國立臺灣大學法律學院法律學系

碩士論文

Department of Law

College of Law

National Taiwan University

Master Thesis

監視社會與犯罪控制

Surveillance Society and Crime Control

吳庭毅

Ting-Yi Wu

指導教授：謝煜偉 博士

Advisor: Yu-Wei Hsieh, Ph.D.

中華民國 108 年 2 月

February 2019

doi:10.6342/NTU201900452

謝辭

感謝李茂生老師為論文背後的價值觀與實踐之間的交集提供方向，從碩一開始接觸老師的課程以來，在許多理論上受到老師的影響，可惜最終呈現的結果上仍有許多不足之處。但能在研究生生涯中參與到老師的課堂，真的是感到十分幸運。

感謝林琬珊老師詳細的就論文的形式與實質問題提供建議，老師也指出了許多論述有待進一步釐清或是有所矛盾的論述，實在是很抱歉在形式上留下的錯漏，也很感謝您仔細地閱讀整篇論文並且協助修正。

感謝恩師謝煜偉老師從選題以來，合宿、研討會、每次 Meeting 中提供的意見與方向。這篇論文選題的野心太大，且論文方向幾經修改，直到最後呈現的架構仍難以稱作完善，甚至留下許多沒有處理到的問題。在寫作過程之中，若沒有老師的協助的話論文的方向真的難以決定下來，而且當初設定的許多目標最終也只完成了一小部分，實在是學生的能力不足。

也感謝謝門的大家以及 1801 研究室、刑法組的夥伴們在這段過程中提供的大大小小協助，以及家人的支持。

吳庭毅

於霖澤 1801 研究室

doi:10.6342/NTU201900452

摘要

伴隨著資訊時代的來臨，監視社會逐漸轉變為新的形態。近代監視技術之發展以及資料流動的數據化與網路化，兩者結合之後帶來的是監視聚合體的膨脹，以及資訊化人格與個體之間的割裂問題。在監視系統演算法的運行之下，以未來預測與風險抗制為目標的監視系統其實施可能性逐漸地被發展，為社會帶來了新形態的控制模型。此一模型選擇放棄個人的隱私換取社會的安全，並且試圖預測未來的風險。本文將分析此一系統與監視技術結合帶來的利處與害處，並且試圖對監視社會提出抵抗性的論述。

關鍵詞：監視、控制社會、環境犯罪學、生權力、圓形監獄、刑事政策、結構論、監視器。

doi:10.6342/NTU201900452

Abstract

With Information Communication Technology (ICT) and Internet, surveillance society continues to expand. Body under surveillance system tend to be Data Double, and then be governed by statistical technique. Surveillance system try to predictive future trends, turn everything into numbers and risks, and then try to reduce risks by using Algorithm. People's privacy tend to be abandoned in surveillance society. Thus this article try to analyze present situation and find some resistance arguments to surveillance society.

Key words：surveillance; social control; Environmental criminology; Biopower; Panopticon; Criminal policy; architecture; Closed-Circuit Television

doi:10.6342/NTU201900452

簡目

doi:10.6342/NTU201900452

doi:10.6342/NTU201900452

詳目

doi:10.6342/NTU201900452

doi:10.6342/NTU201900452

doi:10.6342/NTU201900452

doi:10.6342/NTU201900452

第一章 序言

第一節 研究動機與問題意識

日本內閣提出的未來構想イノベーション２５之中有這樣一幕：放學回家的小男孩，被可疑人士盯上並且即將被攻擊。但小孩身上配戴的監測系統即時發現了環境中的「不良行為」，並且迅速通報防犯網路系統，及時阻止了犯罪的發生。在這一構想之中，只要適當地使用科技與監視網路，危險便能被扼殺在搖籃中，犯罪將不會再發生或者在發生前便被阻止。《一九八四》小說中所描寫的「Big Brother」意象似乎將要轉換型態，並且以對人民「有益」的樣貌重生。

另一方面，在中國社會信用制度的理想目標之下，每個國民都被建立了一個履歷檔案，裡面記載了籍貫、年齡、性別、職業、收入情況、病歷、家庭成員、常用的交通工具、信用卡交易紀錄、網路購物的購物履歷。所有的資訊均能被轉換為數據並且儲存在資料庫中。透過這些資訊的收集，國家能夠描繪出每一個人的圖像，同時在這些資料之中，透過國家所選擇的特定要素的比對，可以藉此找出所謂的偏差／逸脫之個體，而後對其進行分類、排除、差別待遇。此種以安全作為目的，以監視技術作為基礎，以風險因素的設定做為危險因子之定義標準，以預測未來可能性作為運作方式，以演算法所得結果作為差別待遇基準之系統，在監視技術的結合之下可能產生許多種的應用。在這樣的應用下，引發了如下問題：「監視社會與監視技術發展狀況、監視技術與犯罪控制的關聯、監視技術作為一種結構的運行、結構與刑事政策的交互作用、對監視社會與結構進行的抵抗如何進行等等」。

監視技術與犯罪控制在此一發展之下，呈現出一種新型態的權力作用。本文希望藉由簡單的對監視技術與其背後所代表的規範意義變遷進行梳理，結合風險與資訊社會之特徵，試圖指出監視社會可能潛藏的危險性，以及對監視社會進行對抗的可能性。法學者所依賴的法律，在官僚組織以及犯罪控制領域中已經與監視技術深刻結合。即便在部分國際公約、法律之中已經意識到資訊科技與監視技術結合所帶來的危險性，並且試圖以法規範的形式對個人資料進行保護，仍無法完全阻止監視社會的擴張。同時監視技術的發展與結構論有所關聯，星羅棋佈的監視網路成為一種橫跨了現實空間與虛擬空間的結構，在許多政策傾向上帶來變化。本文將先探討監視社會形成的歷程與概況，梳理如今社會中常見的監視系統概況。並且指出這些圍繞著個體的系統，在人口管理與風險控制兩大目的傾向之下對於個人資訊的蒐集與控管如何進行，接著分析實際應用這些系統後在政策上的效果與帶來的問題。最後就法律與刑事政策層面與

doi:10.6342/NTU201900452

監視技術領域的交錯狀況進行分析，試圖檢討對抗的可能性是否存在。本文希望藉由對這些脈絡的分析，呈現出監視社會之中結構與法律所扮演的角色，監視技術與資訊社會所帶來的優缺點，以及可能潛藏的危險性，而後試圖進行對抗的論述。

第二節 論文架構與研究方法

第一項 論文架構

就論文架構部分，本文聚焦的重點在於監視社會之發展以及其中所包含的系統如何演化並且與其他領域結合之過程。在此前提之下，首先應該釐清所謂監視社會究竟為何，應如何定義，以及其於古代、近代、現代呈現何種樣貌。而後以此為基礎，對影響此一歷程的資訊科技之發展以及監視技術之變化進行簡述。於處理完監視社會發展之概況之後，就各該論者對監視社會之各種現象進行之詮釋，亦即監視理論之發展進行說明，並且試圖找出近代監視社會之中，影響系統發展以及人民對於監視社會觀點改變的重要因素為何。在這些理論支撐之下，本文接著以環境犯罪學以及結構論兩個領域中對於監視技術之設置如何進行、如何詮釋作為引子，試圖將監視理論與對社會進行的新型態控制加以連接。並且對此一以監視技術與資訊科技為基礎之新型態控制系統提出其蘊含的危險性，以及個人隱私概念與社會對安全追求之衝突進行說明，在最後試圖提出本文對抗監視社會之論述。

凡例部分，直接引用文獻敘述者以標楷體表示並且加上註腳，引用文獻內容者則以註腳方式標明。內文字體加粗部分則為本文欲強調之內容。

第二項 研究方法

主要採取的研究方法，為文獻回顧與整理法。以針對監視理論進行論述之文獻作為中心進行收集與分析，並且參考外國立法例上對於監視技術的實際運用狀況以及呈現的問題後對監視社會概況進行綜述。

本文所使用的文獻，主要以英文為主，日文為輔。就中文領域則以與論題有關之期刊文章作為補充。原因在於監視理論在發展上屬於較為新穎的理論，以中文進行書寫之專著較為稀少。又因為本文所選擇之論題較為複雜，且具有向各個領域(例如犯罪學、刑事政策)發散之可能性，因此對於文獻主要以各該監視領域針對特定問題所提出之文集、專論作為核心，亦即以監視相關議題為中心進行文獻梳理，而較為缺乏針對監視理論發展進行整體論述之描述。故而就監視理論之發展歷程進行梳理之文獻整理，尚有待後來者完善。本文雖以監

doi:10.6342/NTU201900452

視理論作為基本素材，但重心主要放在描寫潛藏於監視技術應用狀況之下的演算法問題、風險預測問題、誤判問題、以及新型態控制問題。

第三項 名詞定義

監視(surveillance)[1]：在影響、管理、保護、或指導的目的之下，以個人的特定詳細事項為焦點的，具有體系化路徑的關注。

資訊人格/虛擬人格(data double)[2]：在監視或資訊收集系統中，被捕捉到的個人資訊、生活歷程之斷片重新分析、處理、組合後，於監視或資訊收集系統中呈現出的個體。此一個體雖然被用以指代現實中的個體，但不可避免的會與現實中的個體產生斷裂。

Code：在本文文脈下有兩種意涵，其一為構成資訊系統底層結構的基礎程式碼，其二為 Deleuze 之文脈下取代規訓社會之控制社會中，對於個體的調控所進行之編程或者說基礎架構[3]。

老大哥(Big Brother)：小說《一九八四》中，被用以將監視技術與獨裁統治連結之意象。老大哥會用監視技術看著他所統治的人民，人民則隨時活在被監視的恐懼與控制之中[4]。

第二章 監視社會的現況

第一節 監視社會的形成

第一項 監視社會的概況

[1] David Lyon(著)(2011)，田島　泰彦、小笠原　みどり(譯)，《監視スタディーズ－「見ること」「見られること」の社会理論》，頁 22，岩波書店。

[2] Kevin D. Haggerty and Richard V. Ericson (2000), The surveillant assemblage, *British Journal of Sociology*, Vol. No.51 Issue No.4, p.611.

[3] Gilles Deleuze (1992), Postscript on the Societies of Control, *October*, Vol. 59, p.5.

[4] 對此一意象的說明，可參見董娟娟(2005)，〈詮釋新加坡發展的新路徑：監視社會研究的新解與展望〉，《台灣政治學刊》，第 9 卷第 2 期，頁 113-114。

doi:10.6342/NTU201900452

第一款 概述

監視，是指人透過不特定的方式，對於特定對象的行動加以關注的過程。監視的概念，伴隨著權力作用，貫穿在人類社會之中。從早期的專制政權中君主在民間安插眼線、設置特務機關，一直到現代民主社會中政府透過廣泛設置監視器、進行網路監控觀察人民、甚至企業以各種方式收集消費者資料等等，皆為監視作用的型態。除了與政府的統治與企業運作相關以外，監視行為也隨時隨地存在社會日常生活之中，例如父母於賣場注意小孩子的行動、或者救生員在海灘注意有無泳客溺水等等，甚至只要透過眼睛看著他人，也能夠說成一種監視行為。可以說在人類社會中，原本就會互相以互相觀察的方式來對他人進行關注。但為了不讓論述焦點過於分散，本文借用 Lyon 的用語[5]，將監視定義為：「**在影響、管理、保護、或指導的目的之下，以個人的特定詳細事項為焦點的，具有體系化路徑的關注。**」並以此種含有特定目的[6]的監視行為以及其背後隱含的脈絡、可能帶來的衝突，來作為本文以下論述的重心。

在監視行為背後的脈絡之中，通常包含監視行為的目的、手段、對象、選擇對象的方式、所要擷取的資訊、資訊最終的用途等等要素。如果將這些脈絡抽離，對監視行為進行的分析就失去意義。因為即便是同種類的監視行為，仍可能與多種目的有所連結，而其**使用的手段、擷取的資訊、資訊最終的用途，皆可能影響我們對於監視行為的評價。**以監視攝影機的架設位置選擇為例，我們或許會希望將車子停放在附近有監視攝影機的停車格之中，但未必會希望監視攝影機對著家門口甚至家中拍攝。同樣是架設監視攝影機的行為，便會因為架設的地區、鏡頭運作的方式、收集的資訊最後的用途等等而可能產生不同的影響。因此，在處理監視行為背後的脈絡之前，並不能直接加以價值判斷。當然在文學作品甚至電影之中的描寫，有可能直接將監視與極權畫上連結，但那終究只是監視可能出現的其中一個面向而已。舉例來說，醫院對於個人病歷的收集，實際上是有利於病人的健康維持。又例如購物網站收集消費紀錄進而為顧客推薦較可能被購買的商品，也可能使顧客的購物更加便利。但這些資訊如果被不當的外流，情況則又不同。因此僅以監視、收集個人資料的行為本身來看，尚無法進行價值判斷，**真正需要分析的，是行為背後的目的、執行的主體、監控的區域、資訊的分析、重組、使用等等脈絡。**

第二款 監視的歷史

[5] David Lyon，前揭註 1，頁 22。

[6] 需注意的是，此一特定目的經常蘊含向其他目的發散的可能性，亦即原本是為特定目標所收集的資料，卻能運用在其他的領域中。這一點將在後面的章節詳細說明。

doi:10.6342/NTU201900452

監視的歷史幾乎等同於人類的歷史。由於眼睛是人類在生物學上主要用來觀測環境的器官，可以說人類的歷史之中監視的目光總是存在。而不論是古典時代或是近代，監視的目標總是離不開「人口」與「管理」，並且與權力相互作用。但**監視的進程，在現代社會中卻逐漸發展出幾種特殊的型態，變的更加發散、塊根狀而非集中、線性，並且在資訊社會中逐漸超越了視覺感官的範疇。**

監視社會的興起，與近代以來的科技與文化發展有極大的關聯。社會型態從以農村、莊園等地鄰性緊密群體為主的封建社會，過渡到以都市與資本與勞動/消費關係為主的資本主義社會。在這個邁向近代的過渡過程中，個體遵循的典範隨之產生移轉，甚至典範在近代化過程中逐漸消融。原因在於近代化的過程與生產技術的改變，以及啟蒙思想的產生。原本在農村社會之中，個體的生活依附於田地，並且將家族內部的連結、鄰里間的關係(從監視觀點來看便是鄰里的目光)以及宗教/皇權(至高無上的權威、以神職人員、皇權授權的地方官等方式展現)等社會規範做為行動的準則，同時以農業以及簡單商業體系的形式來進行生產活動。在此一時代背景下，由於欠缺資訊科技的幫助，觀看者或者說國家警察很難僅從外觀來具體的辨識特定個體[7]。

對於土地、人口的控制，是這些時期掌握權力的統治者需要達成的目標。宗教必須要防止異端動搖信仰，皇權必須要阻止叛亂與革命。監視技法則作為人口控制的重要手段而存在。但在此時的科技條件之下，監視的目光來源通常皆須透過人力進行，除了特殊的場所(監獄、燈塔、哨站、烽火台)之外，難以直接創設結構性的、脫離人力而能自動運作的監視系統。而社群成員的生活由於生產場所的限定以及生活環境的緊密性質(宗族、封建體制)，個體通常被限制在特定的生活地域，其社會生活與偏差行為的控制可以直接透過地方性社群加以進行[8]，例如日本江戶時期透過長屋以及警察與人民之間的緊密連結來達成對於社群的控制。或者歐洲封建時代透過教會達成社群的連結、古代中國透過大家族的組成以及土地結合生產的概念來維持社會等等，在這些時代之中，社群間的社會連帶相對來說較為緊密，但也同時受到受這些社會連帶所控制。此時**監視的目光通常乘載著來自皇權、宗教、家族的權力而產生作用，同時保持著依賴感官與人力、傳播速度較緩慢、與權力關係緊密結合的特性。**

而在往近代民主體制社會過度的過程之中，政權進行統治的形式從皇權轉換成法律，個體主要的生活場域也從鄉村轉移到都市。在都市之中，生產活動變得多樣化而不受田地的束縛，農民也轉變成市民(Civil)。市民擁有自由，服

[7] Toshimaru Ogura(2006). Electronic government and surveillance-oriented society. In David Lyon(Ed.). *Theorizing Surveillance: The panopticon and beyond* (pp.270-271).

[8] Toshimaru Ogura，前揭註 7，p.272。

doi:10.6342/NTU201900452

膺於法律，並且為自己負責，藉此在社會之中發展自我的人格。家庭的聯繫在這個過程中逐漸薄弱化，個體的價值則被更加的強調。市民社會之中，社會連結變得相對鬆散。都市作為生活場域，其中人口的組成較為複雜，絕大多數生活在個體周遭的人，對於個體而言僅只是「陌生人」或者說「他者」[9]。此時統治的目標從群體聚焦到個體，都市環境之中的政府如何應對個體、個體如何應對他者，以及對越加密集的人口控制的需求皆應運而生。因此在現代化的過程中，監視的技法也必然的隨之轉變了型態。

學者 Ogura 氏認為監視技法的發展在這些歷程中有幾個重要的轉捩點[10]：

1.工業革命的興起，使得掌握技術的勞工成為遠比農民來得危險的群體，因為技術跟隨著個體，而農業附著於田地。**對於技術勞工的控制變得必須，因此產生針對勞工的監視需求。**而在資本主義之下，對於工作場所的控制也變成普遍的目標。

2.接下來監視技法往日常生活中擴展，資本主義的價值觀之下，優良的市民必然是勤奮工作的市民，懶惰者則是市民共同的敵人。伴隨著工作者/失業人口的劃分，失業者或低收入戶被納入國家政策體系之中，希望能透過懲罰/獎勵的方式使其找到工作，成為對國家社會有益的勞動力。原本存在工廠之中的**人口管理因此擴散到整個社會的日常生活之中**，著重的目標則是階級的劃分以及人口的分類，監視技術此時作為對人口進行更精確分類的技法而被使用。

3.第三個階段是冷戰時期，監視技法從針對人口進行的管理進化成針對思想進行的控制。論者在此認為監視技法成為形塑「消費者」與「民主社會的投票者」這兩個概念的延伸。大眾媒體與廣告則推波助瀾，使人民認為自己是個自由的消費者。此時的**監視目標是團塊化的「無名的群眾」**，個體僅僅是作為其中的一員而存在。

4.第四個階段則是消費者與群眾的去中心化開始產生的階段。去中心化導因於高複合-低產量(Hi-mix low-volume)的電腦平台發展，產業的發展趨向精緻化，進行生產的個體被要求提供的與其說是勞動力，不如說是應用技術處理問題的能力，以及適應官僚性質組織的能力。而這些能力的發揮根基在電腦技術的應用之上，亦即**勞動力的發揮不再是僅靠身體或技術進行，而是以官僚組織**

[9] 亦即周遭的個體從「鄰居」轉變為「陌生人」。參見 Aaron Doyle. (2006). An Alternative Current in Surveillance and Control: Broadcasting Surveillance Footage of Crimes. In Kevin D. Haggerty, & Richard V. Ericson (Eds.). *The New Politics of Surveillance and Visibility*(p.202)。

[10] 以下各階段之內容，整理自 Toshimaru Ogura，前揭註 7，pp.272-276.

doi:10.6342/NTU201900452

化的、與資訊科技緊密結合的形式進行。而在消費層面，原本在前一個階段中被想像成一個大團塊的「無名的消費者」被打散成許多個消費團體甚至是個人。這一打散的過程也因此使得監視的目標從「無名的群眾」轉向以特定個體或特定團體成員為目標的身分辨識。

5.第五個階段則是根植於網路與通訊科技(ICT)的監視。此階段從冷戰時期開始持續至今。ICT 因為其**快速傳遞、整合、分析資訊的能力**，迅速從一般通訊應用擴展到警政設備與國家安全活動、國境管理等領域，並且帶來電子化政府的潮流。除了國家使用之外，個人與公司團體也廣泛使用 ICT 工具。此時**監視技術表現出數據化、不同平台間的流轉、不同領域檔案組合的可能性等特徵。**

本文認為 Ogura 氏在此指出的幾個監視技法的轉捩點中，過於強調政府/資本進行控制的角色，監視技法固然隨著這幾個轉捩點持續演進，但其至多也僅發揮協助工具的效果，而非政府/資本對於人民進行控制的根本原因。但仍然值得注意的是 Ogura 氏點出監視目標從「地域性社群」轉向團塊化的「無名的群眾」，最後發展到被「區分辨識的個人」此一歷程。這個歷程對應到監視技術的發展階段，從以人力與社群達成的地域性控制，過渡到藉由官僚組織的運作，將大量群眾化約為一種形象，再以此一形象為基準針對群眾進行監視，最後發展到透過 ICT 與電腦科技，達成特定個體的強調與辨識。這一連串的流程，代表著監視技術對於個體的掌握漸漸深入，監視的目光不再是以視線的方式存在，也不再是以針對特定區塊或者特定團體的方式進行，而是廣泛的、盤根錯節的、有如流動的液體一般散落在社會生活之中，同時監視的目標也在特定的個體、特定的群體、監視資訊的數據化片段之間流轉。

