專題研析

營業秘密之「合理保密措施」要件與其認定—美國經濟間諜法判決之借鏡

國立政治大學科技管理與智慧財產研究所副教授 陳秉訓

摘 要

營業秘密法第 13 條之 1 和第 13 條之 2 分別就非法取得、洩漏或利用營業秘密、及意圖在境外使用而為該些非法行為等行為處以刑事懲罰。不過，成立刑事責任之前提是系爭營業秘密須符合相關要件，例如被害人應對系爭秘密採取「合理保密措施」。本文以美國《經濟間諜法》（Economic Espionage Act，EEA）之相關刑事判決為借鏡，就「合理保密措施」之認定，對我國司法實務和刑事偵察實務提出建言。

關鍵字：營業秘密、經濟間諜法、合理保密措施、獨立經濟價值、著手犯

Determining Reasonable Measures to Protect Trade Secrets—What Can We Learn from U.S. Cases Concerning the Economic Espionage Act

Ping-Hsun Chen

Abstract

In order to find a defendant accused of trade secret misappropriation criminally liable, one must prove that the disputed trade secret meets three requirements one of which is a reasonable measure to maintain secrecy under the Taiwan Trade Secret Act. This article is intended to introduce three criminal cases concerning the Economic Espionage Act of the United States and to provide any implications from those cases to improve the determination of reasonable measures in Taiwan.

Keywords: Trade Secret, Economic Espionage Act, Reasonable Measure to Protect Secrecy, Independent Economic Value, Attempt

壹、前言

為享有營業秘密法的保護，權利人必須證明其據以主張之營業秘密符合三個要件：（1）秘密性：非一般涉及該類資訊之人所知者；（2）價值性：因其秘密性而具有實際或潛在之經濟價值者；（3）合理保密措施：所有人已採取合理之保密措施者[1]。否則，例如於

[1] 營業秘密法第 2 條；楊智傑，《智慧財產權法》，新學林，2019 年 6 月，3 版 1 刷，445 頁；趙晉枚、蔡坤財、周慧芳、謝銘洋、張凱娜，《智慧財產權入門》，元照，2003 年 3 月，2

「重製、取得、使用、洩漏他人營業秘密罪之判斷」（營業秘密法第 13 條之 1）中，「如其秘密，僅屬抽象原理、概念，並為一般涉及相關資訊者經由公共領域所可推知，或不需付出額外的努力即可取得相同成果，或未採取交由特定人管理、限制相關人員取得等合理保密措施」時，則無法使被告成罪[2]。

就「合理保密措施」，根據最高法院 102 年度台上字第 235 號民事判決，其係指據以主張之營業秘密之「所有人按其人力、財力，依社會通常所可能之方法或技術，將不被公眾知悉之情報資訊，依業務需要分類、分級而由不同之授權職務等級者知悉而言」；若「於電腦資訊之保護，就使用者每設有授權帳號、密碼等管制措施，尤屬常見」[3]。此類資訊接觸管制措施，根據最高法院 107 年度台上字第 2950 號刑事判決，「除有使人瞭解秘密所有人有將該資訊當成秘密加以保密之意思，客觀上亦有保密之積極作為」[4]。

另根據最高法院 108 年度台上字第 36 號民事判決，審查「是否達合理之程度」時「應衡酌該營業秘密之種類、事業實際經營情形及社會共識或通念」等因素，而「依具體個案之情形而為判斷」；故「如客觀上足使一般人以正當方法無法輕易探知，即難謂非合理之保密措施」[5]。再者，近期最高法院於 108 年度台上字第 1608 號刑事判決認可二審法院「合理保密措施」之判斷原則，其為「營業秘密所有人已盡合理之努力，使他人無法輕易取得、使用或洩露該營業秘密，亦即營業秘密所有人主觀上有保護之意思，且客觀上已採取保密作為為已足，並不以保密作為達到『滴水不露』之程度為必要」；於判斷時，視「營業秘密所有人依其人力、財力及營業資訊之性質，以社會通常可能之方法或技術，以不易被任意接觸之方式加以控管，而能達到保密之目的者」即

版 2 刷，206-207 頁；王偉霖，《營業秘密法理論與實務》，元照，2015 年 4 月，初版 1 刷，33 頁（稱本文之「秘密性」為「新穎性」，而「合理保密措施」為「秘密性」）。司法實務上，最高法院曾於 99 年度台上字第 2425 號民事判決稱秘密性、經濟價值、及保密措施等。參見最高法院 107 年度台上字第 2950 號刑事判決 / 理由 / 二：「首須確定營業秘密之內容及其範圍，並就行為人所重製、取得、使用、洩漏涉及營業秘密之技術資訊是否具備秘密性、經濟價值及保密措施等要件逐一審酌」。

