾之期待已表現於外，且該期待須依社會通念認

為合理者。系爭規定符合憲法課予國家對上開自由權利應予保護之要求。」

7.隱私權的保護範圍

司法院大法官關於隱私權的解釋中，前三者解釋僅提及隱私權，未加闡釋。後三者的解釋文及解釋理由書則作較詳細的論述，即：「維護人性尊嚴與尊重人格自由發展，乃自由民主憲政秩序之核心價值。隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第二十二條所保障。」本斷解釋文闡明隱私權的價值理念在維護人格尊嚴、個人主體性之維護及人格發展自由。所謂「生活私密領域免於他人侵擾」，乃傳統古典意義的隱私權。「個人資料之自主控制」，乃在肯認資訊社會，個人的自主權利。

學者試將隱私權定義為：個人對其私領域的自主權利，分三點言之：

1.此項概念建立在司法院大法官釋字第 603 號解釋所提出隱私權的人格尊嚴及自由發展的價值理念上。

2.隱私權係由二個核心因素構成之，一為私領域，一為自主權利。私領域指個人私生活的範疇。自主權利指個人得自主決定如何形成其私領域的生活。隱私權的主體為個人，但亦有擴大及於法人團體的趨勢。其保障範圍包括：（1）「私生活不受干擾」，即個人得自主決定是否及如和公眾引退、幽居或獨處，而保有自我內在空間，可稱為空間隱私。（2）「資訊自主」，即得自主決定是否及如何公開關於其個

人的資料（資訊隱私）。二者乃隱私權個別化的保護範圍，屬個別隱私權。

3.在我國釋憲實務上屬資訊隱私（資訊自主）者，如銀行存款等資料（釋 293），指紋（釋 603）。警察執行臨檢執勤或真調會條例第 8 條第 6 項所涉及的隱私，得包括空間隱私或資訊隱私。

（三）小結

根據上開我國大法官解釋，隱私權於我國居於人民基本權地位應係毋庸置疑，該等解釋亦符合當今世界潮流。觀之《歐洲保障人權和基本自由公約》（Convention for the Protection of Human Rights and Fundamental Freedoms）第 8 條規定每個人的「私人及家庭生活、其家庭以及其通訊隱私」的權利與自由必須受到尊重，若需要對此做出限制，則必須「符合法律規定」且「為民主社會所必需」[132]。而參照我國個人資料保護法立法理由多次提及參酌歐洲保障人權和基本自由公約，應可解釋為該法認同將隱私權定性為人民基本權。經由比較上開歐盟數據保護法 GDPR 以及 LED 與反洗錢指令內容，確實得出部分實際運作可能發生衝突之處。然而，就我國司法實務而言，民國 106 年 01 月 26 日由法務部發佈之法律字第 10603501350 號函示:『金融機構利用集保公司統一建置資訊系統，將保有客戶資料與洗錢防制名單進行比對，乃在發揮洗錢防制名單資料庫最大效應，以落實洗錢

[132] 本條明確的規定，每個人皆有免於受到非法搜索的權利；另一方面，歐洲人權法院就公約中所規定的「私人及家庭生活」做出了相當廣闊的解釋以保護此等權利。此與美國聯邦最高法院的見解相比較，其對隱私權採取了相當廣闊的解釋。更有進者，本條亦課予了國家「積極義務（Positive obligations）」：儘管傳統對於人權的保護通常被解釋為禁止國家干涉這些權利，且因此而必須要採取「不作為」的態度（譬如說，基於家庭生活的保護，不能任意的拆散一個家庭），但要能實質的享受此等權利有時必須要課予國家更積極的義務，且必須要有所「作為」（譬如說，使離婚的配偶有接近其小孩的方式）。

防制要求,應可認符合個人資料保護法 20 條第 1 項但書第 2 款「增進公共利益所必要」,而得為原契約目的必要範圍外利用』。似指應以洗錢防制工作為優先,蓋此可解釋為符合公共利益而取得正當法律依據。

參、自動決策機制於犯罪偵查運用之探討

一、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。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。

二、概說

在犯罪日益增多的今天，預防犯罪已成為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[133]。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，法律措施針對自動個人化決策施加了限制，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

[133] 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.

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[134]，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[135]。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，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[136]。

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

---

[134] 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

[135] 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.