在此一簡要的歷程區分之下，雖然各個時期均有較具代表性的監視手法存在，但此一特徵並不代表特定時期便僅存在一種監視技法。由於監視技法具備聚合的多樣性，仍有在各個時期之中同時運用不同的技法針對不同的目標展開監視的可能性。例如在現代進行的監視手法之中，針對「無名的群體」之監視仍然存在，以監視器的設置為例，其原始的目標即非針對特定個體的辨識，而是對在通過某個區域的「無名群體中的個體」概括性的監視及收集影像。雖然此一監視技術最終針對的目標仍然回歸到個體，但這兩者之間仍有層次上的差異。藉由監視器進行的監視影像收集，其原始的設計仍是以非特定的群體為標的，而必須要在針對影像進行處理過後才能對欲標示的個體加以特定，前述第五階層的監視技法則是自始自終即以辨識出特定個體的特定傾向(例如購物興趣、政治傾向、犯罪風險)為目標，這點不同於針對廣範圍的非特定目標所進行的監視手法。而監視針對的目標、監視手法的選用、監視機制如何被創設，這些監視社會重要的問題，亦可從前述的歷程區分之中尋找到切入點。又因為監

doi:10.6342/NTU201900452

視技術的聚合體特性[11]，一旦經過適當的設計與安排，以上這些層次中提及的技法都有被混合使用、產生嶄新排列組合的可能。具體事例例如中國在新疆所進行的針對少數民族之整體性監視，包含了針對個體的、針對群體的、針對現實的、針對虛擬空間的全方位控管，此部分內容本文將於後續應用層面提及。

而在監視歷史之中，網路與通訊科技的發展是最為重要的轉折點。網路與通訊科技賦予了個體與政府甚至媒體具有幾乎同等力量的傳播工具，影像的產製與資訊的收集門檻大大的降低。網路具備著去中心化、匿名性、跨越國境的特質，另一個特點是在網路世界之中並不存在「可統治的身體(governance body)」此一實體。舉例來說，政府可以對現實中被統治的身體進行拘留等等人身自由的限制，或者藉由不同的建築設施、制度設計對身體進行控制。但對於網路中的虛擬人格，則必須採用對連線加以限制、對網路內容與數據加以調整或刪除等方法來管制。這些管制措施雖然在所達成的效果未必與對身體進行的統治有太大的差異，仍然提示了一種不同於現實身體的「虛擬身體」存在，對其進行的統治較難透過空間進行，而注重在對數據與資料進行處理。

政府的統治在此一層次上來說無法如同其於現實中統治身體一般，直接統治存在網路之中的虛擬身體。但另一方面其也同樣試圖透過網路與通訊科技以及對網路科技載體的控制(例如智慧型手機、電腦設備、伺服器)來奪回對此一場域的掌控，同時在不同目的之下試圖從中取得資訊。在這個層面來說，網路世界成為了新的資訊流通場域的同時，也成為了值得被監視的標的。相較於過往以身體為中心的監視，網路場域中以虛擬人格為中心的監視所能取得的資訊更加直接，因為網路場域的資訊流動原本就已被轉換為數據的方式進行[12]，能夠更快的被轉化讀取。因此 Ogura 氏認為，網路將成為一個持續爭奪中的監視場域[13]。值得注意的是，此一場域除了個人與政府之外，尚有社群網路提供者、以資本為基礎的公司、甚至恐怖分子參與其中。原因在於踏入網路場域的門檻相對較低，而網路能夠覆蓋到的範圍卻又超越國界。

[11] 由 Kevin D. Haggerty 所提出之概念，其指出監視技術所具備的彈性使其可與任何具有資料需求的政策領域、消費領域、軍事領域、治安領域結合，此部分本文將於後續章節加以整理，另可參見 Kevin D. Haggerty and Richard V. Ericson (2000), The surveillant assemblage, *British Journal of Sociology*, Vol. No.51 Issue No.4, pp.605-622.

[12] 作為網路場域構成基底的程式碼，與本文後續章節欲處理的「結構」問題有所關連，簡言之，構成網路結構的底層場域與現實空間不同，虛擬空間的運作規律依循程式語言而進行，亦可藉由對於程式語言進行的編輯改變其結構。

[13] Toshimaru Ogura，前揭註 7，p.276.

doi:10.6342/NTU201900452

第三款 小結

在一個人人都是觀看者的社會之中，「看」的動作以及周遭視線的存在變得再為尋常不過。也因此，雖然國家仍然是監視技術最主要的使用者與控制者，但交錯於社會之中的監視眼光背後的存在早已不再僅限於國家。個體的視線，在科技帶來的螢幕，例如電視、電腦網路、智慧型手機支持之下，極大程度的擴展了所能到達的範圍。這些技術除了帶來視線的擴張之外，也讓個體同時成為了能夠自行捕捉影像、作為監視目光發起者的存在。在這些技術的圍繞之下，視覺的監視技術已然成為人類感官的延伸，一旦傳遞影像的螢幕存在生活每一個角落，個體同時是監視目光的所有者，也是目標。

但在監視社會持續發展的進程之中，影響更為強烈的反而是「視覺以外」的監視手法。監視的重心從依賴視覺的觀察轉移到對於「資訊」以及「人格」的收集，例如個體活動的軌跡、思想的表達、政治傾向、身體特徵資訊、消費習慣、人格描繪等等。此種監視手法與視覺性監視最大的不同在於，監視的「視線」已經不再需要照射到特定的個體，只需要收集個體的「數據化資訊」即可。**從視線到對資料進行掃描的轉變，同時反映了監視場域從空間轉往數據之轉變。**當然這些資訊大部分仍然需要依賴以視覺路徑運作的傳統監視技術取得，但是取得的資訊一旦轉化成數據之後，這些數據的分析、處理、流動便脫離了傳統監視技術的視覺化路徑，轉而以數據形式的、得以被統計學操作的形式存在。此一特點導致了監視社會的迅速擴張以及看守塔的多點散布。而這些特徵的成因則與監視科技與監視系統的發展有深刻的關聯。以下先針對監視科技的發展現況進行說明，接著再與對應這些狀況的監視理論進行連結。

第二項 資訊科技與監視系統

第一款 監視器(CCTV)

監視器[14](Closed-Circuit Television,CCTV)的普及，或許可以說是監視社會的發展最為顯著可見的特徵。監視器能夠將藉由攝影鏡頭所取得的畫面，放映在電視螢幕上、或儲存在特定的儲存媒介之中留待日後觀看與應用。藉著此一科技，針對特定地區特定時間點的影像收集不再需要依賴人類的肉眼在場觀看，而可以透過監視器鏡頭的事先設置來取得影像。在廣泛裝設監視器的國家之

[14] 原意是指在封閉的迴路之中播放的電視系統，例如錄影機、道路上設置的監視器等等。在英美文獻中，經常用來指涉設置於街頭的監視器系統。參照星 周一郎(2012)，《防犯カメラと刑事手続》，頁 3，弘文堂。

doi:10.6342/NTU201900452

中，路口、車站、甚至店家裡隨處可見的監視器，甚至個人住家、汽車的行車紀錄器、機車安全帽等等，皆成為乘載監視鏡頭的載體。在這些國家之中，一旦離開住家，幾乎就是讓自己暴露在四面八方的鏡頭之下，公共場所中到處散布的鏡頭也幾乎成為習以為常的風景。

作為具備明確象徵意義並且與日常生活切身相關的監視技術，監視器的分布在進入近代之後發展迅速。除了技術門檻較為容易跨越之外，另一個重要的理由便是監視器與犯罪預防之間在形象上的緊密相連。在前述提及的近代化歷程之中，個體逐漸受到重視，而國家政府也被要求保障每個人的安全。以英國為例，作為世界上已架設監視器數量數一數二的國家，在英國國土上至少架設了 420 萬台[15]以上的監視器。值得注意的點是，英國監視器數量持續增長的潮流，是在短期間內達成的。其原因則被認為是在 1985 年 8 月，英國的伯恩茅斯(*Bournemouth)*市議會以對在該市海岸地帶的破壞行為加以遏止為由而開始設置監視器，以避免破壞行為繼續發生。在此之後，監視器系統迅速的由地方自治機關、警察、中央政府機關等等推行、設立。而在英國民間，由於當時時代背景**將犯罪與反社會行動視為對消費者以及商業發展的威脅，同時國民一般傾向認為應該對犯罪帶來的恐怖發起行動**，因此帶來強烈犯罪防治印象的監視器，剛好契合這個時期的刑事政策動向。在新聞報導之中，能夠協助警方破獲重大案件，並且取得極有力證據的監視影像。監視器與破案以及治安維護這三者之間的連結，在媒體的渲染之下便使得監視系統的設置成為民眾心目中維持治安的最佳工具之一。在大眾能夠接觸的電視頻道之上，撥放監視影像這件事情，象徵著鏡頭所籠罩的範圍處在政府、警方的控制之下，犯罪的軌跡被記錄下來這一點，也同時象徵著安全[16]。弔詭的是，在此潮流下被警方用以偵查、破案的監視影像，所針對的標的是已經發生的，存在過去時間軸上的犯罪。「對於過往犯罪的成功破案」與「對於未來的犯罪防治、治安維持」之間還欠缺了一些連結[17]。但媒體的報導以及人民的觀感習慣性的會忽略此一連結，警察機關也

[15] 這個數量來自 Michael McCahill & Clive Norris (2002), *CCTV in London*, Working Paper No.6. 這一篇報告的估計數值，網址為 http://www.urbaneye.net/results/ue_wp6.pdf (最後瀏覽日期:2019.01.11)。

[16] Aaron Doyle. (2006). An Alternative Current in Surveillance and Control: Broadcasting Surveillance Footage of Crimes. In Kevin D. Haggerty, & Richard V. Ericson (Eds.). *The New Politics of Surveillance and Visibility* (pp.199-201).除了在新聞上以監視影像做為報導素材之外，更為容易被民眾所理解的手法是透過電視劇集達成。

[17] 其預設的前提是犯罪者知道監視器的存在後，會因為害怕未來被逮捕接受司法懲罰而選擇不要犯罪，藉此達成犯罪預防的目標。這個想法結合了後續將會提及的理性選擇理論、日常活動理論、環境犯罪學等等議題，並且作為監視器的設置以及影像收集行為其中一個有力的正當化

doi:10.6342/NTU201900452

樂於提供監視影像給媒體進行報導。英國的電視節目例如 Crimewatch UK，與警方進行合作，於節目中每周提供被篩選過的監視影像作為節目內容播放，使得民眾相信他們可以透過監視器追蹤犯罪者的行動軌跡，藉此解決犯罪問題並且增強治安[18]。也因此輿論通常傾向支持監視器的設置。在這些因素的綜合影響之下，使英國監視器設置的數量持續的增加。而持續成長的監視器數量，當然也帶來了是否會發生小說《一九八四》裡面所描寫的威權監視社會的疑慮。但在政治家與媒體的正面評價之下，仍然有越來越多的地方自治機構廣泛的設置監視器，也因此使得英國成為著名的監視器大國。

針對監視器之設置抱有疑慮的論者，則認為針對公共空間所進行的大範圍監視，必然會與權威主義下對人民進行管制的警察活動有深刻關聯。這種全面性的監視將帶來「歐威爾式的噩夢」，並且轉向以高科技為主體的科技警務(techno-policing)，此種警務活動隱含著失控的危險性。因此批判論者將警察描寫為持續收集資料，並且利用新的情報技術來侵蝕個人的隱私權與法律正當程序之組織。並且主張應該為了防止這樣的情況，對 CCTV 進行嚴格的管制[19]。

第二款 管制與效果

由於監視器的設置會帶來侵害人民隱私權的疑慮，因此在歐洲人權條約第八條的要求之下，英國內務省提出以下的標準[20]來檢驗監視器的設置是否對人民的隱私權存在危險性或威脅。1.均衡性(proportionality)，2.適法性(legality)，3.說明責任(accountability)，4.必要性、急迫性(necessity/compulsion)，5.補充性(subsidiarity)等五個要素。簡單來說，監視器的設置目的必須要與人民的隱私達到平衡，並且在法律保留原則下進行。政府部門對於監視器設置的理由、曾經考慮過的替代手段等等皆必須要進行充分的書面說明。而監視器的設置必須是「在民主社會中被認為必要」，且監視器必須以對人民權利侵害最小的方式加以設置。但雖然有著這些要求存在，大部分在公共場合設置的監視器都能夠不費力的通過這些考驗。因為除了惡意針對某些住宅隱私設置的情況，一般來說只要監視鏡頭設置的位置處在公共空間，又能夠有助於犯罪預防甚至交通事故的

理由而存在。但實際上這一個前提充滿了許多需要被說明的問題，並不是表面上看起來這般理所當然，這部分本文將於後續章節處理。

[18] John McGrath (2012), Performing surveillance. In Kirstie Ball, Kevin D. Haggerty and David Lyon(Eds.). *Routledge Handbook of Surveillance Studies* (p.86).

[19] 參考自星 周一郎，前揭註 14，頁 42-43 之整理。

[20] 星 周一郎，前揭註 14，頁 114。

doi:10.6342/NTU201900452

取證，則在隱私與監視器設置兩者間進行利益衡量之後，只要政府部門進行一定的書面說明，並且依法申請設置後，通常都能得到設置監視器的許可。**主要的原因則在於監視器所能帶來的多重功能，以及設置於公共場所時，社會整體對於安全的渴望通常高於對於隱私的要求[21]。**

與英國的歷史發展相類似的狀況也發生在 1990 年代的台灣。在當時的台灣，數起重大刑事案件[22]連續發生，加上電視剛剛普及到台灣民間，這些重大刑案經過媒體大篇幅報導，伴隨著部分拍攝到犯人之監視影像的播放，使得民眾得以透過電視系統與監視影像直接接觸到「犯罪者」的形象以及「刑事案件」的現場。這些畫面一方面為社會帶來恐慌，另一方面也滿足民眾對於社會狀況的認知需求。具體而言，由於媒體居於輿論的優勢地位，並且具備較高之公信力，媒體所報導之狀況經常直接轉換為視聽者對於社會狀況之認知。因此連續數起重大刑案的報導使得社會人心惶惶，政府也在輿論壓力之下開始加強針對治安之維護。例如內政部對於這些犯罪的回應，是自 1998 年起開始推動「建立全國社區治安維護體系-守望相助再出發推行方案」，接著在 1999 年繼續推動「天羅地網」計畫，促成大量監視器的架設[23]。「監視器拍攝到犯人影像」此一事實則帶有兩個詮釋的方向，**一為犯罪事件發生在人民視野可及之處(雖然事實上監視影像要呈現在民眾眼前時，必須藉由未必可靠的「媒體之眼[24]」作為媒介)，二為監視器有助於捉捕犯人以及犯罪偵查。**社區監視系統與網路科技促成警民連線守望相助，便是當時許多地方自治團體提倡的目標。監視器的設置目的，除了在事後協助保留證據以便進行犯罪追訴之外，最主要希望產生的效果如下:**1.嚇阻潛在犯罪人，2.促使更多人願意進入有設置監視器的地區，3.協助警力與保全更有效率的部屬，4.鼓勵一般民眾投入犯罪預防工作。**以保全證據此一功能而言，監視器之設置所能達成之效果較無疑問。因其能夠即時、完整、連續的留下特定範圍內的影像資料，只要影像之品質保持足夠之水準，並且排除掉干擾識別之因素後，監視影像能夠做為有力的證據協助特定類型犯罪的追訴。

---

[21] 星 周一郎，前揭註 14，頁 56-57。

[22] 影響最為重大的主要為白曉燕案、彭婉如案、劉邦友案。這三件重大刑案在當時經過媒體廣泛報導，並且對社會輿論帶來重大影響。

[23] 張煜麟(2004)，〈台灣監視器系統作為集體逃避自由的機制？一種自由主義的觀點〉，《資訊社會研究》，7 期，頁 196。

[24] 媒體報導的案件經過篩選，所能取得的影像來源則須經由警察局或監視器的設置者提供，即便要求媒體自律、報導中立，仍然無法避免報導摻雜入一定的立場。

doi:10.6342/NTU201900452

第三款 監視器與安全

設置了監視器的場所經常被認為是較不會發生犯罪的場所，同時帶來了區域處在控制之下的安全感。加上政府的推動，地方自治團體積極設置監視器並且與警察機關連線亦屬常態。藉由媒體的報導，**監視器與偵破犯罪、維護治安之意象互相連結，並且象徵著治安與安全**。也因此在公共場合設置的監視器，在民眾對於安全的追求之下，較為容易被接受。即便如此，監視器仍然存在部分需解決的問題。首先雖然能夠透過軟體的設計以及硬體設備的加強，使得單一監視器盡可能的涵蓋大量的範圍，但若要取得較為清晰而可供分析的畫面，單一監視器所能拍攝的範圍仍屬有限。

另外亦須注意，就監視器之設置所能達成之效果而言，其最主要被人民寄望能達成的效果固然是預防犯罪發生此一目標，但學者[25]指出，在**犯罪預防領域來說監視器的效果測定受到以下因素影響，因此難以直接將監視器之設置等同於產生犯罪預防效果。**亦即監視器預防犯罪之效果並非絕對，而是受各種因素影響，而主要需考慮的因素如下：1.犯罪種類與設置地區的特性。2.犯罪轉移與抑止效果的擴散。3.事後追訴效果與犯罪偵查的支援效果。4.治安意識的提高與安全感支持。

1.犯罪種類與設置地區的特性[26]

監視器所選擇的地點會極大程度的影響其所能阻止與紀錄的犯罪類型。例如以路口為目標之監視器通常能夠協助交通案件與街頭暴力案件之處理以及針對通緝犯之追蹤。商家自行設置之監視器則能協助偷竊、強盜案件等財產犯罪之處理。而對於在非公共場合(例如家庭)等地發生之犯罪，監視器之設置則較難直接產生預防效果[27]。另外監視器的效果亦會隨著設置地區的區位特性不同有所差異。因此監視器雖然能夠為民眾帶來安全感，但必須要注意其對不同犯罪類型及不同地區的影響程度差異。

2. 犯罪轉移與抑止效果的擴散

監視器的存在固然對特定類型犯罪的犯罪者有一定嚇阻能力，但犯罪者可以選擇轉移到未設置監視器之地區作為進行犯罪的地點、或者採取破壞、迴避監視器的方式進行犯罪。因此可能造成的結果是，監視器密集設置的地區固然降低了犯罪率，但周圍設置監視器數量較少的地區反而提高了犯罪率。抑止效

[25] 星 周一郎，前揭註 14，頁 40-41。

[26] 以下內容整理自星 周一郎，前揭註 14，頁 27-41。

[27] 此一原因在於監視鏡頭覆蓋範圍的有限性，一般來說至多在已經特定犯人之情況下協助追蹤行動軌跡，但於防止犯罪發生這點來說並無多少效用。

doi:10.6342/NTU201900452

果之擴散則是指部分密集設置監視器之地區連帶使周圍地區犯罪率減少。除了這些效果之外，亦有部分研究指出監視器的設置未影響到設置地區之犯罪率，甚至部分區域設置監視器之後特定犯罪類型之犯罪率反而提高[28]。

3.事後追訴效果與犯罪偵查的支援效果

相較於對犯罪預防效果的實證研究結果而言，監視器之設置對事後追訴效果與犯罪偵查的支援效果反而是明顯可見。原因在於影像本身作為證據的證明力強大，雖然受限於監視器之畫質、拍攝範圍等等因素，但一旦成功取得能作為直接證據使用之監視影像，幾乎皆能有效協助犯罪的事後追訴。就協助犯罪偵查之部分來說，由於大部分主要幹道皆會設置監視器拍攝行經車輛、行人，商店內也經常會有私人架設的監視器，這些監視影像能夠有效協助警方追查犯人之蹤跡。

4.治安意識的提高與安全感支持

此一因素是支持監視器設置的重要原因之一。在媒體的報導中監視器經常作為協助破案的重要工具，因此與治安的意象緊密結合。又由於社區治安要求以及地方自治團體的配合，監視器由社區自發性設置的情況也不少見。在這些因素影響之下，投入監視器的設置有助於社區整體守望相助與治安意識的提升。而知悉周圍有監視器之設置也有助於人民對於犯罪預防的安全感提升[29]。

第四款 身分識別與行動軌跡

另外一個重要的發展，是對於身體資訊的收集。隨著收集技術與儲存媒介技術的發展，針對身體特徵的資訊收集與儲存成本持續下降。對於國家來說，身體特徵資訊由於其複製的困難性，能夠成為區別、辨識個體、確認身分的有效工具。與傳統的方法比較，這些具有唯一性而難以偽造的身體特徵，在國境管理以及身份辨識上較能夠保持正確性。