2 最高法院 107 年度台上字第 2950 號刑事判決 / 理由 / 二。

3 最高法院 102 年度台上字第 235 號民事判決 / 理由。

4 最高法院 107 年度台上字第 2950 號刑事判決 / 理由 / 二。

5 最高法院 108 年度台上字第 36 號民事判決 / 理由。

可[6]。

在智慧財產及商業法院（稱「智商法院」）過往的營業秘密法刑事判決中[7]，有肯定被害人已完備合理保密措施者[8]，亦有否定系爭營業秘密受到合理保密措施之保護者[9]。針對合理保密措施遭否定的案例，本文欲以美國《經濟間諜法》（Economic Espionage Act，EEA）之相關刑事判決為借鏡，對我國司法實務和刑事偵察實務提出建言。以下本文先介紹 EEA 和相關上訴法院判決；再介紹智商法院相關判決；最後，再提出兩點建議。

貳、美國經濟間諜法相關判決之介紹：以合理保密措施為中心

一、經濟間諜罪與竊取營業秘密罪

美國於 1996 年制訂 EEA 用以制裁國際和國內的經濟間諜活動[10]。EEA 的罪刑有二類，即經濟間諜罪（18 U.S.C. § 1831）及竊取營業秘密罪（18 U.S.C. § 1832）[11]。

二類罪刑之共同處為皆由主觀要件與行為要件所組合，但差異是主觀要件內涵有異。關於主觀要件，經濟間諜罪要求被告具有圖利外國政府、外國政府所控制之單位、與外國代理人之意圖或

---

6 最高法院 108 年度台上字第 1608 號刑事判決 / 理由 / 四 /（二）/ ②。

7 智慧財產法院刑事判決中涉及其他爭點者包括秘密性（108 年刑智上訴字第 37 號、106 年刑智上訴字第 40 號、108 年刑智上訴字第 1 號、106 年刑智上訴字第 39 號、106 年刑智上訴字第 38 號）、量刑（109 年刑智上訴字第 8 號、108 年刑智上訴字第 6 號、108 年刑智上訴字第 3 號、107 年刑智上訴字第 20 號、107 年刑智上訴字第 5 號）、證據（109 年刑智上訴字第 18 號、107 年刑智上訴字第 23 號）、告訴人適格性（108 年刑智上訴字第 5 號、104 年刑智上訴字第 52 號）、故意（106 年刑智上訴字第 30 號）、法人犯罪（106 年刑智上訴字第 29 號）、管轄權（103 年刑智上訴字第 41 號）。

8 相關智慧財產法院刑事判決包括 109 年刑智上重訴字第 9 號、108 年刑智上訴字第 50 號、107 年刑智上訴字第 43 號、109 年刑智上重訴字第 3 號、109 年刑智上訴字第 12 號、109 年刑智上訴字第 2 號、107 年刑智上訴字第 4 號、107 年刑智上訴字第 13 號、107 年刑智上訴字第 14 號、105 年刑智上訴字第 35 號。

9 相關智慧財產法院刑事判決包括 108 年重附民上字第 10 號、108 年刑智上訴字第 52 號、108 年刑智上訴字第 43 號、107 年刑智上訴字第 19 號、107 年刑智上訴字第 24 號、107 年刑智上訴字第 18 號、106 年刑智上訴字第 17 號、105 年刑智上訴字第 11 號、104 年刑智上訴字第 61 號。

10 *See* United States v. Hsu, 155 F.3d 189, 194（3d Cir. 1998）.

11 王偉霖，前註 1 書，231 頁。

知悉[12]。竊取營業秘密罪的主觀要件有三項：（1）意圖將營業秘密轉化為非所有人之經濟利益；（2）營業秘密係關於商品或服務，且該商品或服務係使用於或欲使用於州際或外國商務；（3）意圖或知悉其犯行會傷害營業秘密所有人[13]。

在行為要件部分，二類罪刑在制裁的犯行包括五種：（1）偷竊實體；（2）複製內容；（3）明知違法而取得；（4）著手從事前述三種行為；（5）共謀從事第一種至第三種之行為，且其中一位共謀者為了共謀的目標而已採取行動[14]。又二類罪刑於此部分之差異是經濟間諜罪要求證明被告知悉（knowingly）其所得到的資訊是營業秘密，但竊取營業秘密罪的被告僅知悉所得到之標的為「資訊」（information）即可[15]。

「營業秘密」則定義在18 U.S.C. § 1839(3)，內容包括資訊性質與三項要件，前者指所有格式與形式的財務、商務、科學、技術、經濟、或工程上的資訊，而後者為:（1）合理保密措施、（2）事實上或潛在的獨立經濟價值、和（3）該價值係來自於系爭資訊非屬他人所可

---

[12] *See* 18 U.S.C. § 1831 (a) ("Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent ….") .