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

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[137]。

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化決策系統（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取得平衡。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又一次的里程碑[138]，可以想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現行立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

---

[137] 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。

[138] 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。

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》（GDPR），以及《執法指令》(Law Enforcement Directive 2016/680,LED)組成，此二者均業於 2018 年 5 月 6 日生效實施。LED 乃專門適用於司法、偵查單位處理用於執法目的的個人數據的規則，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」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，資料控制（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[139]，不論如何，目前歐盟成員國內的公民根據上開 GDPR 規範，擁有請求取得相關數據訊息的權利。以下將進一步介紹 GDPR 以及 LED 對於自動化個人決策的規範及限制。

三、歐盟對於自動化決策相關規範

[139] 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.

（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[140]。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[141]」。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[142]。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[143]。」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

[140] Art 22(1) GDPR

[141] Thomas H Coormen, Algorithms Unlocked (MIT Press 2013) 1.

[142] 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.

[143] 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。

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[144]。

此外，在 GDPR 舉例說明第 71 點[145]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，資料控制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權利，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[146]：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意義的，並具有邏輯性[147]。簡言之，當人民提出請求希

---

[144] 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。

[145] 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.

[146] 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.

[147] Article 29 Working Party

Meaningful information about the 'logic involved'

望得到更多關於自動決策結果時，數據控制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，以及做成該決定所依憑的標準。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[148]。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[149]。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控制者、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

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.

[148] 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

[149] LED Article 11 (automated individual decision-making)

1. Member States shall provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller.

取授權歐盟成員國各自以內國法律授權的方式[150]，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。

四、資料主體解釋權

歐洲學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權。GPDR 第 13 條第 2 項（f）[151]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）[152]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)」。

---

[150] 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.

[151] 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.」

[152] 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.」

除此之外，GDPR 第 15 條第 1 項（h）[153]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[154]；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[155]；反之，亦有學者認為前揭 GDPR 第 22 條以及第 13 條至第 15 條僅規範資料控制者「通知義務」以及資料主體對於數據資料之「取得使用權」。事實上，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 相關條文中明定出現，資料控制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[156]。

反觀 LED 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;所有其他可能得以賦予資料主體的額外

[153] 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.」

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

[155] 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.

[156] 唯一明確提到解釋權的為 Recital 71。

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自動決策對民眾個人的影響，這種限縮 LED 適用範圍的結果將影響民眾權利甚鉅。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歐盟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[157]。

五、小結

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。否則一昧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前揭所介紹之歐盟相關立法例，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

[157]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 .

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。試想於歐盟現有保障隱私權制度如此嚴密情況下，仍會發生上述倫敦警方濫權事件，殊難想像若一味發展犯罪預測機制而忽略等同重要之人民隱私權保護措施，未來可以完全避免犯罪預測制度侵害人民隱私權之爭端。

肆、結論暨建議

本文主要研究在反洗錢作為暨銀行登記系統制度與個人數據保護之間的潛在衝突。在反洗錢指令與 GDPR、LED 之間，已經確定了若干此類潛在衝突。根據 GDPR 規定，只要關於歐盟境內以及歐盟公民（即使在歐盟境外）的私人數據資料蒐集、處理均需適用 GDPR；又我國身為艾格蒙聯盟（The Egmont Group）正式會員，與外國 FIU 交換洗錢防制情資同時，確實有相當大機會處理關於歐盟公民數據而擔任數據控制者角色，故而吾人無法自身事外，瞭解 GDPR 以及該等數據隱私保障規範與洗錢防制作為之間如何操作兼顧得當，乃當務之急。蓋違反 GDPR 最高可處以 2000 萬歐元罰鍰[158]。

[158] 依照 GDPR 第 83 條第 4 項及第 5 項規定，對於違反本規則者，可能會被處以 1000 萬至 2000 萬歐元，或全球年營業總額 2%至 4%的罰款，處罰金額十分的龐大。並會依案件違反情節而給予不同程度的裁罰，舉例說明：發生個人資料外洩事件時，如果企業沒有合法理由而遲延向監管機關進行通報，依 GDPR 規定最高將可能被處以 1000 萬歐元或前一會計年度全球年營業額之的 2%的罰款，兩者金額以較高者為準；另外，如果有違法向第三國傳輸個人資料、違反 GDPR 與資料主體權利有關之規定(第 12 條至第 22 條)等情形，最高將被處以 2000 萬歐元或前一會計年度全球年營業額之的 4%的罰款，兩者金額以較高者為準。又，GDPR 於前言 149 及 150 中表示，違反 GDPR 者除了可能遭受行政罰鍰之處罰外，歐盟會員國對於違反 GDPR 者，可在 GDPR 的規定及其所限制之範圍內調整制定內國法，對於違反規定者，可擬定刑罰規範，該等刑罰亦得允許沒入違反規定者所獲得之利益。此外，GDPR 第 82 條亦明白揭示任何資料主體因資料控制者或資料處理者違反 GDPR 規定而導致其受有損害時，不論是實質或精神損害，都可以向其請求損害賠償。詳請參閱 GDPR §82、§83(2) (4) (5)以及 GDPR recital §149、§150。參見" GDPR 規範嚴格懲處條例，違反者將處以鉅額罰金與刑罰"，https://www.acw.org.tw/Events/Detail.aspx?id=22，瀏覽日期：2019 年 9 月 6 日。