以實際應用的辨識技術來說，經常被收集的目標有虹膜、指紋、DNA 等等。需要注意的是，這些資料的儲存其實有著許多種應用的可能性，例如在智慧型手機上使用虹膜、指紋辨識等等方式確定使用手機者是否是本人，或是針

[28] 論者指出可能的因素是由於監視器之設置使得原本未能發覺之犯罪黑數浮出水面，例如在道路上進行的鬥毆行為。參見星 周一郎，前揭註 14，頁 39。

[29] 雖然實證研究上究竟安裝監視器對於特定區域特定類型犯罪預防的功效如何莫衷一是，但可以確定的是人民比較容易對監視器較多的地區具有安全感。相較於犯罪白皮書等官方文件公布的犯罪統計，在日常生活中四處可見的監視器反而更能夠象徵著社會的治安狀況。

doi:10.6342/NTU201900452

對被判刑的犯罪者收集指紋、DNA 資料用以建構資料庫等等。這些資訊的收集與辨認直接連結到個人的身體，並且能夠實現對身體的識別與控制。例如對於國境出入人口的控管，藉由指紋來對個體進行識別，便是準確率與效率較高之方法。

早期的監視器系統，受限於儲存媒介的大小以及零件故障、影像解析度問題，所能取得的監視影像之品質與數量皆較為有限。但在現代電腦與網路技術的支持之下，影像的儲存、傳輸、處理門檻已經大幅降低。影像不再只是保存封閉的迴路電視之中，而是可以進行再製、加工、分析的媒介。在監視器問世之前，要收集特定地區的影像，必須要依賴人力藉由肉眼或是攝影機來進行。但在監視器技術持續發展之後，只要配合電腦系統運作，可以使監視器在無人控制的情況下自動進行大範圍收集影像訊息的工作。同時監視器也是其他監視技術賴以進行的基礎平台之一，例如異常行為識別系統、人臉辨識系統、車牌辨識系統等等系統，皆是將監視影像加以分析處理的應用結果。在設置足夠數量監視器的國家之中，藉由這些自動進行的、持續性的、依循時間軸的大量影像的收集與儲存，這些系統有了大量能夠加以運用的素材以使監控的範圍更加擴大。

例如在犯罪偵查領域中，科技定位監控，亦即以科技設備或技術掌握特定對象於公開場所中行止的偵查方式，逐漸取代人力跟監及無線電波發報器的使用。科技定位監控主要藉由 GPS 追蹤器以及行動電話訊號定位等方式進行。GPS 因為其能達成隨時定位、精準度與效率較高等特性，對於警察機關而言是定位特定對象的利器[30]。行動電話訊號定位則可透過相關技術與數學公式計算，分析行動電話訊號位址資訊，掌握該特定對象的移動路徑及其所在。除此之外，監視器技術的提升也是支持科技定位監控的重要原因之一。現今的監視器所能達成的目標，已然遠遠超出了其原本的設計紀錄影像用途。除了監視器網路化之外，主要尚有以下重要技術[31]:

1.觀察技術

亦即使監視器得以上下左右迴轉、縮放視野、夜視、紅外線追蹤等功能。此種觀察技術可以手動操作，亦有可能與 AI 結合交由電腦自動控制。

2.記錄技術

使影像同時包含時間、地點、經過車輛數、經過人數等因子，便於儲存、

[30] 李榮耕(2015)，〈科技定位監控與犯罪偵查：兼論美國近年 GPS 追蹤法制及實務之發展〉，《臺大法學論叢》，第 44 卷第 3 期，頁 874。

[31] 以下整理自星 周一郎，前揭註 14，頁 16-17。

doi:10.6342/NTU201900452

計算、檢索之技術。

3.追蹤技術

搭配觀察技術與網路化連結，可以使複數個監視器即時追蹤特定目標的行蹤，也可以從保存下來的監視影像中快速抽出特定目標的行動軌跡。

4.認證技術

以人物的面部特徵或車輛的顏色等特徵以及車牌的辨識等手法來協助識別目標物之技術。

5.數位遮罩技術

搭配觀察技術，藉由程式設定使監視器自動迴避有較高隱私保護需要的區域、或者屏蔽目標以外人物之技術。

6.影像的密碼化技術

藉由密碼、影像模糊化等認證方式避免影像外洩之技術。

7.電子浮水印技術

藉由電子浮水印確保影像為真正，同時記錄曾經對影像進行連接的時間次數等資料之技術。

針對特定標的行動軌跡的追蹤，即是以上監視器科技與其他監視技術結合所可能進行的手法。在這些技術的綜合應用之下，對於特定個體的資訊收集達到新的高度。其應用的手法又可分成以視覺性質監視系統為主體的監視影像路徑，以及以其他個人資訊足跡為主體的個人資料路徑。以監視影像路徑來說，普遍的使用方式係以特定區域中大量設置的監視鏡頭為基礎，取得大量的監視影像。之後將這些影像以人力或電腦軟體加以處理，確認標的出現在不同監視鏡頭的時間點之後，定位標的在特定監視區域中行動的軌跡並且進而預測標的離開監視鏡頭所及範圍之後可能的移動路線[32]。此種技術經常被用以協助犯罪偵查，通常針對的標的則為人體與車輛。較早期員警調閱監視影像時所使用的手法通常是以人力進行，例如以案發地點為中心，鎖定可疑嫌犯後以同心圓方式逐步調閱周遭監視器預估案發時間段的監視影像，並最終找出嫌犯。但此種以人力進行篩選的方式效率較為低落，處理大量影像的時間成本也較高。在效率的要求之下，資訊科技逐漸被導入監視影像的處理之中。藉由電腦與軟體的設計來對所取得的監視影像進行分析，能夠大幅提高影像辨識的速度與效率，

[32] 溫哲彥(2013)。〈影像處理技術於偵查與鑑識之應用－由二維到三維空間〉。載於法務部司法官學院(編)，《刑事政策與犯罪研究論文集〈16〉》，頁 244。

doi:10.6342/NTU201900452

同時有助於辨識標的的精準度提升[33]。其運作的方式，是將標的的特徵加以編碼，以程式運作的方式在影像之中找出包含此一編碼或類似編碼的數據，特定並標示出來[34]。可能被用以追蹤的特徵以人物來說例如身高、衣著、面部特徵等。以車輛來說則是車牌號碼、烤漆顏色、車款等。只要系統內監視鏡頭的數量足夠多，或者有更廣範圍的監視鏡頭被涵蓋在系統之中，可以說要追蹤甚至預測出現在監視鏡頭之下的特定標的行蹤並不困難。

除了事後對收集到的影像進行分析之外，針對特定更高安全需求區域可以採用即時影像判讀技術，直接由系統偵測危險源的發生，並在影像中出現設定狀況時直接發出警報。常見的應用例如針對距離較長的隧道出入口及內部設置鏡頭偵測是否有車禍、火災等等情況發生，以及銀行針對提款機或銀行出入口設置鏡頭偵測進入人士是否穿戴口罩、安全帽[35]，或者藉由人臉辨識系統以及資料庫的建置達成更加精確的人臉資料[36]蒐集等。下一個階段的應用則是對於可能發生之危險的預測。例如在大眾運輸系統的車站中針對過度靠近月台邊緣的人物進行特定，或者針對集會遊行群眾進行攝影，及時特定可能產生失控狀況的位置以便進行處理等等[37]。這些以高科技為基礎，或者以資料庫與比對軟體為基礎的整合監視系統，固然有較高的可能性達成其預設目標，但同時也帶來了更進一步侵犯隱私的問題。**原因在於監視影像所牽涉到的個人資訊，此時不單純只是被收集，而是被進一步用來分析、處理、儲存。**就此問題，有論者認為可以在設計整合監視系統時藉由程式的運作盡可能地規避過於嚴重之隱私權侵害，例如以影像辨識技術進行處理，將監視影像拍攝到的人物自動以馬賽克模糊化，在警方確實有偵查需要時再以逆向解碼之方式除去馬賽克[38]。此一想法雖然確實有助於隱私之保護，但仍無法迴避監視器本身持續性的收集影像所帶來的疑慮。

---

[33] 謝劍斌等人(編著)(2016)，《無人監控：技術原理與應用》，第五章〈巨量視訊搜索〉，佳魁。

[34] 溫哲彥，前揭註 32，頁 242-243。

[35] 溫哲彥，前揭註 32，頁 244。

[36] 人臉辨識系統在技術運用上尚有許多影響辨識精確度之因素，例如帽子、鬍子、髮型、身型的改變，以及監視器本身影像解析度是否足夠系統進行辨識、以及人臉資料庫之資訊是否充足等等。

[37] 謝劍斌等人(編著)，前揭註 33，第六章〈異常行為識別〉。其中提及的常見可疑行為例如徘迴、聚集、尾隨、遺留物品、越界、攀爬、匍匐、跳躍、下蹲、倒地等等。

[38] 小林健人、稲村勝樹、金田北洋、岩村惠市(2016)，〈プライバシ保護と犯罪防止を両立させる監視カメラシステム〉，《情報処理学会論文誌》，Vol.57 No.1，頁 172-183。

doi:10.6342/NTU201900452

第三項 小結

監視器作為監視技術最為直觀的代表，其發展也經常與其他監視技術進行結合，或者作為其他資料收集的基礎技術。監視器之設置與犯罪意象緊密連結，同時具備與各個監視技術均能互相連接的特殊性質，影像辨識技術的提高澤強化了對於行動軌跡追蹤的可能性，以及即時判斷危險源是否發生之能力。但隨著監視技術的自動化、網路化、藉由監視器所能蓄積的資料量也大幅提高。

第二節 資料與監視技術

第一項 官僚組織

監視社會除了監視技術發展之外的另一個重要特徵，**是透過監視技術所達成的資料蒐集的便利性、數量、與範圍的擴大。**大量累積的資料儲存在許多資料庫之中，這些資料的取得與應用過程中所蘊含的問題便變得十分複雜。其中需要先提及的是作為重要近代特徵之一的官僚組織，因為官僚組織通常同時也會是監視技術的主要掌握者。由於官僚制度被認為是使民主主義得以運作的手段之一，且因為在資訊傳遞的機關之中有著上下層級的設定，同時特定事項的資訊傳遞被要求秘密進行、機關所有的權限由規則和法令定義等等原因，因此被認為是技術上較為優良的社會組織型態，在現代廣泛被各國政府所採用。而由於官僚制度有著監督、收集資訊的能力，因此其也做為監視的一種形態而呈現。最主要的原因有以下幾個，由於官僚制度依循著能被檔案化的知識(在官僚組織之中被集中保管著的資訊)、以及一定的規律(法律、行政規則、行政命令)等等合理的規律而運作，其必然需要大量資訊的保管與累積[39]。由**官僚組織所進行的監視具備著不具感情的、精密計算的、如同機械一般進行的性質，並且主要由四個要素影響其進行：檔案的容量、中央集權化的程度、情報流動的速度、直接接觸人口之監視地點數量[40]。**這幾個要素，在資訊時代中由於科技以及電腦工具的發展，這幾個要素都得到了技術上的增強，也促使官僚體制的運行更加強固，所能收集、保存的資訊更多。

但是，官僚制度的運行也有其問題。Lyon 借用 Weber 針對官僚組織的闡述，認為在官僚體制內工作的人，將會傾向確保自身的權利並且試圖迴避來自

[39] 在官僚體系之下如果要使機關的權責得以劃分，便需要明確的分離出各個機關所負責的工作內容為何，並且留下過往處理類似案件之紀錄以供遵循。

[40] David Lyon，前揭註 1，頁 127。

doi:10.6342/NTU201900452

上層機關的監視，而且容易為了自身的便利而固執於規則的運作。Lyon 並且以「對情報的饑渴」來形容官僚制度之中非必要的派出更多人力，以蓄積更多檔案的傾向[41]。在將官僚組織與監視技術進行連結之後，Lyon 並且進一步認為，這一個渴求更多情報的傾向，在資訊時代更加增幅。**其原因是資訊的流動、取得、儲存、處理在科技輔助之下更加快速而容易，**其中最關鍵的因素即是「**在不同目的下，能夠迅速連結到個人資訊的資料庫**[42]」。Lyon 初次提出此一概念的時間點在西元 2002 年，以當時的硬體環境尚無法廣泛的使用此種資料庫，且資料庫的容量以及不同資料庫之間的連接也有其極限。但在本文寫作的時間點，資料庫的建置、資料的搜尋、切割、組合、再利用等等問題，皆已不再有難以克服的技術門檻存在。除了各國政府對這些資料庫有所掌握之外，連企業以及網路供應商皆可能建置供自身商業使用的資料庫。甚至是個人也僅須透過智慧型手機或平板電腦等小巧的終端，即可連接上龐大的資訊網路獲得資料。

官僚體系之下的機關，在其成本允許的情況下，為了更有效率的履行職責、或者更方便的執行管理，會傾向將手上所有的資訊精緻化並且建立供機關使用的資料庫，如此一來其能更精確的判斷其職務應如何履行[43]**。**也因此，官僚組織將會需要更大量的資訊來做為運作基礎。這一點可能產生過剩收集情報的疑慮，而此一疑慮也不僅僅存在政府機關之中。在商業與社群網路層面，個人資訊的監視與大量收集同樣蘊含許多商機，在消費導向的社會之中，由企業進行的顧客資料收集變得越來越普遍。而其收集資料的方式也與官僚組織的運作類似，不會對所收集的資訊抱有感情，而是注重在數據如何取得、呈現、轉化成可以被使用的資料。由這種私人組織所進行的資料監視與收集，也反映了後續將會提及的轉變，亦即監視視線的圖像不再是直線的上對下關係，或是圓形監獄般的環繞關係，也不是樹狀圖般的延伸，而是液體化的流動、塊根狀的分布。各個監視節點所追求的也不是全知的資料收集，而是注重在節點與節點以及伺服器之間的資料串連。簡單來說，監視的目光未必要以視線的方式存在，監視的標的也未必僅限於身體。穿透過身體的監視目光與其說是視線，不如說是波，而這種波是由各種監視節點所發射，能夠穿透整個身體。資訊的碎片被這些節點收集，而後在各自的資料庫之中視需要重組。舊型態的依賴視線的監視也作為其中的節點存在。

第二項 個人資訊與社會安全

[41] David Lyon，前揭註 1，頁 126-127。

[42] David Lyon (2002). Surveillance as social sorting: Computer codes and mobile bodies. In David Lyon (Ed.). *Surveillance as Social Sorting: Privacy, risk, and digital discrimination* (p.14).

[43] David Lyon，前揭註 1，頁 126-127。

doi:10.6342/NTU201900452

第一款 安全社會的追求

監視技術包含各種能夠針對個人、群體收集並保存大量資訊的手段。此種收集資料的欲求，除了用以支撐前述的官僚組織運作必須之外，還受到許多不同因素影響，例如安全、福利、消費需求等等。

20 世紀之後，安全的追求成為影響監視技術發展的重要原因。由於 911 事件以及其後接連發生的恐怖襲擊，導致以保護國家安全為目標的監視以及對國境控制的要求迅速發展。尤其影響重大的是，美國國土安全部(DHS)的設立。在反恐的旗號之下，國土安全部的業務最初是以市民的全情報認知(TIA, Total Information Awareness)為目標，並且使用大量的資料庫來進行資料的挖掘、連結、精製。其具體運作的方式，是將諸如自動提款機的使用、信用卡的刷卡履歷、網路瀏覽器留下的快取紀錄、病歷檔案、社群網站使用紀錄等等各種資料收集整合，**針對所欲調查的個人將與其相關的資料互相連結，整合出可能具有一定意義的關聯性。**藉此判斷對象的安全性、是否與恐怖份子有所關聯。這樣的預測手法，依賴著詳盡的資料收集，以及資料庫之間迅速的互相串聯，藉此實現對於個人資料與行動軌跡的大範圍追蹤。這一點與前面所提到的官僚組織圖像十分符合，同時也體現了資訊時代的監視特徵之一，即資訊的整合使用。

除了國土安全部之外，在 911 事件之後，美國國家安全局也開始推動 PRISM 計畫(稜鏡計畫)以進行網路監控。該計畫於 2013 年被衛報與華盛頓郵報公開，計畫的目的，是監視收集美國境內與國外的通訊，以檢查是否有恐怖攻擊的可能性。計畫運作的方式，是以使用電信服務商[44]的境外客戶以及與國外人士通話的美國公民為對象，對使用網路電信服務進行的即時通信和伺服器上所儲存的資訊進行監控，使美國政府可以得到使用者的電子郵件、影像、語音通話、照片、文件傳輸等等內容，並藉此檢查通訊內容是否與恐怖組織有關。此一計畫的前身，是美國總統小布希任期中，在 911 事件之後推動的恐怖份子監視計畫(Terrorist Surveillance Program)。從這些計畫的推動看來，911 事件與後續發生的恐怖攻擊事件，成為加強監視以追求國家安全的重要理由之一。但以前面提到的幾個計劃實際運作的情況來說，也帶來了侵犯隱私權的疑慮。

而在國土安全的控制方面，伴隨著身體識別技術的發展，出入境各個國家除了護照之外，經常需要留下更多足以代表個人身分的資料[45]，而國家對於入境者的資訊收集，也更加注重。這些管制以及資料收集的目的，固然是為了因

[44] 如 Google, Facebook, Microsoft 等等公司皆在被揭露的名單之中。

[45] 例如入境日本時必須在海關留下指紋紀錄。另一個影響則是出入境時安檢的嚴格程度提高，同時對於可以攜帶上飛機的行李也加上更多限制。

doi:10.6342/NTU201900452

應國家安全的需要，卻同時也顯示出在國家安全以及國境管理這面大旗之下，個人的隱私權經常在利益衡量的過程之中處於較容易被犧牲的位置[46]。

第二款 社群網路與通訊軟體

2004 年之後一連串社群網站的出現，則使得社群網路與監視技術、個人資料的收集進入新的次元。在社群網路的發展中，監視技術不再是單向的、透過視覺而進行，而是由用戶亦即資料提供者主動的參與到資料分享的過程中，社群網路供應商則透過收集用戶所留下的網路足跡來取得用戶的資料，並且藉此達成監視的目標。舉例來說，作為規模龐大的社群網路供應商之一，Facebook 從許多地方收集用戶的資料。與政府所進行的具有強制性質之資訊收集不同，社群網路供應商收集用戶的資料，是在取得用戶同意之後才進行的。即使用戶並不一定真正理解有哪一些資料被利用、也不清楚如何利用。

以其資料政策敘述的內容看來，從用戶使用 Facebook 傳遞的訊息、所參加的社團、人脈網路、付款資料、使用裝置的資訊、打卡地點等等，都在其收集資訊的範圍之內。Facebook 收集的這些資訊，最主要的用途是經由演算法的整理，來決定呈現在用戶時間軸上的動態、以及投放的廣告類型。除此之外，還會將這些資料分享給與其合作的遊戲開發商、廣告商、第三方網站等等。透過這些功能，其能收集極大量的個人資訊，而這樣中心化的資料儲存也可能帶來極大的風險。如果需要，**能夠輕易地從其收集的資料之中拼湊出用戶的生活圖像，甚至在用戶沒有打開應用程式時，仍持續從使用的裝置之中收集用戶資料。**而這些資料的收集其實也都在用戶的同意之下進行。簡單來說，這些網路平台除了允許平台供應商收集用戶資訊之外，也同時培養了用戶在平台之中留下訊息的習慣。而這一切經常是在用戶的無意識之下進行。原因在於服務的便利性、隱私資料條款的複雜、以及交互介面的設計結構。

第三款 消費與物聯網

[46] 林子儀大法官於釋字第 603 號解釋協同意見書中便認為，相對於全面蒐集本國國民指紋，於國境管理方面蒐集出入境之外國人指紋較有正當性。首先，為入出境管制及國境安全之目的，針對外國人蒐集生物資訊；與基於不特定的人別辨識需要，蒐集全國人民之生物特徵，係不可相提並論之二事。國境管制較諸於國民的一般身分辨識有更高的需要、更明確且狹隘的適用範圍及更多的自主決定空間，因此也較具有正當性。可見得在利益衡量的天秤之中，本國人與外國人得以合理的給予差別待遇，例如於出入境時收集指紋資料等等。

doi:10.6342/NTU201900452

第三個領域，是消費取向下進行的對消費者之監視手法。對於廣告供應商與商品供應者來說，如果能夠針對較可能對商品抱有興趣的客群精準的投放廣告，則廣告的投放成本能夠下降，販售商品的成功機率也會提高。但是在一般情形下，客戶對於特定商品是否具有興趣、是否有購買之能力等等因素，在其第一次購買特定商品之前並不容易探知。以往販售者需要透過對顧客進行的市場調查、反覆購物習慣的觀察等等方式，才能確定特定的個體是否屬於商品的消費客群。但進入網路資訊時代之後，隨著個人用資訊終端的發展以及使用網路的人口越來越多，個人的興趣與購物傾向更加容易在這些介面之中留下痕跡。以往想要知悉一個人在日常生活中經常購買的物品類型，需要花費的資訊收集成本太高，不符合效益。但一旦這個人開始使用信用卡、網路商城購物，並且在網路上瀏覽資訊、使用搜尋引擎服務之後，了解一個人的購物傾向突然變得不再困難。使用信用卡留下的消費資訊由於保存在銀行，相對來說可能較為安全，至多作為銀行內部消費金融產品的參考。但在網路商城以及搜尋引擎的使用條款中，通常都載明了這些供應商將收集用戶的瀏覽紀錄與購物履歷，並且提供給商品供應商及廣告業者。甚至購物網站自身也會收集顧客每次瀏覽、購買商品的紀錄，推算出可能比較容易激起購買慾望的商品，並且呈現在推薦購物清單之中，或者適時提供特定類型商品的廣告給予特定顧客。

對於業者來說透過這些資訊的收集，讓廣告精準的投放到可能購買商品的客群這一點，在銷售策略上是一項重大的突破[47]。尤其透過收集瀏覽紀錄、搜尋關鍵字等等方式所進行的購買傾向與顧客資訊收集，所得到的顧客興趣傾向推測，遠比透過問卷、市場調查等方式來得高。因為問卷調查等等方式，皆有誤差的可能性存在，但顧客在使用網路瀏覽資訊以及購物的時候，所搜尋的多半都是真正感興趣的事物。只要使用網路供應商所提供的搜尋引擎或是購物網站的購物服務的次數越多，**整合了顧客的年齡、收入、興趣愛好、購物習慣的「顧客檔案」，就越容易被完整的建立出來[48]。**監視技術在此表現的形式，主要是供應商對顧客交易履歷的收集、購物喜好的分析、未來購買傾向的預測。此種對於顧客個人興趣以及品味的監視，可以說是與傳統監視目的截然不同的全新面向。**此種監視不具備古典以來描繪監視技術時，經常採取的以「控制」為目的或者帶有規訓動機的形象[49]。**因為消費者的靈魂與自我究竟如何選擇並非其關心的重點，這一點不同於本文後續章節所提及的圓形監獄與規訓之模型。

---

47 Joseph Turow (2006). Cracking the Consumer Code: Advertisers, Anxiety, and Surveillance. In Kevin D. Haggerty, & Richard V. Ericson (Eds.). *The New Politics of Surveillance and Visibility* (pp.282-283).