[13] *See* 18 U.S.C. § 1832 (a) (" Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret ….") .

[14] *See* Thierry Olivier Desmet, *The Economic Espionage Act of 1996: Are We Finally Taking Corporate Spies Seriously*?, 22 Hous. J. Int'l L. 93, 109-11 (1999) ; *see also* 18 U.S.C. *§* 1832 (a) ("Whoever, … , knowingly—

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in paragraphs (1) through (3) ; or

(5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3) , and one or more of such persons do any act to effect the object of the conspiracy,

(6) shall ….") .

[15] *See* United States v. O'Rourke, 417 F. Supp. 3d 996, 1005 (N.D. Ill. 2019) .

通常知悉或可以適當工具發掘者，且該第他人能因該資訊的揭露或使用而獲得經濟價值[16]。

以下介紹三件刑事判決，以顯示美國司法實務如何檢驗「合理保密措施」要件。

二、United States v. Lange, 312 F.3d 263 (7th Cir. 2002)

㈠系爭營業秘密

在 *United States v. Lange* 案[17]中，本案被害公司 Replacement Aircraft Parts 公司（稱「RACOP」）針對飛機零件的售後市場，購買市場上的合格零件來進行逆向工程（reverse engineering）的研究，並研發與製造等效零件；而系爭營業秘密所涉及之零件為煞車器[18]。RAPCO 對他廠的煞車零件不僅是測量其尺度與規格，而是須投入大量的研發資源來進行合金材料的選擇、材料製程的開發、結構表面的處理、相關法規的安全測試等等工作；因而，在經過不斷的試驗品測試後，才能完成符合飛航安全主管機關要求的煞車零件[19]。

㈡合理保密措施

本案被告被控犯竊取營業秘密罪，其擅自偷竊 RAPCO 的煞車產品的工程製圖相關 AutoCAD 檔案，並對外以高價兜售，直到被執法單位逮捕為止[20]。

於上訴時，本案被告主張系爭營業秘密不符合合理保密措施之要件，但美國聯邦第七巡迴上訴法院（United States Court of Appeals for the Seventh Circuit）不同意此抗辯[21]。本案上訴法院認為被害公司 RAPCO 已採合理保密

---

16 *See* 18 U.S.C. § 1839 (3) ("[T]he term 'trade secret' means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—
(A) the owner thereof has taken reasonable measures to keep such information secret; and
(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public") .

17 United States v. Lange, 312 F.3d 263 (7th Cir. 2002) .

18 *See id.* at 264-65.

19 *See id.* at 265.

20 *See id.* at 264-65.

21 *See id.* at 266.

措施之考量如下[22]：

1. 所有圖示與生產資訊皆存放在特定房間（稱「CAD 室」），且以特殊鎖、警示系統、與行動偵測裝置等而保護著。
2. 對具敏感性的資訊，其副本維持最低數量，且會銷毀多餘本。
3. 計畫中的部分資訊會加密，且僅極少數人才有該加密的解密鑰匙。
4. 圖示與其他資料上有標註「RAPCO 的智慧財產權」之警示。
5. 每位員工皆被告知其所接觸的資訊具有保密性。
6. RAPCO 的承攬商不會收到所有的工程圖示副本，而 RAPCO 將工作切割分配給其供應商以確保任一供應商無能力完成相關產品。對此，RAPCO 是否與其供應商簽署保密協定則無關合理保密措施之判斷，即其依賴任務的分工而非依賴保密承諾。

另欲回應被告指出工程師與繪圖師皆知道 CAD 室鑰匙的放置處，本案上訴法院指出合理保密措施之要素並非是「排除相關員工接觸相關資訊」，否則沒有員工可以執行工作[23]。此觀點亦適用於將計畫提供給承攬商之情境，亦即將資訊散發給供應商的情形並不會弱化營業秘密主張[24]。