事實上，歐洲部分法律實務工作者認為基於洗錢防制為今日世界趨勢，基於優先理論，可以直接援引 GDPR 第 6 條（C）及同條文（F）作為洗錢防制下關於私人金融數據資料之蒐集處理的法律基礎[159]。

反觀我國是否也會發生洗錢防制作為，例如相關的金融數據蒐集與分析，跟個人資料保護法衝突的情形？依據目前法務部法律字第 10603501350 號函示內容，任何洗錢防制工作似乎均可藉由認符合個人資料保護法第 20 條第 1 項但書第 2 款「增進公共利益所必要」而得為原契約目的必要範圍外利用。再者，我國個人資料保護法亦尚未全盤繼受歐盟 GDPR 或 LED，因此，目前我國基於洗錢防制目的之相關個人數據使用，應不至於遭認定侵犯人民隱私權[160]。

值得注意者，反洗錢目的要求私人金融數據進行相關蒐集分析，但 GDPR 卻要求個人數據處理最小化（Data Minimization），未來操作上可以想見可能出現兩者扞格之處。金融機構是否於執行處理分析客戶數據時是否都能嚴格遵循僅就反洗錢相關的數據加以處理？尚有待觀察。又 GDPR 明示揭櫫個人數據資料僅能使用於蒐集之最初目的使用，然而關於反洗錢措施及採行銀行登記制度的總體問題是它們對於金融數據使用目的解釋太廣泛，我們應該瞭解，銀行登記系統是一種新的金融數據處理方式，因為它可以對一個人的經濟活動有一個全面的瞭解，也可以對這個人的生活得出廣泛的結論。再者，FIU 和其他當局獲得這些資料的可能性非常大，且他們獲得這些資料的目的並

[159] Article 6(c) – which allows for the processing of personal data "for compliance with a legal obligation to which the controller is subject" – typically, AML laws or sanctions.
Article 6(f) – which allows for data processing for "legitimate interests", justifiable on a case-by-case basis.

[160] 然而，本文認為既然隱私權在我國被視為人民基本權之一種，對於我國人民個人資料數據之運用必須符合原本的預設目的，若主管當局欲就相同數據作其他目的使用，應盡到告知責任，惟若事先告知數據主體將造成妨礙金融犯罪偵查程序，亦應於事後加以告知，方可謂善盡隱私權保護。

不總是明確的，此潛在風險在於它變得不清楚是為了什麼目的處理數據？什麼時候處理與實現這個目的是成比例的。這些問題主要與用途限制、數據最小化和存儲限制的原則相衝突。2019 年 7 月 11 日，歐盟發佈了 2019/1153326 號指令，該指令為利用金融信息打擊犯罪制定了更具體的規則。它提供了一些關於在銀行登記簿中獲取信息的新規則[161]。初步看來，一些新規則有望解決本文所探討的一些問題，例如某些數據信息的取得限制和有關當局得以獲取個人數據的條件。準此，建議國內金融機構主管機關以行政函示，明確指導銀行於操作反洗錢相關措施並牽涉處理客戶金融數據時，遵循上開數據保護規範，而我國調查局或其他單位擔任 FIU 角色時，更應確實遵守上開 GDPR 相關規範，俾利以合規方式進行私人數據資料處理分析。

未來，自動化決策機制必定與金融犯罪，乃至於一般刑事犯罪案件偵辦或預防息息相關。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，未來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

[161] 請參閱：https://eur-lex.europa.eu/eli/dir/2019/1153/oj，瀏覽日期：2019 年 10 月 10 日。

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、處理及使用，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。