48 Oscar Gandy, JR (2006). Data Mining, Surveillance, and Discrimination in the Post-9/11 Environment. In Kevin D. Haggerty, & Richard V. Ericson (Eds.). *The New Politics of Surveillance and Visibility* (pp.364-365).

49 Kevin D. Haggerty and Richard V. Ericson，前揭註 11，p.615。

doi:10.6342/NTU201900452

其也不具備控制顧客行為的動機、亦不具有一個「善」的價值追求[50]。毋寧說這些業者所關心的是顧客是否消費，以及驅動消費的動機如何創造。更有效地賣出商品並且促進消費的進行，才是消費面向之監視所想要達成的目標[51]。監視技術在這些網路供應商以及銷售公司的運作之下，與資本/消費關係有著緊密的連結。同時對於顧客來說，能夠針對自身需求提供即時資訊的服務也未必沒有好處，方便快捷的購物以及消費資訊的迅速傳遞，皆是顧客願意繼續使用網路購物服務的理由。也因此，如果試圖以權力運作的觀點來看這些對顧客進行的資訊收集行為，在解釋上有可能會遇到困難。

另一個問題，是物聯網與身體之間的關係。在研究動機裡所提及的日本政府未來施政構想之中，有幾個特殊的點值得注意。首先是其讓老年人配戴隨時監測身體情況並且與醫療機構連線的手環，可以針對老年人所患有的症狀或慢性疾病所可能呈現的身體特徵(例如血糖的降低、不正常血壓)即時反應，並在需要的時候通報醫療機構。而家裡的冰箱也與網路相連，會及時偵測冰箱所剩的食材，並且提供直接透過冰箱快速訂購食材的服務。家中小孩則配戴智慧型手環，在上下學時提供定位以及與警政機關隨時連線的作用，並且搭配與監視系統一同設置的犯罪預測系統，預先防止可疑人士或歹徒實行犯罪[52]。在政策所描繪的藍圖中，生活是如此便利與安全。但此一政策構想也帶來許多值得討論的問題，例如身體資訊的收集、監視系統的廣泛建置與安全之間的連結，以及透過這些資訊所進行的未來預測可靠程度以及可能帶來的風險等等。於此先處理身體裝置與身體資訊、生活資訊的收集問題，簡單來說，物聯網與身體裝置能夠直接的使得監視技術與身體緊密連結，並且直接達成對於個體的持續的、自動化的資料收集。

政策構想所提及的身體裝置與智慧型家電，或者說所謂的「物聯網」終端，在現代科技與網路的支持之下要加以應用並不困難。但這些裝置現階段有幾個問題存在，一是資料的過量取得與資料使用流向的不透明，以及物聯網終端的資訊安全漏洞問題。例如在智慧型手機之中，網路供應商所提供的地圖與 GPS 定位服務來說，在連接網路的狀態下其會持續記錄手機所在的位置資訊，

[50] 在進行消費取向監視的同時，監視者可以藉由所取得的資訊對商品的廣告投放、銷售方式等等內容進行調整以使得消費者更容易接觸到特定商品，或是更願意購買特定商品。其具體運作方式可能有調整商品擺放位置、針對不同消費族群提供不同種類優惠等等。雖然以消費取向監視作為基礎的前提之下確實能夠藉由這些手法對消費者消費之動機進行影響，但本文認為其與後續將處理的圓形監獄中監視與權力運作的方式仍有程度上的不同。

[51] Kevin D. Haggerty and Richard V. Ericson，前揭註 11，p.615.

[52] 參見日本內閣府官方網頁，針對イノベーション 25 政策之說明，取自：https://www.cao.go.jp/innovation/，最後瀏覽日期 2019.01.11。

doi:10.6342/NTU201900452

甚至協助分析使用者這一個月使用交通工具以及步行的時間，以及行動距離的長短。在使用者抵達交通轉運站時會詢問是否需要時刻表資訊、抵達特定商家時會詢問使用者對該商家是否願意評分或給評語等等。APP 的使用者經常為了功能上的便利，開放過多權限或者是概括授權 APP 收集資料。另外進行電子支付時，也會在商家、電子支付端、進行電子支付的終端等地留下數位軌跡，例如搭乘大眾交通工具的進出站紀錄等。在這些身體裝置與物聯網的組合之下，對於特定個體的「生活 style」收集變為可能。這一點帶有藉由對於身體資訊的了解以對人口進行控制的空間。雖然現今大部分出現的身體裝置形式停留在計步、測定血壓、提醒吃藥時間等看似對隱私並無太大侵害之功能甚至是對個體有所益處，但與物聯網概念結合之後，身體裝置所收集的資訊一樣能夠被數據化並連接到資料庫之中。而這些資料收集的方式帶有「持續性」與「指向性」特徵，亦即只要身體裝置持續運作且連接在網路上，資料通常也會持續被收集。且資訊與個體將被綁定，身體被納入成為資訊網路的其中一員，並且能夠以網路、電信途徑追蹤到特定個體的身體軌跡。

第三項 個人資料與監視技術應用

單純的資料收集未必會直接對個人帶來不利益的結果，但大量累積的資料如果經過整理、分析、應用，則可能產生嚴重的影響。依個人資料保護法第二條之規定，個人資料指**自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料**。個人資料保護法在個人資料的定義上採取一個寬鬆認定的標準，除了其所例示的幾種資料類型之外，將社會活動以及其他得以直接或間接方式識別特定個人的資料也納入範圍之中。究其原因，乃是因資訊社會之中，個人資料的使用在社會生活中不可或缺，且型態也極大程度的發生轉變。而這些資料除了有利於國家政府統治的進行之外，也經常被用在商業與消費的用途。在這個寬鬆的定義之下，有幾種較特別的資料型態與監視技術密切相關。

第一款 新種類資料類型[53]

1.電子通信紀錄

[53] 整理自 Ernesto U. Savona (2004), *Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research*, pp. 84-89.

doi:10.6342/NTU201900452

依照通訊保障及監察法第三條之規定，所謂通信紀錄指電信使用人使用電信服務後，電信系統所產生之發送方、接收方之電信號碼、通信時間、使用長度、位址、服務型態、信箱或位置資訊等紀錄。這些資訊無法直接指涉個體使用資訊設備所進行的「通訊內容」，而僅能得出通訊的時間、地點、長度、對象、所使用的設備等資訊。但藉由這些資料的收集與分析比對，能夠辨識出通信雙方的關係。

2.定位資料

定位資料主要包含前所述及的 GPS 與手機位置資訊兩種，除此之外尚有社群軟體打卡、圖片拍攝位置等等變體。這些資料除了用以確定終端(GPS 接收器或手機)所處位置之外，亦可用以追蹤特定車輛的行蹤、甚至用以描繪個人的人格檔案。智慧型手機中所開啟的定位功能也能持續收集手機所在位置的資料，並且由網路服務供應商保存。

3.影像資料以及生體特徵分析

影像資料的取得主要依賴監視錄影系統的設置，並且作為監視技術較基礎的平台加以運用。通常可以搭配人臉辨識技術、車牌辨識技術、特定人物行動軌跡追蹤等等系統應用。生體特徵的分析則包含聲音、指紋、虹膜、DNA 數據等。生體特徵分析最大的價值是個人身分的精準識別，相較於其他的個人資料，生體特徵的偽造難度較高，也因此廣泛用於國界管理等用途。

這些新型態的資料收集手段有助於更精確地對個體達成識別，並且進一步為後續的決策目標提供資訊。

第二款 統治的應用

個人資料的收集與監視技術，在政府的統治目的之下有許多應用的可能性。以新加坡為例，論者指出[54]，「新加坡的監視社會是各種媒介例如監視器、網路、監視資料庫的連結與再現，整合了成實體空間與虛擬空間的數位化監視網絡。」在新加坡的公共空間中，幾乎每棟建築物內外都設置了隱蔽的監視攝影系統，且為達到更好的監視效果，鏡頭還可調節遠近追蹤目標物。車輛安裝讀卡器搭配公路電子收費系統、衛星掃描交通系統、高速公路監察與提示系統、衛星傳呼計程車系統等多重監視設備。搭配上人口、住屋登記系統的登錄，在新加坡要追蹤到特定國民的行蹤並不困難。其中值得注意的是，除了針

[54] 董娟娟(2005)，〈詮釋新加坡發展的新路徑：監視社會研究的新解與展望〉，《台灣政治學刊》，第 9 卷第 2 期，頁 110-112。

doi:10.6342/NTU201900452

對現實的社會環境進行監控之外，網路此一平台原本被認為是推廣民主反抗威權的的重要工具之一，但藉由傳媒法令限制網路通訊內容、由網路服務供應商對通訊進行監控、阻擋特定網站內容等等方式，新加坡政府成功使得使用網路的群眾為了避免平台無法使用而開始自我審查，進而達成防止社會團體運用網路作為爭取民主場域的目標。禁制法令、技術控制、監視系統、懲罰行動等各個手段結合之後，網路等新科技的政治社會應運迅速轉化成監視、控制、治理人民的輔助道具[55]。在這些交錯之下，實體社會空間與虛擬社會空間中已然被佈下了複雜的監視手法。固然因為新加坡面積與人口密度因素，使得當地政府施行這些監視手法的成本相對來說較其他國家低廉，而使得其他國家未必能全盤複製新加坡所採取的手法，但採用多重監視手段構成的監視網路，其實在各個國家都有程度不一的類似設施存在。例如我國的 ETC 收費與車牌辨識系統即能明確的辨識行駛於國道上的車輛資料。

中國新疆則成為威權統治與監視技術應用的實驗平台。依據人權觀察報告揭露之內容[56]，當地居民的智慧型手機中必須安裝政府提供的監視應用程式，車輛則安裝 GPS 定位系統。唯一允許使用的通訊軟體是微信，而政府當局能夠藉此監聽電話與通信的內容。除了應用高科技技術之外，當局也使用大量的人力介入當地居民的生活之中。當地人民被依照信仰、種族、對政權的危險程度等等因素區分成「放心人員」、「一般民眾」、「危險分子」。公安部門使用「一體化聯合作戰平台」，系統性的收集民眾的個人資料。監視系統配置人臉辨識系統與紅外線感測，WIFI 嗅探器可以收集電腦手機等上網裝置的識別位置，通過交通檢查站時也會將交通工具的資訊記錄下來。除此之外，日常生活的資訊一樣是被記錄的標的。例如購車、就醫、計畫生育、銀行卡、司法紀錄等等，均會被整合到該平台之中，甚至購買菜刀時，需要於系統中登記購買菜刀之資訊，並在菜刀上打上浮水印。這些數據的收集並沒有說明理由，當地居民也無法拒絕數據的收集，而資料的收集確實也能夠為官方的統治帶來極大的便利，因為當地公安執法時能夠快速掌握人民的身分資料。但是背後潛藏的危險，則是威權政治以及言論自由的控管。因為一旦人民的記錄顯示出政府不願意人民表現出來的傾向，其就有可被分類成政府不願意看到的「危險分子」，而受到公安的差別待遇，甚至被送進類似集中營的機關進行思想改造。

[55] 董娟娟，前揭註 54，頁 121-123。

[56] Human Rights Watch, “Eradicating Ideological Viruses” China’s Campaign of Repression Against Xinjiang’s Muslims, September 9, 2018.取自：https://www.hrw.org/report/2018/09/09/eradicating-ideological-viruses/chinas-campaign-repression-against-xinjiangs，最後瀏覽日期 2019.01.17。

doi:10.6342/NTU201900452

依照中國大陸國務院關於印發社會信用體系建設規劃綱要[57]所設定的目標，中國大陸在各地開始推行社會信用評分制度。值得注意的是，雖然中國大陸政府所使用的名目與政策目的是以社會信用為名，其所涵蓋的範圍卻遠遠大於一般金融業務中對客戶所進行的信用評估。大部分銀行對於客戶所進行的信用評估僅涵蓋到薪資與工作狀況、過往信用紀錄、是否有金融犯罪等等因素。社會信用評分制度可能收集個人資訊用以評估信用分數的範圍包括：位置信息、交友關係、健康記錄、保險、私人通訊內容、財務狀況、遊戲時間、智能家居統計、首選報紙、購物記錄以及約會行為等等。這些資料的來源來自社交網路，公共和私有機構等平台的數據。而這些數據通常來自於個人在這些平台自有的帳戶資料，以及網路活動紀錄，平台運營方可以分析個人留下的的數據軌跡從而獲得完整的社交檔案，並且這一切皆在人民的同意、政府與公司的合作之下進行。該政策的終極目標，係以獎懲執行的方式，促使人民遵守社會信用系統的各個評分項目。其懲罰內容例如無法搭乘交通工具、無法開設公司、無法使用金融服務等等。而社會信用評分得到較高分數的人民，則能夠享有房屋補貼、優惠貸款等等服務。除了獎懲機制之外，由於社會信用評分系統所收集的資訊範圍廣大，政府一方面能夠掌握民眾的思想傾向、行動安排，另一方面，也能夠通過各個平台的配合進行網路封鎖和控制，並且有針對性地引導輿論。最常見的手法便是設定特定關鍵字，使這些關鍵字無法被搜尋。此一信用評級系統在科技與網路的支持之下，逐漸在中國大陸推行。

這些統治的應用呈現出一個特點，即透過監視技術的環繞，造成民眾自我規訓自我審查的傾向產生。監視技術→資料蒐集→分類(sort)→差別待遇的過程之中，制度的建構者對於「良民/優秀勞動力」之形象以不同個人資料因素做為區分標準，因此在這些體制之中，人民被要求的目標並非關注自身，而是如何達成分類表中的項目、如何獲取較高的評分與較佳的差別待遇。

第三款 福利與安全的應用

另外一個應用的方向是福利政策的使用。與福利掛勾的監視類型可以追溯到 19 世紀至 20 世紀，當時在社會契約論的思潮之下，人民將主權交付給國家並換取安全、保護以及福利。而國家為了提供福利給人民，必須要了解市民之中誰需要福利的給付，以及這些人所在的位置。這個對市民資訊的需求，發展

[57] 《国务院关于印发社会信用体系建设规划纲要（2014—2020 年）的通知国发〔2014〕21 号》。

doi:10.6342/NTU201900452

成一種監視的型態，並且開始收集大量市民的資訊[58]用以落實社會福利的提供。此種類型的監視，除了福利政策的需求之外，同時也是官僚組織對於其所經手資訊收集渴求的一環。

澳洲政府在其社會福利政策中，採取了 BasicsCard[59](下稱基本卡)此一結合科技與監視的措施。基本卡裡面儲值的金額，僅能用來購買「生活必需品」，例如食物、衣服、健康管理用品，而無法拿來購買嗜好品、菸酒、遊戲點數、賭博、成人媒體甚至釀酒用具。基本卡裡面的金額無法換成現金，購物的找零也會回到卡片中，且僅能在特定店家使用。基本卡是澳洲政府收入管理政策的一環(Income Management)，處在收入管理狀態下的福利受領人所受領的社會福利津貼會直接入帳到基本卡之中，而不是領取現金後自由花用。澳洲政府以此方法避免受領人的家庭收入與社會福利給付被用以購買前述的「不良商品」。同時能使用基本卡的商店受到限制，每張基本卡所購買的商品、時間、地點，也會被基本卡系統記錄下來。此一政策所宣稱的目標，是減少接受福利受領者對福利的依賴，培養對自我理財行為的責任感，並最終使其投入勞動市場。其背後的思想，一般稱作家父長主義。其內涵係指在特定情況下，國家為了當事人的利益，而干涉、介入當事人的選擇自由。澳洲政府認為接受補助的族群，其可能缺乏對於家庭收入的分配能力，因此透過收入管理的方式來介入這些族群使用其收入的自由。較為弔詭的是，剝奪福利對象自我決定如何消費的能力之後，是否能夠培養出能夠進行理財行為的責任感容有疑問。

另一個面向則是社會安全層面中政府針對高風險人口的控制。對於這些高風險人口的區分方式，**同樣維持監視技術中資料收集、分類、定性此一路徑，將特定人口劃分出來並給予不同待遇。**其可大略分成兩種類型，其一為針對有前科者所進行的治安人口訪查，其二則是社會安全網指導原則下針對適應社會功能失常的族群所進行的分類。如我國治安顧慮人口查訪辦法第二條之規定，即以曾犯重大犯罪者作為警方列管並查訪之對象[60]。社會安全網考量的例子則有新北市針對兒童及青少年保護所設定的高風險家庭預防方案可供參考。其所設定的六大風險因子如下，1.貧困、單親、隔代教養。2.家人死亡、出走、重

[58] Toni Weller (2012). The information state：An historical perspective on surveillance. In Kirstie Ball, Kevin D. Haggerty and David Lyon (Eds.). *Routledge Handbook of Surveillance Studies* (p.59).