三、United States v. Chung, 659 F.3d 815 (9th Cir. 2011)

㈠系爭營業秘密

在 *United States v. Chung* 案[25]中，被告被控之犯罪包括犯經濟間諜罪，其參與中國政府對美國的間諜活動[26]。被告原是被害公司 Boeing 公司的退休員工，其於退休後仍擔任 Boeing 公司的約僱人員[27]。

系爭營業秘密涉及太空梭的通訊天線，其為 Boeing 公司參與美國太空總署（National Aeronautics and Space Administration，NASA）的技術競標時所開發的技術[28]。該天線技術為促使通訊功能升級所發展，其內容包括太空梭艙體的應力分析、天線的元件配

---

22 *See id.*

23 *See id.* (“[K]eeping these employees out can’t be an ingredient of ‘reasonable measures to keep [the] information secret’; then no one could do any work.”) .

24 *See id.*

25 United States v. Chung, 659 F.3d 815 (9th Cir. 2011) .

26 *See id.* at 818.

27 *See id.*

28 *See id.* at 826.

置、冷卻系統的置入等等[29]。關於此天線計畫，被告持有的營業秘密文件包括內容有組裝計畫之工作項目與時間之文件、及解說通訊升級用之簡報資料（內容有天線的規格，例如相關零組件的數量）[30]。

㈡合理保密措施

美國聯邦第九巡迴上訴法院（United States Court of Appeals for the Ninth Circuit）認為系爭營業秘密符合合理保密措施之要件，其參酌的事實情境包括[31]：

1. 雖沒有一份文件是以鎖鑰方式保護，但Boeing公司對其整個廠房採取一般的實體安全檢查措施。當員工進入建築物前，安全警衛會要求其提出身分認證。Boeing公司亦保留對員工的隨身物品與車輛之搜查權。
2. Boeing公司會舉辦訓練課程，以教育員工不要將文件與外部人員分享。
3. Boeing公司要求員工（包括本案被告）簽署保密協定。
4. 系爭文件中的兩份上有標記為「財產」（proprietary）。

值得注意的是系爭簡報資料，其有部分內容曾發表在NASA所贊助的研討會上，且有Boeing公司的競爭者參與聆聽；不過，本案上訴法院指出就相關零組件數量的資訊並未在該研討會揭示，故該事件不影響系爭簡報資料的秘密性[32]。

四、United States v. Nosal, 844 F.3d 1024 (9th Cir. 2016)

㈠系爭營業秘密

在 *United States v. Nosal* 案[33]中，被害公司Korn/Ferry International公司為協助客戶招募高階主管的公司，其設置內部用的資料庫「Searcher」以利員工進行資訊整理、登錄與檢索[34]。員工於利用Searcher資料庫時，會鍵入相關檢索條件以產生「來源名單」（source lists）；而既有的「來源名單」可提供員工於後來的檢索工作中所利用，以加速檢索工作，例如針對相似的職務[35]。Korn/Ferry公司將該些「來源名單」視

---

29 *See id.*

30 *See id.*

31 *See id.* at 827.

32 *See id.* at 826-27.

33 United States v. Nosal, 844 F.3d 1024 (9th Cir. 2016) .

34 *See id.* at 1030.

35 *See id.*

為「財產」[36]。

系爭營業秘密為該些「來源名單」，其為被告等所利用以與被害公司競爭[37]。被告等為被害公司的前員工或現任員工，其擅自登入 Searcher 進行資料檢索或取用來源名單，以供給主犯所成立的人力招募公司使用[38]。

㈡合理保密措施

本案第九巡迴上訴法院雖未直接討論合理保密措施，但判決文內有相關描述，例如：（1）Searcher 是建置於公司內部電腦網路，且視為機密性質而僅能用於 Korn/Ferry 公司之業務；（2）每個員工有自己的帳號與密碼以登入公司的電腦系統，其用相同密碼登入 Searcher；（3）Korn/Ferry 公司和員工間有簽訂保密合約，並約定不能分享密碼；（4）當員工於 Searcher 檢索時，Searcher 會顯示一串訊息指示相關檢索結果限員工使用於 Korn/Ferry 公司之業務上[39]。

另本案上訴法院提到 Korn/Ferry 公司投入資源發展相關程序以保護資料的秘密性，包括建置於電腦系統的科技保護措施、及檢索結果散佈的限制等[40]。其次，雖 Korn/Ferry 公司的政策是不得對客戶揭露來源名單，但在少數情況下曾在有保密理解（an understanding of confidentiality）之條件下向客戶揭露來源名單[41]。對此，本案上訴法院認為在保密情況下對員工、被授權人、或其他人的揭露不會導致系爭資訊失其營業秘密之性質[42]。

甚至，本案上訴法院斥責本案主犯原為 Korn/Ferry 公司的高階主管，怎可能不清楚 Searcher 的競爭優勢和公司對於來源名單的保護措施；且該主犯亦簽署保密協議，而該協議揭示資訊資料庫和公司記錄為公司業務上之高價值資產，並受營業秘密規定之保障[43]。本案上訴法院指出雖秘密標識本身不代表其為營業秘密，但 Korn/Ferry 公司已採取

---

36 *See id.*

37 *See id.*

38 *See id.*

39 *See id.* at 1031.

40 *See id.* at 1043.

41 *See id.*

42 *See id.* at 1043-44 (“It is also well established that ‘confidential disclosures to employees, licensees, or others will not destroy the information’s status as a trade secret.’”) .

43 *See id.* at 1044.

相關措施保護，故大幅削弱本案主犯其不知來源名單為營業秘密之主張[44]。

五、小結

Lange 案、*Chung* 案和 *Nosal* 案等所涉及的營業秘密皆為利用中的資訊。在 *Lange* 案中，員工必須要使用 CAD 室內存放的工程圖示，而相關圖示必須提供給承攬商或供應商，以製造相關零件；在 *Chung* 案中，相關資訊必須揭露給客戶與客戶的供應商；在 *Nosal* 案中，員工必須使用資料庫的資訊。這些使用行為只要施以保密措施，即不會讓系爭資訊喪失營業秘密的性質。

至於保密措施，*Lange* 案的放置保密資訊於專門空間，*Chung* 案的工廠安檢措施，和 *Nosal* 案的電腦系統專屬帳號與密碼等皆為個案上訴法院所認可之適當方法。甚至，*Lange* 案的給予相關承攬商切割的資訊，其不會因未和承攬商間無保密約定而造成合理保密措施之喪失。

參、未達合理保密措施之案例分析：以智商法院刑事判決為中心

本章所討論的個案中，被害公司皆和被告有營業秘密保密約定，且被告拿取被害公司的資訊並用以與被害公司競爭[45]。可惜的是該些案例的智商法院認為系爭資訊非營業秘密，且其理由之一為未達合理保密措施之要求。

一、案例一：智慧財產法院 106 年刑智上訴字第 17 號刑事判決

在智慧財產法院 106 年刑智上訴字第 17 號刑事判決中，系爭營業秘密包括「自動製糊機設計圖」與「自動製糊機操作說明」；本案法院指出「自動製糊機設計圖為依客戶廠房擺設位置、大小不同而繪製之配置圖」，其「在繪製完成後」由被害公司人員「提示予客戶確認」，而「操作說明為安裝自動製糊機時，[被害] 公司方面及客戶端參考準備事項」，故「在客戶要求下，[被害] 公司人員亦有可能提供予客戶」；因此，本案法院認為「[被害] 公司並未規定

---

[44] *See id.*

[45] 智慧財產法院 106 年刑智上訴字第 17 號刑事判決 / 事實 / 一；智慧財產法院 107 年刑智上訴字第 18 號刑事判決 / 理由 / 一；智慧財產法院 107 年刑智上訴字第 24 號刑事判決 / 理由 / 二；智慧財產法院 107 年刑智上訴字第 19 號刑事判決 / 理由 / 一（判決內容未明確指出被告與被害公

不得提供予客戶」，而「難認 [被害] 公司就 [系爭營業秘密] 有採取任何之保密措施」，且「顯然欠缺秘密性」[46]。

二、案例二：智慧財產法院 107 年刑智上訴字第 18 號刑事判決

在智慧財產法院 107 年刑智上訴字第 18 號刑事判決中，本案法院認為被害公司將「面膜結構與面膜成分表」（系爭營業秘密）交給代工廠生產時未採取合理保密措施[47]。本案法院指出「按代工廠對 [被害公司] 之 [系爭營業秘密]，應知悉後方得以生產」，而被害公司「對代工廠內之派駐人員、加工地方處所、在場人數等，均未提出相關資料」，且被告亦指稱其受被害公司派遣至中國接觸面膜結構廠商時，「並未與任何工廠簽署保密協議」，而工廠「現場也沒有清空其他人員」；因此，本案法院認為被害公司「並未與其在 [中國] 合作之代工廠商簽署任何保密協議，應堪先認定屬實」，且被害公司「所稱對相關資料如何如何保護，且對代工廠人員、場地有如何如何之限制云云，均無從採信」[48]。