[59] 以下有關 BasicsCard 之內容整理自澳洲政府之說明網頁，Australian Government Department of Human Services, BasicsCard.
取自：https://www.humanservices.gov.au/individuals/services/centrelink/basicscard，最終瀏覽日期 2019.01.11。

[60] 法源為警察職權行使法第 15 條。實務上執行之具體情況受限於本文之研究範圍，並不打算於此處理。

doi:10.6342/NTU201900452

病、入獄。3.負擔家計者失業。4.家人有自殺風險。5.家人有精神疾病、藥癮、酒癮。6.家庭紊亂、衝突。作為社會安全網的一環，之所以區分出高風險家庭此一分類，其目標是盡早從改善家庭環境開始，避免兒童及青少年長期未得到妥善的照顧或者受到家庭暴力[61]。其確認這些家庭中風險因素存在的方法，則是透過大數據整合民政、教育、勞工、警察、衛生、消防、原民、工務、司法等單位的通報，整合製作出風險家庭熱點圖，並且將這些因素做為社工參訪時評估兒童家庭狀況的一環。在此，監視技術呈現出「數據化」與「流通性」的性質。經過評估的資訊可以轉化為數據儲存在資訊設備之中，並且迅速的在不同機關之間流通。這一點代表行政效率的提高，以及對於數據的依賴加強，並且與本文後續章節提及的官僚組織問題有所關聯。

在這些政策之中，監視技術的意象轉變為福利國家對於國民的關懷。如同前述監視的歷史章節部分所提及，更恰當的稅收以及更精確的福利政策皆仰賴於對於國民的關注以及監視，以達成福利國家的目標。此時的監視技術毋寧說是作為一種較為柔軟的狀態而被使用。

第三節 小結

既然隱私權本非絕對受保障之基本權[62]，國家對隱私權加以限制亦屬合理之事，惟須符合憲法第 23 條之要求「除為防止妨礙他人自由、避免緊急危難、維持社會秩序，或增進公共利益所必要者外，不得以法律限制之。」後方能進行。於此產生疑問的是，國家所進行的監視行為通常皆能夠找到維持社會秩序或增進公共利益的理由作為支撐，因此大部分監視行為皆能找到一定之正當性存在。惟需要注意的是，存在於這些政策之中層疊的監視手法互相結合的可能性與危險性。目前散見於各個不同組織之間的監視系統雖然各自運作並受到法律等機制的管理，但僅須透過網路與程式的輔助，在技術上要進行全面的整合其實並非不可能，存在的問題僅有成本效益問題以及法律管制問題而已。如同本文研究動機中所提到的日本內閣施政願景，若政府有意將監視系統的擴大作為未來方向，則勢必必須要注意到潛藏於監視機制之中的問題。同時官僚組織與社群、消費、安全等方向的應用，使得個人資訊之價值越來越高漲，亦成為監視技術實際運作時需要考慮的利益衡量重要因素。

---

[61] 以這些目標來看，其目標設定亦有與犯罪預防之結構路徑相符合之部分，亦即藉由針對結構性因素(貧窮、教育、家庭問題)及早處理，避免個體在未來犯罪。

[62] 事實上在尚未廢除死刑的我國來說，本無絕對受保障之基本權存在。在此前提之下，運用法律對於隱私權進行保障或是限制時所進行的利益衡量即成為重點。另由於隱私權之保障與人格發展自由之保障有深刻之關聯，因此亦經常被用以作為保障隱私對抗監視之論述方法。

doi:10.6342/NTU201900452

第三章 監視理論與技術的演變

第一節 監視理論概說

第一項 早期社會學觀點

監視社會的形成之所以會成為值得分析的問題，是因為監視能夠與各個領域結合的多面向性，以及其牽涉到的權力作用、對隱私權可大可小的影響。但也因為其可能涉及的範圍太過廣泛，因此本文將先從已經長久累積理論基礎，且論及監視問題的幾個社會學領域來切入，先為早期社會學觀點下的監視理論提供一個概觀的認識。而這幾個領域共通的特徵，是重視對於領域成員的管理、並且將監視作為便利管理的手段。

對於監獄之中囚犯的管理，經常必須透過監視來進行。Bentham 於 1785 年提出圓形監獄(Panopticon)概念，試圖提供監獄管理的改進方案。而此一概念也為監視社會的分析提供了重要的理論素材。在圓形監獄之中，獄卒位在監獄的中心，而囚室則以圓形方式排列。獄卒所在的位置經過特殊設計，由囚犯的位置看過去會因為逆光而無法看清楚是否有人正在監視。這時囚犯會時時刻刻懷疑自己正被獄卒監視著，即便囚犯實際上並無法確定監視塔中到底有沒有獄卒存在。透過引發囚犯的心理作用，監獄的管理者就可以以更少的人力來監視更多的囚犯。Bentham 所提出的這個構想，是為了回應十八世紀後半英國所進行的刑事政策改革思潮。但須注意的點是，其論述的焦點集中在管理的機制之上，而不將監視當作對個人的關注[63]。

在勞動管理部分，監視的目光則是作為促使勞工產出勞動成果的工具而運作。如 Zureik 便指出，Karl Marx 等學者將「勞動者的觀察、任務的斷片化、精神上的任務與作業上的任務分離、工作的規格化」等措施認為是使勞動從屬於資本，進而對勞工進行管理的手段[64]。其提及的對勞動者的觀察，便是監視行為的應用。具體來說例如資本方藉由安排監工、對工作場所進行設計等手段，來確保勞工確實產出勞動成果。例如使工廠作業員的座位的方向一致、工作臺不設遮蔽物保持視野開闊，以方便監工透過視線確認是否有消極怠工的情

[63] David Lyon，前揭註 1，頁 91。

[64] David Lyon，前揭註 1，頁 51-55。

doi:10.6342/NTU201900452

況。或是辦公室中，將主管的座位安排在可以看到每個人電腦螢幕的位置[65]。這些「視線」的安排，就是工作場所中以監視方式進行的管理手段之一。從 Marx 等學者的觀點延伸，資本與勞動的關係之中這種由資本方所進行的監視，被詮釋為對於勞工的不信任[66]，這些視線的存在則體現了資本對勞動力的控制。

Dandeker[67]則指出，軍事力的發展也助長了監視的浪潮。其認為，戰爭行為以及軍隊的發達，這兩個目的幫助監視行為成為構築國民國家的中心之一。近代國家將權力領域與市民分離開來，在此同時也不得不監視市民。監視隨著對外部的敵人以及市民社會內部的敵人的情報收集逐漸成長。Weber 將軍事與官僚的紀錄保存加以連結，由於戰爭是此類國家為了存續所必須進行的行動，軍事組織首先被官僚化以加強效率，而在收集士兵與市民資訊、對他國情報進行間諜行動時，監視便作為成果被展現出來[68]。

從這幾個例子來看，以社會學途徑所進行的涉及監視行為的論述，最初並不是有意圖的發展監視理論，而是在對其他領域進行分析的同時，間接的論述到監視相關的問題，並且將監視視線的創造與結構安排做為觀察其他領域時一個重要的素材。本文認為，原因與後段所提及的「視線」問題有所關連。在這些理論提出的時代背景下，「視線」所能抵達的距離有其極限。而這些「視線」在覆蓋到被監視的個體的同時，明顯具備背後權力行使者的影子。這一點也體現出另一個重要的特徵，即是監視視線的存在與管理緊密的結合，通常皆是由國家、官僚系統、資本家等等具備一定支配能力的組織、群體所發起。

第二項 近代

另一個重要的想法，則是「視線」的重要性。由於近代所創造的「陌生人的社會」，長期以來以個人關係為主流的社會中，所預設的社群之間之信賴關係

---

[65] 隨著科技發展，應用上也出現更多可能性，例如監測鍵盤按鍵的次數、以 RFID 方式進行打卡管理、以影像分析技術分辨員工是否有偷懶等等。此為以空間與結構之安排進行監視視線創造之類型。

[66] 例如商店中裝設的監視器，除了朝向陳列商品的貨架之外，通常也會朝向收銀台。當然這種面對收銀台的監視器，並不單純只是監視員工，通常也兼具有防範竊盜的目的。

[67] Christopher Dandeker (2006). Surveillance and Military Transformation. In Kevin D. Haggerty, & Richard V. Ericson (Eds.). *The New Politics of Surveillance and Visibility* (p.239).

[68] David Lyon，前揭註 1，頁 77。

doi:10.6342/NTU201900452

被陌生人所取代，為監視社會的繁殖提供了理想的條件[69]。此處的個人關係，是指生活在群體(家族、封建體制、村落)中，而認識周圍的鄰居、能夠親身與他人建立溝通的社會中，個體所發展出來的人際關係與信賴。事實上是依循於社群的緊密連結而產生的人際關係。因為個體的視線不再能夠抵達生活在周圍的陌生人，未知與未見等同於不安，為了要能夠看見這些陌生人，或者說對這些脫離了視線的個體進行關注與監視以抹消這些不安，超出個體之外的視線便逐漸有了發展的條件。亦即，**近代的社群關係消融並且重鑄在都市與虛擬空間之中，對於充斥在生活環境之中卻又不再具備社群關係的他者，若能將這些他者放置在視線之下，或許能有效撫平此一轉變帶來的不安感。**

第一款　Foucault 與「Big Brother」

Foucault 對於 Bentham 提出的圓形監獄(Panopticon)概念，以如下的觀點加以闡釋：「圓形監獄」的主要效果來自於此：在囚犯身上招來保證權力自動運作的可視性之意識與永久狀態。使權力的運作達到永久，即便它在其行動中是不連續的；〔……〕致使囚犯被捕捉於一種他自己就是權力情境乘載者的權力情境之中[70]。藉著此一譬喻性的結構，Foucault 發展出全景敞視主義(Panopticism)。其認為圓形監獄運作的基礎，是將囚犯置於「無法確定是否有人在看著自己」的狀態中，在這個「被看見」的恐懼之下，囚犯將會遵循監獄裡面的規則。透過囚犯自身的認知對自身產生的作用，獄卒以及管理者對囚犯的權力不再需要透過身體的接觸來進行。囚犯會隨時認知到自己可能正被獄卒看著，而這個認知是存在於囚犯的心中，即便看守塔中沒有獄卒，仍然會持續作用。囚犯在這樣的構造之中，被恆常的可視化，同時也被構造本身促使其認識到自己處在可視狀態之下，囚犯將會認為在這個空間之中所有的一切都能夠被看見。即便監視者未必真的存在於中央的高塔，囚犯仍會自行預設來自獄卒的「凝視」(gaze)存在，最終囚犯將會使自己成為載體而乘載整個權力結構，並且持續被這個結構所規訓(discipline)。正如 Foucault 所說：一種虛構的關係自動地產生出一種真實的征服。Deleuze 則針對全景敞視主義這樣總結[71]:藉由視覺布置與光線環境，監視者可以一覽無遺卻不虞被看到，而囚犯本身則無時無刻不被凝視卻又甚麼都看不到。

---

[69] David Lyon，前揭註 1，頁 78-79。

[70] Michel Foucault (1995), *Discipline & Punish: The Birth of the Prison* (Alan Sheridan, Trans.) (pp. 199-201.) (Original work published 1975)，標楷體部分內容為筆者節譯。

[71] Gilles Deleuze (著) (2000)，楊凱麟(譯)，《德勒茲論傅柯》，頁 91，麥田。(原著出版年:1986 年)

doi:10.6342/NTU201900452

這種未使用暴力手段，而僅以結構與可視性的安排便能實現的權力運作方式，正是全景敞視主義帶來的重要理論素材。而其中值得注意的特點，是權力表現形式的轉換。在其全景敞視主義的設定之下，權力以及統治更傾向使用「可視性」以及「結構」作為載體運行，而不再使用身體、外表、光線、凝視等等方式表現[72]。這一個結構的圖像並不僅限於監獄，似乎有著能夠存在於任何具備權力秩序場域的可能性，Foucault 這樣說道：「全景敞視是權力秩序中一種科技上的發明，猶如蒸汽之於蒸汽機一般。此發明已運用在許多地方性區域，例如學校，兵營，和醫院。」舉例來說，只要學生認知到自己的活動與行為可能受到監控，其便會依照此一前提行動，則學校想要達到的規訓目的(依循學校的規則、成為應該成為的人)便已達成。Foucault 認為圓形監獄中的權力此時已經不再屬於獄卒，而是被覆蓋進這個自動運作的、匿名的結構之中。對於囚犯靈魂的訓練，便可以由這個結構持續的進行，從而達成規訓的目標。而這個結構不管由誰來操作，都不影響其功能，結構本身便能夠自動的運作。最重要的是，透過這個結構，權力運作和規訓目標的達成變得更加輕便、迅速、簡單。Deleuze 進一步說明，全景敞視主義並不僅只是建築與光學之系統，同時也能被看作是一種機器。其被普遍運用在可視材料(如工作坊、軍營、學校、醫院與監獄)，且普遍貫穿所有可述功能。全景敞視理論的抽象公式因而不再是「看而不被看」，而是在任意一個人類多樣性中強加任意一種教化(conduite)[73]。亦即，視線/光線的設計其實彰顯的是隱藏在背後的以身體為目標之權力作用。

Rose 如此概括 Foucault 對於圓形監獄的觀點：「將人個別化、規格化，基於永續的監視而進行的將人等級化的政治技術圖式。使得具備多樣性的政治機構變為可能、進行某一種不會被妨害的持續性判斷，在減少人類身體所具有的抵抗力道的同時，使得身體的經濟上、社會上便利性最大化。[74]」亦即，透過能夠使超越的視線順暢地、快速地運作的結構，讓具備多樣性的政治機構得以實現。並透過構造的安排，使個體將這樣的權力內化到自我之中，以柔順而非暴力的方式讓身體發揮經濟層面的、社會層面的價值。Foucault 所提出的這個模型雖然是針對結構而提出，但必須要注意的是其影響的主要面向仍然是「個體對於視線的認知」。假設將一個睡夢中的囚犯放入圓形監獄結構之中，在囚犯醒來之前其並未認知到自己周圍環繞的目光存在，此時圓形監獄的規訓作用對於這位囚犯來說並不存在。直到囚犯認知到自己處在監視之下的事實這一個時

[72] 可視性與光線、凝視的差異在於，可視性的結構創造的是可能性，而未必會有實際的凝視產生。也就是說，光線不一定要直接打在目標身上，而只需要目標知悉其處在光線隨時可能照映於其身體的狀態，即可創造出可視性。此時被加諸了可視性的目標是處在「可能會被看見」的狀態。

[73] Gilles Deleuze，前揭註 71，頁 92-93。

[74] Nikolas Rose (1999), *Powers of Freedom: Reframing Political Thought*, p.187.

doi:10.6342/NTU201900452

點，這一個構造才真正開始對這個囚犯產生作用。另一方面 Lyon 指出，從圓形監獄中將囚犯等級化區分，並且將囚犯的身體分配在不同牢房的制度看來，圓形監獄之中也同時存在著生權力的運作[75]。因此圓形監獄同時可以作為規訓與生權力運作的理論模型。從 Rose 的概括之中，可以得知政治機構在資本主義社會之中的目的，是以最高的效率，發揮每一個身體最大的經濟價值。同時這樣的機構與生權力密不可分，並且透過收集人口資料、劃分等級並將身體以及身體上糾纏的資訊加以分類的手法加以實現。

尚存有疑義的則是虛擬場域以及存在於虛擬場域中用以指涉現實存在的身體之資訊(即虛擬人格/資料疊加 Data Double[76])此一虛擬身體的運作與圓形監獄模型的關係。在現實空間中，圓形監獄模型試圖加諸教化於身體，同時對於身體能夠直接運作生權力(透過結構安排、建築設計、系統、社會防護機制)。但在虛擬空間中，對於虛擬的身體/資訊如何加諸權力，則是圓型監獄模型無法直接掏用的場域。

另一個帶有譬喻性質的模型，出現在 Orwell 所創作的小說《一九八四》之中。在《一九八四》的世界裡，生活在大洋國(Oceania)的人民一切的言論與行動都被大洋國政府藉由電幕(telescreen)、鼓勵告密、安插線民等等種監視手法監控，並且必須服從於「Big Brother」這個絕對的領導人。書中的政府所施行的統治，在全面進行監視這點來說，是圓形監獄結構的極限擴張，從特定的建築結構擴展到整個社會。另外在書中的世界，「Big Brother」不只針對人民的行動，連言論以及思想也都納入監控的範圍。《一九八四》之所以會是重要的理論素材，是因為其直觀的提供了一個「監視」與「極權社會」的連結。監視技術被連結到「維持階級控制」此一目標[77]。在其所描繪的圖式之中，當政府可以對人民的所有行動一覽無遺的時候，極權統治的施行以及思想的控制能夠順暢的執行，而國家進行的「監視」也自然的與統治權力產生強固的連結。

但這兩者的監視意象，仍有些微的差異。Foucault 在發展全景敞視主義時所注重的是，讓對象在意識到來自看守者與結構的視線時，同時將規訓內化到己身之中。亦即最終追求的，是使囚犯自發的改變自身。但《一九八四》的大

[75] David Lyon，前揭註 1，頁 91。生權力是指透過人口統計、區分等方式，以生命為標的而運作的權力。與監視技術交錯的運作，主要體現在對人口進行辨識、分類與差別待遇方面。

[76] Data Double 乃指人在虛擬空間的數位複製體，這個複製體來源於我們的生活中被轉化為資訊的資料，並且能夠在作為監視聚合體的資訊系統之中迅速傳播、再製、利用。詳情可參閱 Kevin D. Haggerty and Richard V. Ericson，前揭註 11，pp.605–622。本文將於後續資訊聚合體章節處理相關問題。

[77] Kevin D. Haggerty and Richard V. Ericson，前揭註 11，p.615。

doi:10.6342/NTU201900452

洋國所描寫的監視社會看來，對 Orwell 來說，監視手法與獨裁統治綁定在一起，同時是對社會進行階級控制的手段，以及對思想進行洗腦的手段。Orwell 的目標應是將監視社會作為一種寓言式的結構來對逐漸深化的監視社會發展提出警告。當然，這樣的警告在現代社會中仍有其意義，卻也產生了一些質變。原因在於，監視技術的發展逐漸添加了許多似乎對人民有利的目標，例如對於犯罪的控制、對於社會和諧的促進、對於恐怖份子的防範等等。如果能夠以全面的監視換來全面的安全，似乎對於人民來說也並非不能接受。在民主憲政主義的保護之下，對於監視的恐懼從「對獨裁的恐懼」變質為對「基本權限制的恐懼」，而主要用以抗制監視意象的基本權主要為隱私權與人格發展自由，此二者皆非受絕對保障之基本權，在經過此一質變之後，對於監視的反抗力道似乎變得較為柔軟。

全景敞視主義與《一九八四》兩者背後共同的脈絡，是將監視與統治權力的分析互相連結，而監視與「可視性」的創造被當作權力運作的手段之一，其所採取的路徑建立了對於監視分析的基本模型，使得監視理論的骨架變得較為清晰。但由於時代因素，Foucault 所發展的全景敞視主義未能將資訊技術以及電腦帶來的影響納入考量。而《一九八四》雖然已經有了超越距離的電幕出現，但其同樣未能處理到電腦與網路的影響。主要的差別在於，在《一九八四》的意象中電幕(當然此一電幕意象已然具有部分現代網路的特徵，例如散布性、即時性、雙向/有限的單向通訊性質等。)嚴格控制在統治者手中，現代社會中的網路卻非統治者所能嚴格掌握，而是如同本文前述，須藉由較為間接的方式試圖爭奪此一虛擬場域的控制權。也因此在現代資訊社會之中對於網路場域的控制力道並不如《一九八四》所描寫的意象一般嚴格。且事實上本文所討論的資訊社會極大程度的仰賴網際網路之連接，對於網路設備尚未普及的國家來說，監視社會尚不會成為嚴重的問題。

另一個問題是，此處的權力運作結構無法完全說明國家以外主體所進行的監視行為。此外，資訊社會之中監視行為的目的漸趨多元，其背後的動機已經難以僅僅使用「資產階級的維持」、或是「規訓的要求[78]」來說明。論者亦指出[79]，不論是監獄的結構，還是小說中所描繪的監視社會，其實都忽略了現今的

[78] 但此一目標仍然是犯罪預防問題中，使用監視技術的重要理由之一。其類比的大致狀況是認為空間中設置的監視視線可以使潛在的犯罪者改變對於犯罪的決定。需要注意的是，在犯罪預防問題中，嚇阻潛在犯罪人的犯罪固然是重要的目標，但能否依賴監視技術達成其實容有疑問，且一般日常生活中所設置的監視器其設置方式與圓形監獄此一圓型的概念仍然有所不同，一般的單一監視器並不具備圓形監獄中全視的視角，且圓形監獄中囚犯無法接觸到看守塔，但日常生活中設置的監視器則並非不可迴避或破壞。

[79] 張煜麟，前揭註 23，頁 205。

doi:10.6342/NTU201900452

主流國家皆已經轉變成法治社會，而這兩者的圖像之中皆沒有現代意義下以自由主義與人權保護為前提的法律存在。

舉例來說，構成民主法治社會基本的法律保留原則與基本權的保障等等問題與監視技術之應用交錯之後如何處理，即是 Foucault 發展的圓形監獄模型與《一九八四》所帶來的意象中較無法直接類比的問題。因此，直接將現代社會以類似圓形監獄的圖像來加以類比的話，必然在部分領域會失之精確。以全景敞視主義來說，從「監視行為/監視行為的可能性→可視性/可視性意識的創造→結構的建立/內化→權力運作/教化」這一連串路徑，可以用以說明許多以管理為目的之特定設施(例如學校、醫院、軍營、監獄)的運作。但對整體社會來說，將之比喻為一個巨大的圓形監獄則並不合適。對於現今監視社會之狀況更精確的描述是，監視社會由無數個大小型態各異的圓形監獄、看守塔、守衛所組成。看守塔的守衛可以是未必存在的狀態、單數、複數甚至互相連結，被監視的目標亦可以是單數、複數甚至互相連結。甚至圓形監獄意象中原本僅能被監視並恐懼著目光的囚犯，其實在資訊科技的支持之下也能夠扮演守衛的角色監視他人(例如行車紀錄器的運用、對警察進行的反蒐證等等情況)，亦即視線關係的反轉。而現代法律規範與監視技術的關係，也無法單純以這些概念類比，因為以法律做為基礎的監視行為基本上除了賦予監視行為合法性之外，亦同時會在基本權保護的面向上對監視行為進行限制。而以契約為基礎的監視行為通常與消費領域連結，較為無法直接與圓形監獄中「維持階級」或者「規訓」的考量相類比。另一個問題是民主憲政中的法律究竟扮演何種地位。例如圓形監獄與看守塔的形成，如果依循於基本權保障及法律保留原則的控制之下，是否便能打破 Foucault 與《一九八四》的監視意象，或者僅只是統治權力的轉變，皆尚有未明之處。