另本案法院質疑被害公司的離職程序所造成的合理保密措施問題[49]。本案法院指出「按一般公司員工在辦理離職手續時，公司會阻斷其能再度進入公司電腦資料、使其不能再用公司電子郵件帳號、變更相關密碼等」；特別「對業務上可能知悉公司祕密之員工」，本案法院指出公司「更會慎重其離職流程辦理事項」，而此乃「判斷公司是否有採取合理保密措施之一部」，但被害公司卻「對被告相關的離職手續辦理過程，均付之闕如」；因此，本案法院認為「在被告離職時，並無證據證明 [被害公司] 對於 [系爭營業秘密] 已採取合理保密措施，或有採取任何其他不易被任意接觸之方式控管該等資料」[50]。

三、案例三：智慧財產法院 107 年刑智上訴字第 24 號刑事判決

司間曾有保密約定，但被害公司有營業秘密管理制度，故可推得二者間應有保密約定）。

46 智慧財產法院 106 年刑智上訴字第 17 號刑事判決 / 理由 / 乙 / 貳 /（三）。本文中引文內的「[]」符號為筆者所加。該符號內的文字為就原文內容的相對應部分所改寫，以符合本文論述的流暢。

47 智慧財產法院 107 年刑智上訴字第 18 號刑事判決 / 理由 / 四 /（一）/5/（2）。

48 智慧財產法院 107 年刑智上訴字第 18 號刑事判決 / 理由 / 四 /（一）/5/（2）。

49 智慧財產法院 107 年刑智上訴字第 18 號刑事判決 / 理由 / 四 /（一）/5/（3）。

50 智慧財產法院 107 年刑智上訴字第 18 號刑事判決 / 理由 / 四 /（一）/5/（3）。

在智慧財產法院 107 年刑智上訴字第 24 號刑事判決中，本案法院認為系爭營業秘密（即系爭工程設計圖）未符合合理保密措施之要件，主因是被害公司的員工於對外的電子郵件中，「從無記載 [系爭] 工程設計圖係屬 [被害公司] 之營業秘密，或該資料應予保密，不得提供予無關第三人之相關聲明」，且被害公司「亦未見任何防止 [系爭] 工程設計圖外洩之措施」[51]。另雖被害公司主張員工使用工程設計圖前須填寫管制表，且系爭工程設計圖的利用亦有管制紀錄佐證 [52]，但本案法院認為被害公司之「生產部工程模具設計圖管制表」中「僅係填載 [系爭] 工程設計圖初稿」，故無法佐證對系爭營業秘密採取合理保密措施 [53]。

四、案例四：智慧財產法院 107 年刑智上訴字第 19 號刑事判決

在智慧財產法院 107 年刑智上訴字第 19 號刑事判決中，系爭營業秘密包括「Release Check List」文件（應指產品正式生產時的相關製造資訊）與「實驗單文件」，二者皆被本案法院認為無合理保密措施要件之滿足。

其理由可分為二類。第一類是關於文件標識問題。本案法院指出「系爭『Release Check List』文件雖置於『DCC 文件控管中心』，但該控管中心對系爭『Release Check List』文件標明:『文件密等:一般，保密文件設定值:非保密（無保密，可調閱、搜尋）』等情」，故「顯見該等文件係以未保密文件控管」[54]。另關於系爭實驗單文件，本案法院指出其「沒有標示任何機密等級」，故「客觀上連員工都無法了解 [被害] 公司有無將系爭實驗單作為營業秘密保護之意」[55]。

第二類是關於系爭營業秘密儲存在工廠（稱「CF 廠」）內電腦系統的共用槽 [56]。本案法院指出「該公用槽並未設定密碼」，故「無論是否與該實驗有關之人員，只要是 CF 廠的員工均可以

---

51 智慧財產法院 107 年刑智上訴字第 24 號刑事判決 / 理由 / 五 /（四）。

52 智慧財產法院 107 年刑智上訴字第 24 號刑事判決 / 理由 / 二。

53 智慧財產法院 107 年刑智上訴字第 24 號刑事判決 / 理由 / 五 /（四）。

54 智慧財產法院 107 年刑智上訴字第 19 號刑事判決 / 理由 / 四 /（二）/3。

55 智慧財產法院 107 年刑智上訴字第 19 號刑事判決 / 理由 / 四 /（一）/2。

56 智慧財產法院 107 年刑智上訴字第 19 號刑事判決 / 理由 / 四 /（一）/2（指出系爭實驗單文件存放在公共槽的問題）；智慧財產法院 107 年刑智上訴字第 19 號刑事判決 / 理由 / 四 /（二）/3（指出系爭「Release Check List」文件因儲存在一樣的公共槽而有相同的問題）。

接觸該等資訊」；雖然被害公司主張其「設定員工在電腦開機時須輸入帳號、密碼才能開機」，但本案法案指出「雖然 CF 廠的電腦開機時需要輸入帳號密碼，但仍可以使用共用的帳號密碼登入」，故此「代表 [被害] 公司對於員工登入 CF 廠電腦時，並未分級進行管制」；又「CF 廠電腦開機登入後，CF 廠任何人即可隨意接觸共用槽內的文件」，而被害公司「並未再以密碼對可接觸共用槽者作管制」，則因「CF 廠下設有許多部門」，且「並非所有 CF 廠內的任何部門員工均有接觸系爭 [營業秘密] 之必要」，故本案法院認為被害公司「對系爭 [營業秘密] 之管制方式，並未依業務需要做分類、分級、授權接觸職務等級之管制措施」，而「將使得許多不需要接觸該等資訊之人亦能接觸該等資訊」，故「實難認系爭 [營業秘密] 已符合『合理保密措施』要件」[57]。

另雖被害公司主張 CF 廠所屬之「第六廠各部門有管制卡作實體區域的管制」，但本案法院認為「公司設有門禁管制，其主要目的在於人員進出管理及員工安全維護，此為稍具規模之公司即有之通常管制措施」，而被害公司「自承其第六廠占地就有約 765 個籃球場大，廠內有 ARRAY 廠、CF 廠及 LCD 廠等等」，故其「公司之規模，實與一般小型企業有很大的不同」，則「若謂 [被害] 公司單純以門禁管制即可作為合理保密措施，豈非 CF 廠門禁內之所有大大小小資訊，均屬於營業秘密法所保護之營業秘密，此實在太過廣泛」[58]。

五、小結

前述案例一至案例三涉及相關營業秘密在流向客戶或承攬商，但在資訊流動過程中，被害公司並未有明確的保密措施，例如最基本的於文件上或信件中標識「營業秘密」或「機密」等文字也沒做到。

但是，案例四中，被害公司事實上有營業秘密管理制度，包括文件管理、廠房進出管制、電腦登入管制等等。特別是，該被害公司其「公司電腦開機時會出現提醒員工行為準則、保密義務的畫面」，且「公司提醒畫面說『員工負責保密義務，嚴禁洩漏公司任何機密』」[59]。只是電腦系統的共用槽處「並

[57] 智慧財產法院 107 年刑智上訴字第 19 號刑事判決 / 理由 / 四 /（一）/2。

[58] 智慧財產法院 107 年刑智上訴字第 19 號刑事判決 / 理由 / 四 /（一）/2。

[59] 智慧財產法院 107 年刑智上訴字第 19 號刑事判決 / 理由 / 四 /（一）/2。

沒有提醒畫面」，而有員工指證若「拿到資料後有些上面不見得會有機密等級」，則「他們比較難去判斷是屬於什麼樣等級的機密」，例如「如果上面有清楚標示『密件』，就會知道是機密，如果沒標示，則主觀上就無法去判定是否為機密文件」，此造成本案法院認為不符合「合理保密措施」要件[60]。

肆、代結論：美國 EEA 司法實務之借鏡

從美國 EEA 相關司法判決，本文提出二點建議。

一、考量使用情境

在 *Lange* 案中，被害公司建置特殊空間存放相關資訊，但該空間的進入方式並未限定特殊人員或有特殊程序[61]。該案法院強調排除員工接觸相關資訊並非合理保密措施，否則無人能執行業務[62]。然而，在智商法院之案例四中，系爭「Release Check List」文件與「實驗單文件」儲存在廠區內電腦系統的公共槽中，的確是有登入權限的員工皆能讀取該些資訊。不過，該案法院認為相關資訊沒有分類、分級、和授權接觸職務等級而未達「合理保密措施」要件[63]。二件判決相比較凸顯智商法院未考量系爭營業秘密之使用情境。