第二款 近代的類型區分

以前述的圖像作為出發點，接著觀察監視技術的發展的話，可以發現幾種不同型態的監視技術運作。Lyon 將這些技術按照時代的演進順序與特徵，區分為三種類型[80]。需要注意的是，這樣的區分僅是作為協助理論論述的手段，而一個監視行為之中極有可能混用複數的手法同時進行。例如以承包客服業務的公司來說，負責接聽客服電話的員工其背後可能有上司在監視著員工的工作，而電話通話的位置、時間長短則是由客服中心的主機以電子方式隨時記錄儲存。也因此雖然資訊社會發展出新的形態，但傳統的監視行為並未消失，而是持續的演進與改變，以複雜多樣化的狀態存在。以下就其分類說明：

[80] 以下三種分類整理自 David Lyon，前揭註 1，頁 119-130。

doi:10.6342/NTU201900452

1.面對面(Face to face)之監視

即傳統的、伴隨人類歷史之由人為主體藉由肉眼所進行之監視。此種監視手法直接依賴人類的身體與感官而進行，其最大的特徵，是空間上的近距離、以及時間上的現在性。例如監工在工作現場監視工人是否確實進行工作、哨戒塔以及警衛之設置等等。而實際上此種類型也是最早存在人類社會之中的監視型態，古代進行此種監視的方式，除了以間諜、跟蹤方式進行之外，還有竊聽、甚至聽取告解等等手法。透過監視所獲得的資訊，通常以書面資料加以留存。值得注意的是針對個人資訊的詳細記錄，已經出現在監視的脈絡之中。以十四世紀歐洲盛行的異端審問進行來說，生活在當時封建社會共同體之中的村民，為了不讓有可能是教會眼線的鄰居告密，在生活中會對話語內容以及說話的對象小心翼翼。而當時留下的異端審問書[81]也成為紀錄共同體生活的重要史料。此種類型的監視手法，其施行仰賴人力，且單一人力能同時監視的目標與範圍皆受到人類活動範圍的物理性限制。對於資料的紀錄與儲存也仰賴較為原始的儲存媒介例如紙張，因此雖然在各種場域持續進行，但其規模仍受到限制。事實上此一藉由感官進行的對他人之關注，亦是人類社會基本的存在型態之一。因此在監視理論之中，通常將之當作是基礎架構的一環，較不會針對此一手法本身加以討論。

2.檔案(File)之監視

進入近代之後，進行監視的手法，則加入了會計學、統計學的手法，並且以大量檔案的累積作為基礎。其進行的方式，基本上是蒐集資料之後，將資料以**命名、識別、計算數量、等級化、保存檔案**等等方式加以處理。也就是說，所獲得之資料已經逐漸開始在特定的目的之下進行重組或是保存。舉例而言，社會福利例如低收入戶的補助，便會依照此一流程進行[82]。基於檔案而進行的

[81] David Lyon，前揭註 1，頁 123。在歷史演進到具有足夠便利的紀錄工具之後，監視技術與個人資料記錄的連結便逐漸開始發展。

[82] 就具體實踐來說，首先必須先定義何為低收入戶，創設出足以精確數據化的標準，例如收入在多少以下、家庭成員數、年齡、有工作能力者數、是否領有身心障礙手冊、身心障礙程度如何等等要素之後，再來從人口檔案之中識別出符合該定義之群體，之後進一步計算低收入戶的數量，將其區分類別之後保留下檔案。檔案化的好處是方便在官僚組織之中傳遞、儲存、使用。且整合過後的個人檔案不只在社會福利建構上通用，同時也能與戶籍機關、兵役機關、司法機關互相流通使用。例如新北市家暴防治中心其政令宣導即提及，其對家暴高風險家庭之評估流程中，會廣泛收集不同機關之資料進行整合，並製作出一目瞭然之表格來評估該家庭青少年受到家暴的風險高低。主要的評估要素則有家庭組成狀況、收入狀況、家庭成員前科紀錄、學校對青少年之紀錄資料等。

doi:10.6342/NTU201900452

監視，與近代官僚制度的發展有深刻的關聯，甚至可說官僚制度仰賴檔案與資訊的累積而運作。**此種監視類型透過檔案的累積對現在與過去兩個方向進行分析，同時具備國家性，並且具有獎勵同質性的傾向。**具備國家性的原因在於近代國家興起之後，現代科技進入資訊時代之前的時期，有能力大規模統計資料的團體通常有政府的支持，甚至便是政府本身在執行資料收集之工作因而通常具備國家性。同質性則來自於資料蒐集之後所進行的分類過程。個體在分類過程之中會被依照特定的屬性歸檔到特定群體，並由於此一分類帶來的區別待遇而傾向融入群體之中並且共享同樣的特質。舉例來說，白領與藍領階級的劃分，所適用的保險類型、勞動法規不同。需要注意的是，此一同質化的傾向未必便會對被分類的個體帶來壞處，且在牽涉到國家福利制度時，個體也可能透過此一同質化的過程更加適應社會生活，因此在這些層面上來說監視行為是否有害，仍須就各該差別待遇本身進行判斷。實際上較有危險性的部分會在分類機制的不透明以及檔案累積的加劇傾向。

3.介面(Interface)之監視

此種型態的監視技術以電腦設備作為運作的媒介，擷取人類在行動學、生態學上的特徵作為基礎資訊，並且指向未來、連接了微觀(身體)到巨觀(地球)[83]，而具有排他的傾向。在這個新的監視手法中，藉由技術的進步，監視的目光超越了距離、晦暗不明、物理的障壁，檔案的蓄積、篩選、分析、結合、傳遞超越了時間。資訊本身已經具備了轉變成**指向未來的預測之可能性**。舉例來說，電子支付、GPS 與手機定位技術、DNA 分析、生物識別技術、無線射頻(RFID)、網路軌跡追蹤等等科技普及在社會之中，在這些科技與網路、資料庫等技術互相整合的現況下，除了對資訊本身(消費履歷、身體位置、個人身分的確認)的收集之外，種種資訊尚能夠與風險評價結合，製作出「高風險清單」而轉化成對未來的預測[84]。Lyon 認為，**在這個監視技法之下，監視所得的資訊會經過特定的介面處理之後轉化成易於使用、傳遞的數字型態，資訊的收集、儲存、散播的速度，皆得到極大程度的擴展。**在資訊隱私權相關的論述之中，經常被論者指出的「藉由監視所達成之人格測繪」問題，也與此種透過介面所進行的監視技術有深度關聯。與個體連結的現實－數據資訊介面越多，能夠蒐集的資訊也就越多，進一步使得人格測繪有更多的素材得以進行。例如整合前述的相關技術，從存款、交通工具使用、手機位置分析、通聯記錄獲取、網頁瀏覽紀錄、社群軟體使用情況、監視鏡頭中的人行動軌跡等等方向著手，若政府機關試圖要將特定個體的生活歷程完整呈現，在技術以及足夠的監視設備支持

[83] 意指從被監視之身體本身以及身體所在環境周遭之特徵出發，擷取資訊片段並加以整合。

[84] 例如從信用卡刷卡履歷中分析是否有為恐怖份子提供接應、從出入境紀錄檢查是否涉及跨國犯罪等等。

doi:10.6342/NTU201900452

之下並不困難，且在我國現行法源授權上並非不可能達成[85]。而其與針對過去所進行的監視(單純檔案累積)最大的差別，是資訊收集範圍與數量的極大擴張，以及資訊與資訊之間越來越容易的的連結、結合、創造可能性。另外針對此一「資料流動介面」的創設與編碼，亦與本文後續章節會處理的規訓社會轉向控制社會問題有所關聯。簡言之，檔案與監視手法數位化的情況下，掌握這些轉換介面者以及有權對轉換介面進行編碼者，將有能力對這些資訊的流動進行更深刻的控制。

Staples 將此種透過介面進行的監視看作是「後現代」監視的一種例子。其認為此種監視的特徵，是被**斷片化的、非確實的、時間與空間受到壓縮，並且具備大量消費性質**[86]。而這樣的監視，又具備兩個特點。首先是其以演算法的複合體作為基礎存在於日常生活之中。Staples 將之稱為「權力的細微儀式」，這個儀式將人們整隊、詳細的點名、並且精查逸脫行為，意圖在施加懲罰或者是差別待遇。這個儀式的重點在於大量收集資訊之後，重新分解資訊並且加以組合，按照一定的演算法得出結論，並且區分正常者以及逸脫者/偏差者(例如恐怖份子、犯罪嫌疑人、信用不佳者等等)。Lyon 則指出，這種後現代類型的監視在 911 事件之後，伴隨著國民 ID 卡計畫、人臉辨識、指紋資訊的保存等等一連串用於國境管理的技術顯著的成長。後現代監視的第二個特徵，則是其具備的**先制攻擊特性**[87]，試圖在狀況發生之前進行預測或處理。Lyon 指出，監視從原本對固定位置的「包圍」轉向流動式的追蹤與收集資訊。Dandeker 對此進

[85] 人格測繪之過程中固不乏需經過法官簽發令狀才能取得的資訊，但也有許多資訊僅須透過警察職權行使法第 10 條:「警察對於經常發生或經合理判斷可能發生犯罪案件之公共場所或公眾得出入之場所，為維護治安之必要時，得協調相關機關（構）裝設監視器，或以現有之攝影或其他科技工具蒐集資料。」、第 11 條:「警察對於下列情形之一者，為防止犯罪，認有必要，得經由警察局長書面同意後，於一定期間內，對其無隱私或秘密合理期待之行為或生活情形，以目視或科技工具，進行觀察及動態掌握等資料蒐集活動」、第 12 條:「警察為防止危害或犯罪，認對公共安全、公共秩序或個人生命、身體、自由、名譽或財產，將有危害行為，或有觸犯刑事法律之虞者，得遴選第三人秘密蒐集其相關資料。」等法條之運作，便能輕鬆取得法律之授權。事實上若將警察職權行使法如此廣泛之法律授權概括適用到不同的監視技術之中，有可能帶來許多疑慮。因為採取不同監視手法、收集資料的多寡對於隱私權所造成的侵害狀況各不相同，法條中所需要權衡之利益例如合理隱私期待、公共安全秩序等等標準，在操作上皆有模糊之空間。

[86] David Lyon，前揭註 1，頁 142。

[87] David Lyon，前揭註 1，頁 143。

doi:10.6342/NTU201900452

一步說明[88]：「監視作用的地點變得不再明確，在空間方面透過網路技術涵蓋了所有可能連接的資料，在時間方面則是從面對過去的資料收集轉向成面對未來的危險預測。」簡單來說，「監視視線」脫離了實質視線的創設，轉而以「對資料進行的穿透」此一型式出現。在監視技術逐漸推離對於視線創設的依賴之後，若要取得一個個體的人格檔案，在數據化與技術支持之下已經不需要對其生活歷程設置監視鏡頭，只需要收集其與各個介面連接之後留下的軌跡[89]，並且將這些資料組合成對應到個體的「資訊人格」即可。此一資訊人格檔案在許多方面能夠有所應用，而資訊的收集程度端看掌握系統者如何決定，甚至可以交由系統在演算法下自行運算決定收集資料之多寡。

Haggerty 和 Ericson 則指出[90]，此種新型態的監視帶來了更多錯誤發生的可能性，同時產生了更多經過精心設計卻仍然可能帶來災難的錯誤系統。其主要批評的點，在於「危險預測」的正確性疑慮，以及演算法濫用的風險。其以收集顧客的消費紀錄以及病歷記錄數據後，進行了錯誤預測的案例來加以舉例。其認為這種系統潛在的問題在於演算法設計的方式。通常這種依賴演算法進行的監視系統其前提設定為，特定的數據情況出現之後，便依照特定的公式來進行類型化。也因此，**一旦預設的條件達成之後，不管實際上被監視者的情況如何，其在系統之中都會被自動被分類化並且標籤化。但這些個人資訊實際上經過數據化的重組，得出來的個人形象[91]已經未必與現實中的個體相同。**此時可能產生的風險，是來自於演算法的設計本身。這些為了能夠被演算法所計算，

[88] Christopher Dandeker (2007). Surveillance: basic concepts and dimensions. In Sean P. Hier & Joshua Greenberg (Eds.). *The Surveillance Studies Reader* (p.40).

[89] 例如與銀行的交易紀錄、電子支付的履歷、日常生活帳單的資訊、大眾交通工具的搭乘與使用、智慧型手機的 gps 定位資訊、社群媒體的打卡、時間軸、動態消息等等。這些軌跡能夠被用以與其他資料一同拼湊，並且達成不同的目標例如信用判斷、危險性判斷等。

[90] Kevin D. Haggerty & Richard V. Ericson (2006). The New Politics of Surveillance and Visibility. In Kevin D. Haggerty, & Richard V. Ericson (Eds.). *The New Politics of Surveillance and Visibility* (pp.16-18).

[91] 可能被用來與個體連結的資訊如下：個人身分、公開分享的個人身分、地理/位置資訊、世俗資訊(例如籍貫、職業等等)、社交圈與人際關係、生理資訊、行為慣性的資訊、信仰、態度、情緒資訊、媒體偏好等等。但事實上這些資訊有可能會隨著個體生活 style 的改變而有所變動，資料庫未必能即時更新，甚至也未必能真正完整將個體所有的特徵均收集起來而建立出人格檔案。**在特徵未必即時反應、未必完全的被收集、數據化的條件下，資訊人格與現實中的個體之間必然存在著一定程度的斷裂。**當然，如果此一斷裂完全被彌補，且資訊人格亦已然能夠完全等同於現實中的個體，則本論文所進行的研究應該也無必要了。因為此時的社會進程大概已經進入下一個階段，例如科幻小說中出現的心靈網路、意識共同體、或是乾脆是「Big Brother」以虛擬網路之姿態再現等等，以現今價值觀難以預測的社會演進。

doi:10.6342/NTU201900452

而被加以資訊化的個體訊息，對於**個體來說卻無法知曉其被類型化的理由、過程、結果，而在不知不覺之間便受到差別待遇。**例如在購物網站留下購物履歷之後，顧客便會被網站劃分類型，並且呈現不同的推薦商品頁面。當然購物網站願意呈現怎樣的商品，社群網站願意呈現怎樣的廣告，對於使用這些服務的個體來說似乎不會有明顯而立即的壞處，甚至可能帶來便利。但同樣的技術與原理，在其他領域的應用，便有可能產生問題。值得探討的領域有兩個方面，即監視聚合體問題以及社會分類問題。

第三項 聚合體與社會分類

第一款 監視聚合體

Haggerty 針對監視社會的問題，提出了聚合體(assemblage)概念[92]試圖加以說明。其跳脫前已述及的，為人熟知的 Foucault 與 Orwell 對於監視所描繪的**權力－視線的圖像**，而嘗試使用另一個分析的方向來處理逐漸與電腦、資料庫等資訊科技深刻結合的監視問題。其認為，監視背後存在的動機是渴望(Desire)，對象則是控制、統治、安全、利益以及娛樂。在這些多重目的影響之下，監視範圍大幅度擴展，監視所得資料的儲存與處理能力因資訊科技而提升。監視技術此時可以輕易地與各種科技結合，使得其具有極大的組合彈性。在 Foucault 使用的描述之中，監視問題與圓形監獄(Panopticon)的意象結合，監視的方向是由圍繞的權力者所創設的構造中投向並包圍個體。但在聚合體概念之下，**監視視線未必承載著權力，而僅作為技術手段試圖達成背後的動機(**控制、統治、安全、利益以及娛樂**)。**且其存在的方式也與圓形監獄之模型不同，**並非包圍個體，而是散落在現實空間與虛擬空間之中，**此時資訊的數據化以及目標的達成才是聚合體監視概念下監視技術所重視的目標。

因此，監視實際上是由多種科技與多種制度組合而成的複雜聚合體。由於監視行為可能存在的多目的性，以及其與多重制度(資本主義、統治、犯罪控制、勞動力控制、娛樂需求)接軌的特殊位置，如果以傳統的政治理論來試圖對抗這個複雜的聚合體，在許多方面將會無從下手。Haggerty 指出，監視問題早已不是單純以對官僚主義或政治制度的分析角度切入便能加以說明。又因為其與無數的科技皆有結合的可能性，僅僅以單一科技來作為分析的切入點，在處理問題時可能也不夠全面。舉例來說，經過監視器紀錄的影像，可能透過電腦保存、網路傳播。因此在**分析時必須要考量到這些科技互相交互的影響。而監視技術本身則成為連接不同科技與構造的潛在可能性**[93]。

[92] Kevin D. Haggerty & Richard V. Ericson，前揭註 11，pp.608-614。

[93] Kevin D. Haggerty & Richard V. Ericson，前揭註 11，p.618。

doi:10.6342/NTU201900452

在這一個觀念之下，Haggerty 針對聚合體概念對於被監視主體的影響，提出以下論述。為了要達成有意義的監視，監視系統通常會依照其目的設定其所要篩選的要素。而這些要素，實際上就是監視對象的性質。**在提高效率以及方便資料傳遞的要求之下，監視對象會被打散成許多要素的集合，以方便監視系統擷取需要的要素加以分析。**此時在監視系統的眼中，個體僅僅是打散過後的資訊片段。將這些片段重新組合起來的資訊集合體，便是監視系統眼中的虛擬人格，而被監視的主體將會消融在這個虛擬人格之中。對於監視以及進行監視的人來說，「資訊」以及資訊轉化後的運用才是真正有價值之物，**在資訊背後的主體樣態並不重要。在這些監視系統之中真正被關心的，是轉化之後的資訊。而個體對於這些被分離出來的資訊，則逐漸失去掌控的能力[94]。而對於這些人格資訊的處理與收集，成為以監視技術達成的社會分類(Social sorting)與差別待遇機制所依據的重要基礎。**

第二款 社會分類

Lyon 如此說明社會分類(Social sorting)概念。「社會分類聚焦在由持續不斷的監視所驅動的差別對待。……這些差別對待的目標是為了設計來以影響並且管理人口與個體並藉此直接或間接的影響這些作為檔案客體的選擇與機會。……而被區分的人口與個體則逐漸虛擬化[95]。」在社會分類以及監視的運作過程之中，線上的與線下的資料將有可能被互相對應並且混合，並且整合在能夠被搜尋的資料庫之中。而此種能夠迅速被索引的資料庫成為監視在許多領域運作的核心[96]，同時基於風險管理的要求，更準確的個體識別能力以及更迅速的風險處理能力便是借用此一資料庫所欲達成的目標。在這些要求之下，**監視技術的運行變得更加日常生活化，個體在社會生活中的軌跡有可能會被持續收集**，並且試圖拼湊出蛛絲馬跡。Lyon 認為，對於在資訊社會中生活的個體，犧牲掉部分的隱私並且被納入資料庫之中似乎是無可避免的代價。因此或多或少的接受資訊的收集是無法避免的，但在此同時仍然必須要注意到個體會持續付出哪些代價，而又能從中獲得那些益處作為交換，更重要的是理解監視技術所帶來的危險性與便利性。這一點與下一節所要處理的監視技術之雙面性有關，因為對於個人資料進行的收集，在資訊社會之中並不完全是對個體有害的毒藥，而在某些時候會成為國家對人民進行福利與照護的方式之一。

---

94 Kevin D. Haggerty & Richard V. Ericson，前揭註 11，p.620。

95 David Lyon，前揭註 42，p.14。

96 David Lyon，前揭註 42，p.16。

doi:10.6342/NTU201900452

第二節 監視社會的新進展

第一項 雙面性與資訊國家的圓形監獄

近代監視社會的發展強調「雙面性」，亦即照護與控制(care and control)的同時存在。從民族國家的發展來看，**政府確保執政的社會正當性便來自於社會照護與社會控制這兩個方面。而這兩個領域皆與監視技術相關，可以說是監視技術的一體兩面**[97]。就社會福利領域而言，福利國家導向下的政府必須收集詳盡的資訊，並且根據人民的不同情況給予不同待遇，同時國家獲得的資訊也透過反饋給民眾的過程使民眾瞭解其在社會體系中的位置，並且進而影響個人人格形成的過程。這點可能帶來的疑問，在前述監視的歷史之中已經提及，實例則有澳洲政府所採取的基本卡政策對低收入戶群體之福利津貼分配使用進行監視，或者醫療機關對於病人的病歷進行共享以確保醫療安全等。另一個領域的問題，則是藉由對與個體的辨識以及人格資料的更精確掌握，加強社會控制的實施與達成。不論採取以視線承載權力的方式或者是行政權結合監視技術的手法，其皆象徵著對於人民的限制。**在雙面性特徵之下，監視技術同時具有能夠用以限制人民權利及保護人民權利的能力，**端看其使用在何種系統之中，系統的管理者又如何創設系統。