案例四的系爭營業秘密屬「利用中之資訊」，放在廠區方便員工取得的環境，應可理解。況且被害公司有基本的接觸管制，包括廠區門禁與電腦登入帳號密碼。在職務範圍內，相關員工可直接到電腦系統之公共槽閱讀相關資訊，以方便執行生產任務。若不屬於其業務範圍，相關員工就不應接觸該資訊，此應屬合理的工作倫理要求。因此，如果參酌 *Lange* 案判決，案例四的合理保密措施應可成立。

至於案例一至案例三所涉及的資訊流動至客戶端或代工廠端之問題，法院可參酌 *Lange* 案判決而考慮代工廠端是否知道所有系爭營業秘密、*Chung* 案判決而考慮系爭營業秘密中未被揭露的部分、和 *Nosal* 案判決而考慮被告本身即是系爭營業秘密使用者等等。亦即，

---

60 智慧財產法院 107 年刑智上訴字第 19 號刑事判決 / 理由 / 四 /（一）/2。

61 *See Lange*, 312 F.3d at 266（"[A]s Lange says, engineers and drafters knew where to get the key to the CAD room door[.]"）.

62 *See id.*

63 智慧財產法院 107 年刑智上訴字第 19 號刑事判決 / 理由 / 四 /（一）/2。

相關資訊雖有機會揭露給客戶端或代工廠端，但不代表其必然喪失營業秘密性質。

二、未遂犯

最後，針對智商法院案例四之情境，該案被告明顯是欲透過其在被害公司的人脈來竊取被害公司「在產品投入生產時（即 Release），有哪些可能危害產品品質之生產流程確認項目」與相關作法，以利用於其受聘的中國公司（亦為被害公司的競爭者）[64]。此行為是營業秘密法刑事條文所欲打擊的犯罪行為，但僅是因法院認為所偷竊的資訊不符合營業秘密的定義而讓該被告開脫罪刑。

案例四的被告事實上是欲偷取被害公司之營業秘密，而僅是其偷得的資訊被法院認為不符合營業秘密的要件。對此類犯行，本文建議未來檢方應思考營業秘密法第 31 條之 1 第 2 項和第 31 條之 2 第 2 項的「未遂犯」，以做為起訴依據或變更起訴法條。

在 EEA 中，18 U.S.C. § 1831(a)(4) 及 18 U.S.C. § 1832(a)(4) 等有提供「著手犯」（attempt）的樣態，其要件為：（1）有意圖完成所涉的罪刑；（2）採取了完成犯罪所需要的實質步驟之行為[65]。法院於審理此類犯行時，僅看被告是否認為其所偷竊之資訊為營業秘密即可，而不須考量系爭資訊是否「事實上」為營業秘密[66]。

刑法第 25 條第 1 項規定「已著手於犯罪行為之實行而不遂者，為未遂犯」，因而類似 EEA 的著手犯型態。如果檢方可以證明被告欲偷竊營業秘密，則即使被偷的資訊最後被法院認為不符合營業秘密的三要件，也可讓被告構成「未遂犯」而受到應有的懲罰。

---

64 智慧財產法院 107 年刑智上訴字第 19 號刑事判決 / 理由 / 一。

65 *See* United States v. Hsu, 155 F.3d 189, 202 (3d Cir. 1998) ("Thus, the defendant must (1) have the intent needed to commit a crime defined by the EEA, and must (2) perform an act amounting to a 'substantial step' toward the commission of that crime.") .

66 *See id.* ("The government can satisfy its burden under § 1832 (a) (4) by proving beyond a reasonable doubt that the defendant sought to acquire information which he or she believed to be a trade secret, regardless of whether the information actually qualified as such.") ; *see also* David W. Quinto & Stuart H. Singer, Trade Secrets: Law and Practice 359 (LexisNexis 2014).

參考文獻

中文書籍

王偉霖，《營業秘密法理論與實務》，元照，2015 年 4 月，初版 1 刷。

楊智傑，《智慧財產權法》，新學林，2019 年 6 月，3 版 1 刷。

趙晉枚、蔡坤財、周慧芳、謝銘洋、張凱娜，《智慧財產權入門》，元照，2003 年 3 月，2 版 2 刷。

英文書籍

Quinto, David W. & Stuart H. Singer, Trade Secrets: Law and Practice (LexisNexis 2014).

英文期刊

Desmet, Thierry Olivier, *The Economic Espionage Act of 1996: Are We Finally Taking Corporate Spies Seriously*?, 22 Hous. J. Int'l L. 93 (1999).