前已述及，若從 Foucault 所提及的意象出發[98]，監視構造的存在最終目標仍是改變個體的自我決定，使其在意識到視線存在的情況下對於自我的決定做出變更。此一過程經過變形之後，成為某些國家用以促使人民自我審查的工具，亦即讓每個人的心中產生一個小警總，並且揣摩上意，依循警總可能的(但其實未必需要政府直接發出的)命令行事。這個過程在前述中國大陸政府針對新疆人民的控制之中可以被觀察到，在中國大陸網路使用上針對特定敏感詞彙、圖片、歷史事件的封鎖以及網站自我審查的達成之中也可以被觀察到。在此觀察的角度之下，現代監視的機制仍有部分符合 Foucault 的圓形監獄模型，即透過提醒被觀看者目光的存在，促使被觀看者的自我決定改變。但有所差異的地方是監視目光構成的方式以及來源。**在 Foucault 提出的模型之中，看守塔是單一的、中心的，看守視線的存在則是曖昧不清、僅僅是潛在可能性的狀態。**但

[97] 董娟娟，前揭註 54，頁 119。

[98] 需要注意的是，圓形監獄的結構模型在資訊社會化以及資訊化人格等領域將會產生變形。此時對資訊化的個體來說，存在的不是視線，而是對數據的掃描、穿透。個體此時不會被結構所束縛，但卻會隨著個體與系統介面進行的接觸，持續地被掃描並且留存檔案。例如病歷的更新、戶籍制度登記、銀行交易紀錄、電子支付履歷、國境進出紀錄、網頁瀏覽歷程等。**以介面進行的掃描與對人格檔案的穿透取代了視線的建置。**

doi:10.6342/NTU201900452

在近代監視機制的發展之下，**看守視線的存在是確實而持續、分散而交錯，在現實空間中能化為實質，在虛擬空間中則穿透過個體。**這點與圓形監獄不同。同時監視目光的來源不再僅有單一的看守塔，監視的對象也不需要被聚集在特定的構造之中，兩者皆是分散的、錯雜的存在，甚至許多監視的對象會自願的與部分監視目光相連結，而未必需要動用到結構設計或是強制力來將個體納入其中。當然在特定的監視場域之中，與圓形監獄相同的場域結構仍然存在，而結構與空間設計以及強制力也仍然是監視或者資訊收集的重要手段。例如政府針對國民的身分證發放、國境管理的生體特徵(指紋)收集、建築與環境的監視設計等等。但監視社會的發展已然再更往前一步，**轉向數據的調控、資料庫的編碼、演算法的建立等領域中，並且持續的數據化、自動化、整合化。**在此的重點是數據化資料與空間中的實體結構互相結合後所形成的複雜監視場域，其雖然與現實空間接軌，主要的結構卻潛藏在演算法與資料庫之中而非肉眼可以直接觀察。

在資訊科技與監視科技的支持之下，現代監視社會並不需要將人放置在圓形監獄或與其類同的結構之中，只需要在之中加入一座一座的看守塔(監視視線的來源)即可。這些看守塔無須配置守衛，而可以交由 24 小時全年無休運作的電腦機器與網路來運行。這樣的看守與圓形監獄不同的是，其並不必然具備全知的目光，反而有可能比圓形監獄中的看守視線脆弱許多，僅能針對看守塔本身所預設的特定事項進行資訊的收集。例如單一監視器所能監視的特定範圍、gps 定位所能追蹤的單一位置、特定裝置連接網路後所進行的瀏覽紀錄、特定通訊軟體中留下的訊息等等。單一的看守塔看顧的範圍有限，但大量設置的成本並不高。例如從本文前述及之英國監視器設置數量、我國監視器設置之狀況看來，甚至連地方自治團體皆能夠承擔。同時這些設置的目的也不再是單一的統治需要，雖然仍然有部分促進個體的自我關注的因素在其中，更重要的要素反而是風險控管的達成，而此一目標依照前述社會分類段落的說明，有賴於對於監視目標更加精確的分類，以及不同監視端點與背後資料庫之間的串連。

另一個不同的點是，對於身處在監視網路之中的個體來說，某種程度上能夠部分對抗特定類型的看守塔。亦即監視視線的覆蓋並非如同圓形監獄模型所呈現的無法逃脫之狀況，仍留有部分選擇迴避視線的空間。分散的監視塔代表個體雖然必然會被某些覆蓋範圍較廣泛的監視塔關注，但能夠選擇不要出現在其他強制力量較低的監視塔之視線中，因此可以說**現代的監視模型是多層次化的、鬆散卻又綿密的狀態。此一狀態尤其在網路場域之中特別明顯，**如同前面章節提到的，虛擬場域在近代迅速發展使得許多個人資訊的取得在虛擬場域之中變得十分容易，而資料的再利用、編譯、流通也經常依賴以網路最為基礎的資訊設備。在此一前提之下，雖然個體經常難以逃脫資料庫的連接，但似乎有著部份的自行創設監視視線以對他人投以關注之可能性。例如商家自行裝設的

doi:10.6342/NTU201900452

監視攝影器、車輛裝設的行車紀錄器、由網路搜尋達成的人肉搜索等等。但若要將這些手法當作對抗分類與資料庫蓄積問題之方式，似乎較為無力。

第二項 個體的辨識與區分

第一款 身分識別與資料

在資訊介入監視場域之後，更加精細的身分識別(identification)成為第一要務。身分識別或者說個體識別是用以指涉我們藉由區別與標記而特定出一個單一而獨特個體的過程。其中對於個體的辨識，有三種基本的要素[99]（three basic elements of identity）：1.生物特徵之辨識（biometric identity）：為專屬個人之特性，如指紋、聲音、虹膜、面貌、DNA、掌形、散熱（heat radiation）等，其中以指紋最為方便使用；2.因出生被賦予之辨識（attributed identity）如全名、出生地點或時間、父母姓名及地址等；3.經歷之辨識（biographical identity）在生命經歷中逐步建立，包括在人生活中發生之事件及人與社會之互動，如出生之登記、學歷、選民登記名冊、給付之申請及納稅紀錄、工作之經歷、婚姻之註冊，財產之抵押及所有權、保險單；與銀行、債權人、公用事業及政府機關之往來等。在**身分識別的需求之下，實存的個體如果欲進行社會生活，皆必須將自身的以上幾種要素，或多或少的提供給不同的系統。**此一過程雖然由於人類之感官與社會組成方式，而屬於社會生活的必然。但正如同本文於介面之監視以及監視聚合體章節部分所提及的論述，這些數據化的要素組成的虛擬人格與實存個體之間，存在著無法避免的分裂[100]。

監視技術的發展，同時帶來大量資訊的累積。除了個人資料以外，由電腦系統控制的監視器所留下的影像、國家針對交通狀況的資料收集、網路服務提供者對網路使用情況的收集等等，這些資料無時無刻的產生並且被收集。此一情況為近年盛行的大數據分析提供了良好的使用環境，在監視技術與資訊科技

[99] 整理自釋字 603 號解釋余雪明大法官部分協同部分不同意見書，603 號抄本，頁 97。

[100] 若從偏向哲學的觀點來看，自從人類逐漸發展出個體意識以來，對於其他個體的認識其實本來便存在著此一割裂的情況。個人眼中的他人，未必能符合他人對自我的認識。甚至個體對自我的認識，也未必能符合自我的潛意識。從此一邏輯出發，既然同樣都會受到分裂問題的影響，資訊人格之分裂似乎與現實狀況無甚區別。但本文認為，資訊人格分裂之問題較現實認識之偏差問題來說更為嚴重。因為此一資訊人格經常被用來做為系統運作時用以判斷個體屬性並且將差別待遇加諸到個體之上的基礎，因此遠較現實中自我認識問題之偏差更為嚴重。簡單來說，現實中人與人之間的認識出了差錯，總比系統把你安排到不正確的分類來的安全。

doi:10.6342/NTU201900452

的支持之下，**資訊收集者所能收集到的資料能夠突破時空的限制，迅速累積。這些大量的單純資料在還沒有處理過之前，尚不具有明確的意義或威脅。**因此資料挖掘技術(Data Mining)[101]應運而生。所謂的資料挖掘是指在特定的戰略目標下(例如風險管理、顧客管理、反恐需求等)，將原始資料以特定的方式篩選轉化為可以利用的資訊。資料挖掘技術最初的雛型是來自於區分顧客潛在消費價值的需求，亦即前述消費取向監視技術發展的一環。而在不同領域大量資料持續收集累積以及資料庫建置技術持續進展的支持之下，在大數據時代中成為重要的手段之一。**數據與量化，對於決策者來說遠比理論容易操作，而在風險評估的要求之下，數據化過後的資料也最能直觀的被用以評估風險的高低。**

數據收集其中一個重要的來源，來自與網路相連的電子終端。常見的例子例如智慧型手機與智慧型手表等。許多網路供應商在智慧型手機內建的系統之中提供許多帶給使用者便利的 APP 以及功能，例如定位系統的提供、電子支付綁定、社群媒體的使用等等。在這些個人裝置之中，**大量的資料會不停地被蓄積，而成為政府、跨國企業等組織[102]試圖收集的目標。**因為在大數據時代之下，不論是為了統治需求或者商業需求，這些資料均能換算成有待開發的財富。同時在個體辨識之過程中取得的身體資料，亦能有效為資料庫提供更精確的資訊，這一點與本文前所提即的社會分類問題有所連結。進行個體辨識的最終目標，仍會回歸到決定對個體應採取何種待遇[103]之問題。此時**個體辨識需求與資料庫之建立兩者之間產生一種持續的循環，資料庫之建立目標本身即是為了能更精確的辨識個體，而在個體持續的與資料進行比對的過程中，資料庫也同時更新自身而擴張。**

---

101 Oscar Gandy, JR (2006). Data Mining, Surveillance, and Discrimination in the post-9/11 Environment. In Kevin D. Haggerty, & Richard V. Ericson (Eds.). (2006). *The New Politics of Surveillance and Visibility* (pp.363-367).

102 此處的組織並不單純指涉政府，任何有對個體進行蒐集資料之潛在需求，且具由層級化組織分類並以資訊科技做為應用媒介之組織均能歸入其中。事實上相較於國家政府對國民進行的資料收集，對消費者進行之資料收集可能更為大宗。因為許多網路供應商服務之消費者已經藉由網際網路之連接，遍布全球各地。例如 google、apple、facebook、twitter 等等。這些組織所收集的個人資訊(除了會員資料之外，還包括瀏覽紀錄、交易履歷、gps 定位等資訊)恐怕比某些國家的政府還要來得多。

103 舉例來說，國家對於出入境的旅客要求以護照或指紋等方式驗證身分，其目標便是決定是否允許特定個體入境或出境。銀行對於客戶的信用資料與交易履歷進行查核，其目標便是決定是否要放款或提供特定服務。差別待遇對於個體來說可能有好有壞，但重點仍在「決定分類」之過程以及演算法之運作。

doi:10.6342/NTU201900452

第二款 統計學與監視技法

有論者認為，「可被應用的情報(actionable intelligence)」是監視技術的進展帶來的其中一個重要價值。這一點一樣可以和資料庫加以連結，因為**依賴資料庫所達成的精確個體識別、對檔案的索引，皆是透過這些情報的使用使得決策目標的達成、以及決策因素的知識化，都變為可能。**亦即進行決策時，藉由這些情報，決策者可以選擇追求、建立、或者維持與存在/客體之間特定的關係[104]。而這些資訊的應用將可能直接影響到社會與社會中的個體。這些「可被應用的情報」的使用，極度仰賴統計學觀點的監視技法(Statistical surveillance)。這些技法的目標仍是用來對個體進行關注，其中有四個重要的技法，即身分識別(identification)、層級區分(classification)、評估(evaluation)與區別對待(discrimination)。

藉由**身分識別**系統將「姓名」與「個體」連結，使得個體不再處於匿名狀態，這一點對於資本社會來說非常有價值[105]。而現代監視系統便是達成此一目標的重要工具。統計學的分析也有效的提高這些系統運作的範圍、準確度以及可信度。需要注意的是，這裡所討論的身分識別，並非指個體本身的自我認知，而是一個「制度化的他者」如何區分個體的過程。**層級區分**(classification)此一技法下監視的目標更關注在定義「個體是甚麼」，此時統治的目標不是追求區別或獨特化，而是追求統計學上的最大公約數，並且得出數個藉由統計學方式區分出來的不同群體之間的差異。亦即定義群體後再決定個體應該歸與屬於哪一個群體之中。此處的重點是，個體屬於哪個群體並非個體本身所能決定，而這個分類的過程持續在社會中進行。**評估**(evaluation)在此則非針對個體的善惡進行，而是針對個體與他者之間的關係是否有害、是否有益進行預測。**區別對待**(discrimination)則可以被理解為在經過識別、區分、評估過程之後，個人或團體針對特定事項或是對特定個體所進行的待遇之選擇。因此所謂**統計的區別待遇**(Statistical discrimination)，便經常成為排除、區別、拒絕、接納特定個體，給予不同待遇，加入、或者不允許加入特定團體的理由。其所依賴的基礎在於大量個體資訊的取得以及數據的轉化，在統計學的支持之下將數據與對未來的預測結果進行連結，而後再以此決定對特定個體所採取的措施。與差別待

[104] Oscar H. Gandy, Jr (2012). Remote sensing in the digital age. In Kirstie Ball, Kevin D. Haggerty and David Lyon(Eds.). *Routledge Handbook of Surveillance Studies* (pp.125-126).

[105] 以下的四個統計學式技法整理自 Oscar H. Gandy, Jr，前揭註 101，pp.126-127.。從資本主義的觀點來看理想的市民除了應當成為優良的勞動力之外，最好也同時是優良的消費者。而一個優良的消費者其顧客的基本資料與消費偏好最好能被完善的把握。當然此一論述過於偏向資本主義中的消費關係，而難以完整用來說明其他領域所進行的監視，但卻能有效說明身分識別以及個人資料收集的其中一個目的，即個人資料的消費取向分析與商業使用。

doi:10.6342/NTU201900452

遇相關的手法，尚有分割(Segmentation)以及定向(Targeting)兩種。分割是將經過層級區分的個體在統計學設定或成本、效益、風險等考量之下再細分成特定類別。定向則是針對分割後的群體藉由適當的管道傳遞特別設計過的資訊。這些技法實際上與 Lyon 所提出的社會分類與差別待遇概念可以相互連接，作為其中一種手法使用。

在大數據與統計學的支撐之下，區分與差別待遇更容易取得正當性。因為相較於未必具有實證基礎的學說論述，以統計為基礎而進行的傾向預測似乎更加具有說服力。但在此一統計過程之中，被做為統計目標個體卻經常對於被分類的過程、依據、甚至可能連監視視線的存在都無法得知。同時統計學的監視並不如傳統監視那般依賴科技對於視覺、聽覺、其他感官的增強，而是將重點放在對於檔案及數據的分析與收集，這一點與前述的**監視視線於虛擬空間的穿透有關。監視目標現在的狀態以及過去的狀態為何並不是其所關心的重點，將其數據化呈現的資料才是能夠使用統計學方法操作的標的。**因此藉由數據計算出的決策及針對未來可能性之應對才是此種依賴數據與檔案的監視技法真正進行的目標。此一技法更進一步加深了資訊人格與實存個體之間的距離。在實存個體與資訊人格之間原本因為個體辨識的需要以及資訊科技的進展，已經經過一次從實存個體到數據的轉變，統計學技法的介入更進一步加深了數據與實存個體之間的割裂。可能導出的問題是，**倚賴這些具有割裂風險的數據來進行對於個體未來的預測或進行差別待遇，是否是剝奪了個體的潛在可能性之作為。**簡單來說，此種單方面進行的分類，是以柔軟的力道推動個體進行符合其被分類的群體之行為，並且具有限定其人格發展之可能性。本文並無意否認大數據與統計技術在與監視技術結合之後可能帶來之好處，諸如犯罪熱點地圖、高風險犯罪因素之統計等等應用固然能夠在施政上提供參考之指標。但於使用這些數據時似乎不能夠忽視隱含在這些數據之中的預設、因素的選擇、資訊人格與實體的割裂問題。

在後圓形監獄的時代之中，我們或許可以得到這樣一個粗略的結論。即監視視線環繞結構之目標轉變為**對於數據以及風險的控管與扼殺，環繞結構本身從物理性結構轉為虛擬而幅散且相互連接的結構，在某些程度上這些結構甚至藉由各種柔軟的手法鼓勵被監視者自願參與在其中。**對特定個體的精細辨識成為可能，個體可能會暫時的從系統中被遺忘，但仍然會被記錄在系統中，等待需要被搜尋到的一天，而這些資料庫所需要考量的卻只有成本效益問題以及法律問題[106]。

[106] 具體上來說法律如何對此一狀況作出部分的抵抗，將於後續章節處理。

doi:10.6342/NTU201900452

第三節 犯罪預防與監視技術

第一項 環境犯罪學

監視技術應用的其中一個重要領域，便是犯罪預防。文獻上對於犯罪預防的進行方式，有以下幾種理論被提出來做為政策施行的參考。以下先就理論的脈絡進行簡單的梳理，而後就已經實際應用在犯罪控制過程中的技術其應用狀況及問題進行分析。最後將就可能成為未來犯罪控制政策手法的技術可行性與其利弊進行說明。

第一款 公共健康模型(Public Health Model)

公眾健康模型參考自醫學上針對公共醫療與衛生問題所提出的分層醫療模型。分層醫療模式認為，在疾病防治領域中，與其僅僅加強進入醫院之後才進行的醫療程序，不如在疾病發生前便區分層次進行多方面的預防。其指出：**如果我們試圖預防一種疾病，僅僅通過治療那些染病的人群而不去觸動疾病背後的深層因素，這樣一種疾病肯定會繼續蔓延**[107]。因此在進行疾病防治時，應該區分不同層次的疾病成因，依照各自的特徵來分配資源進行疾病防治。其主要區分成三個層次，首先第一層次的預防是針對整體人口進行的事前預防，努力防治一切導致疾病發生的可能性。例如透過宣導多多運動、減少吸菸、加強健康教育、改善衛生習慣等等方式減少疾病發生的機率。第二層次的預防則是識別個人處於較高的疾病和傷害的危險時所處的環境。例如針對有較高患病風險的族群，如特定年齡以上者或具有特定遺傳病史者進行較高密度的追蹤與診療，或是對居住於較難取得醫療資源地區的人民提供醫療資源的灌注。第三層次的預防則針對已罹患疾病者，以治療、手術等等方式促使其恢復。

論者認為，公共醫療模型提出的預防勝於治療概念，也可以套用到犯罪預防領域中。將此一模型應用到犯罪預防領域[108]後，第一層次的預防便是強化環境中可以減少犯罪行為的因素，並且減少環境中可能產生犯罪風險的因素。第二層次的預防，則是針對具有較高犯罪風險的族群，進行針對這些族群設計的預防方式，來減少犯罪的發生。第三層次的預防，則是針對已經處在司法系統控制之下的犯罪者進行特別預防的工作。這三個層次，第一層次大致對應到社會、文化、社區環境，第二層次則大致對應到個體的發展、成長過程，第三層

[107] Barkan, S. E. (著)，秦晨 等(譯)(2011)，《犯罪學：社會學的理解》，第四版，頁 624，上海人民出版社。(原著出版年:2008 年)

[108] David A. Mackey & Kristine Levan (2011), *Crime Prevention*, pp.4-5.

doi:10.6342/NTU201900452

次則對應到進入司法程序之後的處遇[109]。此種分層次進行不同密度預防行動的模型，其優點是可以較為合理的分配社會資源，由程度的輕重不同來決定應該投入多少資源進行犯罪預防工作。此模型可能有所疑問的是，大部分常見的疾病成因，在醫學的發展之下已經被順利發現且透過科學方法證實。但大部分犯罪的成因卻無法如此明白的斷定。相反的，通案式的對犯罪的成因進行分析的論述，通常都認為需要綜合考量各種可能導致犯罪的因素。即便通過對特定個案的人生歷程分析來嘗試歸納其犯罪的成因，該因素也未必能夠通案式的適用到其他人的情況。也因此，這些誘發犯罪的因素，至多只能說是可能對犯罪行為的發生產生推力的因子。學者在此提出的幾種可能影響因素如下：貧窮、階級差異、種族因素、學校教育問題、社區家庭環境問題、疾病等等[110]。

在誘導犯罪的因素未能完全得出通案性標準的情況下，各個因素如何定義以及與犯罪風險的關聯性高低便產生疑問。同時需要考量的問題還有各個因素對不同類型犯罪可能產生的影響，因此在定義影響因素時，也需要注意到這一點。在此模型下，除了環境因素的設定之外，還需針對人口族群進行識別、確認預防層次的分配，具體來說，在定義了高犯罪風險的族群特徵之後，尚須從整體社會人口中將之標示出來，此一識別與區分的過程，正是後現代監視的特徵。此處所採用的流程其實與本文前所提及的後現代監視特徵：人口區分與偏差的標記以及澳洲政府福利政策的運作方式有極大的類似性。而在此模型所欲達成的犯罪預防目標來說，同時兼具了兩種特性，即偏差的標記(必須說明的是犯罪高風險族群其實只是處在可能轉為偏差族群的狀態)以及福利政策目標的設定(即預先阻止犯罪的發生、避免這些族群轉為偏差族群或者預先排除可能產生偏差的族群)。而這種「犯罪高風險族群」的認定之有效性與利弊亦是值得檢討的問題。哪些因素的存在可以使人被認定為高風險族群？國家對待這些族群可以施予不利益嗎？區分之後是否能夠對犯罪預防起到明顯的效果？而監視技術、人口治理、統計學以及大數據等技術也因此成為操作此模型的重要工具之一。

第二款 理性選擇理論(Rational Choice Theory)

理性選擇理論[111]認為，人在選擇是否要犯罪時具有自由意志，在自由意志之下衡量犯罪所得與成本，最終決定是否進行犯罪行為。在此前提下，如果社會能夠使得犯罪的成本高於犯罪所得，一個理性的人便不會選擇犯罪，因此透過提高犯罪成本，並且確實使該成本反映到犯罪者身上，便能使理性的人選擇

[109] 整理自 Barkan, S. E.，前揭註 107，頁 628-638。

[110] 整理自 Barkan, S. E.，前揭註 107，頁 628-638。

[111] David A. Mackey & Kristine Levan，前揭註 108，pp.5-6。

doi:10.6342/NTU201900452

不要犯罪，達到犯罪預防的目的。其認為，1.犯罪是有目的的行動，在犯罪者利己的意圖之下被實行。2.犯罪者會將關聯的風險與不確定性作為前提，進行最佳的選擇。3.犯罪者的意思決定，會隨著犯罪的類型有所不同。4.犯罪者是否要牽扯上特定犯罪類型的選擇，以及針對特定事件是否實行的選擇會有所不同[112]。在這些前提之下，對於犯罪者來說其所選擇的犯罪必然有著其所預想的利益，而這些利益具有多樣性，未必限於物質上的報酬，犯罪所帶來的興奮、娛樂、性的滿足、對於他人的輕蔑與支配等等皆能算是犯罪所得的利益。因此即便部分犯行的選擇乍看之下不符合成本利益的計算，對於犯人來說卻必然會有著一定程度的合理性存在。這一點被提倡理性選擇理論的學者稱之為限定合理性(bounded rationality)。但理性選擇理論雖然透過擴大對於「利益」的認定範圍將犯罪者的選擇納入成本與利益計算之中，其仍然無法解決心神喪失或精神疾病患者所進行的犯罪行為問題。另一個弔詭的問題是，選擇心智上的衝動、強迫偏執似乎和傳統哲學觀點上對於理性的預設有所衝突。

隨著理性選擇理論之發展，進一步延伸出威嚇理論(Deterrence theory)。此理論的支持者認為，既然人會進行理性的選擇，在刑罰帶來的懲罰足夠強大時，理性的人不會選擇犯罪，因此便能夠嚇阻犯罪的發生。具體來說，在一般預防層面透過使社會大眾理解法律的內容並且遵守法律，在特別預防層面針對犯罪者使其體會到犯罪成本(在理性選擇理論的框架下，此處的犯罪成本通常是指司法審判後帶來的懲罰)的不適感，其自然會依照理性決定不要犯罪，如此便能夠達到犯罪預防的目標。此理論與理性選擇理論相同，最大的問題在於對理性的預設過於理想，實際上某些犯罪者在犯罪當下可能受到情緒支配，並不會將其強調的犯罪成本納入考量。以監視器的其中一個功能來說，即使監視器預設的目標便是嚇阻在鏡頭拍攝範圍內的犯罪行為，仍然可以常常看到犯罪影像被記錄下來並進而做為追訴的證據。

第三款 日常活動理論與情境犯罪預防

日常活動理論(Routine activity theory)始於學者 Cohen 和 Felson 的研究，其認為犯罪的發生主要由以下幾個因素組成[113]，「必須出現有動機的犯罪者」、「有前者所希望或想獲得的合適的標的物」及「犯罪人和合適標的物出現在同一時地，而且缺乏有能力避免犯罪發生者或阻止犯罪失敗」。這些因素與前述的理性選擇理論有所連結，其認為犯罪者在選擇是否犯罪時會受到促使其犯罪的推力

[112] 守山 正(2017)，〈犯罪予測技法の展開－近接反復被害分析を中心として－〉，《政治・経済・法律研究》，Vol.20 No.1，頁 15。

[113] Marcus Felson (2002), *Crime and Everyday Life*, p.21.

doi:10.6342/NTU201900452

以及阻止其犯罪的阻力影響，因此透過調節這些促成推力或阻力的因素，便能阻止犯罪的發生。亦即透過增加犯罪的阻力以及減少犯罪的推力來作為預防犯罪之手法。具體來說，其可以採取減少犯罪的動機、避免標的物暴露在可以簡單被取得的場所、增加能夠嚇阻犯罪的監視器等等方法。

情境犯罪預防理論(Situational Crime Prevention)則將犯罪推力與阻力之概念進一步具體化，以增加犯罪阻力、增加犯罪風險、減少犯罪誘因、減少犯罪刺激、移除犯罪藉口等五大策略[114]針對環境進行設計，並藉此預防犯罪之發生。其中監視技術的位置被放置在增加犯罪風險位置，其並舉例認為 CCTV 之設置將能夠對潛在的犯罪者造成足夠的威脅[115]。具體上可以採用的犯罪預防對策[116]如下:1.對象物的堅固化，例如將自行車上鎖、將窗戶改成防盜窗等。2.對象物的除去，例如從現金交易轉為電子支付。3.去除犯罪手法所必要之手段，例如為預防劫機及恐怖攻擊在登機前進行行李檢查、槍砲彈藥刀械的販售管制等。4.利益的消滅，例如在所有物上署名，減少其商品價值。5.公共場所的監視，例如透過警察的巡邏提高犯罪偵查的可能性，以及提高一般預防效果等等。6.自然的監視，例如在建築構造上去除死角，並且增加照明，使得居住者有較佳的監視視野。7.由使用者進行的管理，例如在學校或住宅等的配置警衛。8.環境的管理，例如將足球場中支持不同隊伍的觀眾席分開避免糾紛。以上手法，皆是針對環境進行設計，將理性選擇理論的宗旨轉換成可能導致犯罪發生的具體特定狀況後，逐一調整特定犯罪行動可能面臨的風險、困難程度，或是減少特定犯罪行動可能獲得的利益[117]，並藉此達成預防犯罪之目標。

第四款 小結

自公共健康模型、理性選擇理論、日常活動理論、情境預防理論等等理論的觀點轉換之中，可以發現到雖然古典刑法預設的理性與自由意志等考量，仍然存在於環境犯罪學路徑的考量範圍內，但這些理論主要關注的還是犯罪的空間與地點等環境條件，犯罪者內心的自由意志與動機等問題則被作為進行環境設計時綜合考量的因素之一。以環境結構之設計作為應對犯罪方式時，導致的結果是古典刑法學中對於「犯罪者的理性與自由意志」此一預設逐漸不再被環境設計所重視。在環境犯罪學想法下，犯罪者在進行犯罪時考量的不再是「規範」的存在，而是「被發現或逮捕」的風險。以犯罪預防策略的實效性來說，

[114] Ronald V. Clarke (1995), Situational Crime Prevention, *Crime and Justice*, Vol. 19, pp. 91-150.

[115] Ronald V. Clarke，前揭註 114，pp.113-114。

[116] 整理自岩井 宜子(2011)，《刑事政策》，第五版，頁 86-87，尚学社。

[117] David A. Mackey & Kristine Levan，前揭註 108，p.7。

doi:10.6342/NTU201900452

此一犯罪者內心所進行的考量其實並沒有太大的差異，因為不論犯罪者所考量的是規範還是風險，最終所欲達成的減少犯罪效果並不受影響。但刑法的預設與環境犯罪學的路徑卻似乎因此出現了無法接合的部分。原本規範預設的目標中個體應該理解規範內容並且遵守規範。此一想法在現代逐漸被風險、環境設計所取代，與其強化規範效果，不如直接從風險與環境因素著手，直接調整犯罪行為而不處理犯罪者對於規範理解之問題。刑事法雖然有因應此一狀況作出調整，但其核心預設並沒有改變，本文因此將此一不再重視規範意義的傾向稱作規範消融。而於此須注意的是**監視技術作為環境結構而存在/作為具體資料運作手法的多重角色**。

第二項 監視技術與犯罪預測

第一款 預測性警務

在上述環境犯罪學取向之犯罪預防理論之中，監視技術經常被用來作為「可視性的創造」之重要手法，監視技術所帶來的視線被用以「嚇阻」並「增加犯罪成本」。而這些**路徑通常傾向將監視技術的設置與環境結合，使其作為社會中日常存在的結構，並且對犯罪事件產生影響。此一面向基本上是將監視技術作為犯罪預防結構的一環來產生作用。**亦即用以嚇阻及調控之結構性監視。此種監視手法雖然仍具有可視性創造、根莖式散布等近代監視特徵，但並不具備資料處理與蓄積、預測之特性，單純作為結構而存在[118]。

除了以環境與結構設計之手法應用監視技術來預防犯罪之外，另一個重要的方向即是自監視技術與資料處理方面的連結著手，藉由監視技術進行個人資料之收集，並進一步對犯罪之可能性進行預測。例如許多收集個人資料的法規經常將犯罪預防作為其重要的立法理由之一[119]，便是此類型應用的實例。促進此

[118] 需要注意的是由於監視技術的聚合體特性，在環境犯罪學路徑之下雖然將監視技術單純作為可視性創造以及威嚇的手段，實際上這些監視技術在運作的過程中仍然會產生大量的資料，並且可能在其他領域有所應用，甚至與犯罪預防之目標間接或直接相關。以監視器為例，商家設置的監視器在某程度上能夠作為環境犯罪學所設計的結構因素嚇阻部分犯罪的發生，但同時亦持續在收集該範圍內之影像資料。

[119] 例如身分識別以及個人資訊收集之立法，其立法目的經常與犯罪預防以及偵查相關。如南韓在「住民登錄法」強制按捺指紋之目的為（１）因應南北韓分裂之整體安全需求（國家安全）；（２）預防犯罪及協助案件偵查；（３）一般身分確認。英國有生物特徵之身分證法案之立法目的為：（１）防止身分冒用；（２）防止非法移民及工作；（３）防制濫用政府服務（福利）；

doi:10.6342/NTU201900452

類危險預測型監視技術發展的其中一個重要的原因，即為監視技術與國家警察活動的緊密連結。受犯罪率上升、恐怖活動等等治安惡化影響以及監視科技的支持，警方逐漸被要求改變其對犯罪所採取的應對方式，亦即從以犯罪者的逮捕、追訴、處罰為中心的反應式警務(reactive policing)轉向預防式警務(proactive policing)[120]。預防式警務核心的想法認為，單純打擊已經發生的犯罪並不足以維持社會的安全，警方若能強化以預防式資訊收集為主體的警察活動，並且藉人力分配、危險源的及早發覺等方式，在事前阻止犯罪，將能對治安之維持有極大的幫助。

刑事案件的偵查技術以及犯罪預防的手法，隨著資訊科技發展持續改變。一般來說，使用科學技術能夠使得發現真實的成功機率增加，而使用資訊科技則能夠使警政機關能夠更加流暢的累積、使用資訊並進而提升效率。除了警政機關本身作為官僚組織的屬性，使其需要累積並處理資訊之外，另一個重要的原因則是其執行的業務(治安與社會秩序維持、犯罪的偵查)與資訊收集本就具有深度關聯性。以內政部 108 年施政計畫所提示的治安目標為例，與資訊科技的應用密切相關的施政方向即有：治安維護工作、科技偵防、國境安全控管、防範社會高風險族群犯罪等等[121]。在這些施政方向之下，監視器系統的連線、雲端警政系統的建置、分配給個別警員的個人終端等等，皆是科技與警察職務的執行結合的實際應用。而在犯罪預防與偵查領域，近年尤其值得注意的發展傾向則是資訊收集技術與監視技術發展所帶來的變化。例如使用 GPS 系統的位置追蹤、針對智慧型手機與通訊軟體內容所進行的監視等等，甚至透過個人資訊的「取得」、「保管」、「事後使用」等手段達成的「個人人格檔案」建立，也成為值得檢討的問題。在傳統刑法的觀點中，預防分為一般預防與特別預防兩種。前者指對非特定的群眾所進行的犯罪預防，透過構成要件的違反與刑罰惡害的連結來加以進行。特別預防則是針對有犯罪前科者進行，以特定個體的再犯防止為目標。但是，如果運用前述的資訊科技，以針對大量人口所收集的資料作為基礎，是否有其他開展犯罪預防技術的可能性存在，即成為問題。在監視社會與風險社會的想法之下，針對犯罪的應對，是否可能從規範與刑罰惡害的層面，轉向事前預測與預防？

預測性警務(Predictive Policing)的概念因此應運而生。預測性警務係指任何

（４）防止組織犯罪及恐怖主義。法條內容整理自釋字 603 號解釋余雪明大法官部分協同部分不同意見書，603 號抄本，頁 100-103。

[120] 星 周一郎，前揭註 14，頁 43-44。

[121] 節錄自內政部 108 年施政計畫，網址:
https://www.moi.gov.tw/chi/chi_public/policy.aspx?policy_code=02&type=info 最後瀏覽日期 2019.01.11。

doi:10.6342/NTU201900452

發展並使用到資訊以及以資訊為基礎的分析，達成預警式犯罪預防的治安策略、技巧[122]。其通常應用各種分析性工具(混合各種科技手法，並且尤其仰賴資訊科技協助分析)，以標示出需要警方關注的目標、預防犯罪的發生、或者藉由統計手法解決過去的犯罪。

在監視技術與資訊科技加入以前，預防式警務原本被認為並不可行，至多僅能以提高見警率等等方法盡量避免犯罪的發生。其原因除了犯罪原因的複雜性質導致的預測困難之外，還有警察人力資源分配的考量。但在監視技術與資訊科技結合之後，針對犯罪所進行的事前預防技術逐漸邁入應用階段。預防式警務與監視技術的結合主要體現在 1.藉由監視視線的存在嚇阻犯罪的發生。2.藉由監視發現危險源，提早對犯罪的發生進行應對這兩個方面。嚇阻犯罪的應用方式與環境犯罪學路徑處在同一個脈絡之下，於此將重心放在「藉由監視與資料處理來預測可能存在的危險」這一部分。

預測性警務其仰賴的基礎，是大量與犯罪行為相關聯的資料收集、資料庫建構與分析以及資訊科技的應用。目的則是使針對犯罪的國家介入行動早期化，在犯罪發生之前即加以制止，或者在犯罪損害擴大之前盡早加以防治。**這些特徵與前述的後現代監視特徵有極大程度的符合。**犯罪預測系統首先要解決的問題是，其應該選擇何種標的進行預測。目前可能被拿來觀測的標的有犯罪行為本身的發生、具有執行犯行可能性者、行為人的檔案、潛在的被害者[123]等等。以這些可選的標的為中心，主要的預測方向又可區分為兩種，其一為針對環境進行預測，其二則是針對特定人物的人格檔案進行預測。以目前實際開始應用的預測系統來說，主要以針對「環境面向」及「犯罪行為本身」所進行的預測為主流。針對其他標的所進行的資訊蒐集與預測由於經常需要對對象進行人格測繪，嚴重影響到人民的自由權與隱私權問題，因此原則上不會進行[124]。

以環境為中心的犯罪預測系統主要依循的數據來自於特定地區過往犯罪紀錄的整合分析、或是特定環境因素交織之下犯罪率的評估。其背後的理論基礎，是認為犯罪的發生會受到環境的影響，因此曾經發生過犯罪的地點經常有反覆被害化 (repeat victimization)的問題，而論者指出「過去的犯罪是預測將來的被害風險最合適的因子[125]」。因此透過收集過去犯罪的資料，分析曾發生犯罪的地點與時間軸分布，能夠一定程度上藉此預測未來可能發生犯罪的時間與地

122 Ferguson, Andrew Guthrie (2012), Predictive Policing and Reasonable Suspicion, *Emory Law Journal*. Vol.62, p.265.

123 守山 正，前揭註 112，頁 3。

124 例外的狀況可能出現在重大犯罪的追蹤、跨境犯罪的追蹤、恐怖攻擊的預防等。

125 守山 正，前揭註 112，頁 2。

doi:10.6342/NTU201900452

點。以此一預測為基礎來分配警力，有助於警政資源的效率化以及犯罪預防的達成。

在此種以環境為中心之犯罪預測系統中，現今主要使用的分析分法有熱點（hotspot）分析、鄰近反覆被害分析、危險地帶分析(Risk Terrain Modeling, RTM）[126]等等。所謂的熱點分析法，是以歷史上曾經發生過的犯罪檔案為基礎，以此預測具有較高犯罪風險的區域。其所依賴的根據在於，犯罪不論在甚麼區域發生，其分布皆非平均散佈，而是偏在於一部份的地點與地區。藉由對過去犯罪案件的收集，可以區分出犯罪可能性較高的地區。但此種分析手法可能面對的問題，是都市環境的變遷以及犯罪事件的時間軸變化，以及犯罪黑數無法被納入統計的問題。鄰近反覆被害分析法則假設，一部分的犯罪發生在時間上與空間上會與過去發生的犯罪接近。因此犯罪率較高的區域在不遠的將來之中其近鄰區域也將會維持較高的犯罪率。其原因主要在於相近區域的被害者與環境通常有著相似的特徵與屬性(例如群聚的公寓大廈、酒吧等地點)，因此可能會反覆成為犯罪的標的。在此一前提之下，近鄰反覆被害有著群化的傾向，會使犯罪相對容易聚集在特定的區域，因此產生犯罪熱點[127]。危險地帶分析法則先確認犯罪風險較高的地理特性(如酒店、主要道路)，並且以這些特性為基礎來進行犯罪風險的預測。一般警察進行臨檢時也可能會採用類似的想法來設立臨檢地點。由於熱點分析法本身是用以確認犯罪集中發生地點的技法，其必須仰賴過去犯罪的資料作為分析的基礎。危險地帶分析法則是考量地形與地理學的特徵來進行預測，較為依賴精確的描述不同地理學特徵，並且測定其犯罪風險的高低以精準的預測犯罪。

第二款 人格檔案與科技

在刑事政策面向，需要注意的問題則是人格檔案的分析流程如果被用來檢驗個體是否具有犯罪風險時，所產生的誤判可能性。此處所謂的人格檔案，指的是藉由監視技術對個體進行資料收集之後，重新組合這些資訊並且試圖得出一個完整個體形象之過程。當然不可否認的是，在案件偵查過程中，使用類似的人格檔案分析手法亦有可能有助於犯罪偵查的進行，甚至是針對尚未發生的犯罪進行預防[128]，而在量刑階段亦可能使用到此一人格檔案作為判斷的基礎。

[126] 守山 正，前揭註 112，頁 4。

[127] 守山 正，前揭註 112，頁 5-6。

[128] 就以資訊收集為基礎，試圖對尚未發生之犯罪進行事前預防的嘗試，可以參考星 周一郎(2017)，〈犯罪の未然防止・再犯防止と情報の取扱いに関する覚書き〉，《法学会雑誌》，58 巻 1 号，頁 60-62、頁 69-73 之說明。

doi:10.6342/NTU201900452

以人物之人格檔案為中心的監視手法，可參照德國對於「包括性監視」之相關規定。其核心概念在於使用不同的監視手法與監視設備相結合，並且針對個體進行環繞性的資訊收集，例如藉由監聽、通信紀錄擷取、gps 定位追蹤分析等等方式試圖建立完整的個人人格檔案。在資訊設備加入犯罪偵查之後，最主要的差別在於資訊的收集、紀錄變得十分容易，同時收集的過程能夠秘密進行，並且能夠大規模的、跨領域的進行資料收集，這幾點與過往的偵查手法有很大的不同。將這些個人資訊**進行總合性的收集與分析之後，有可能可以得到比單純資訊總量所能呈現得更多資料，**而這些資料可以用在恐怖攻擊對策、組織犯罪對策等方面[129]。其具體運作方式即是由本文前所提到的各種監視技術綜合運用，對於目標的人格檔案進行測繪。論者並指出：「單純以某一個監視措施個別來看，其本身確實符合法律規定，但若將之與其他的監視措施加以結合分析後，會導致『包括性的人格檔案』的產生，則這種『人格的包括性監視』將構成對人格權與資訊自我決定權之嚴重侵害[130]。」。包括性監視的問題便在於，藉由多種監視手法的組合以及對資訊進行重組與分析之後，個人資訊的累積將產生質變[131]。而此一質變的過程，亦是資訊人格與個體之間的斷裂其中一種發生的態樣，因為這些資訊組合的方式可能透過系統，也可能透過人為進行，而這些過程之中均有可能發生錯誤與斷裂，但**這些錯誤與斷裂在系統之中則有可能被當作演算法的結果，更進一步成為差別待遇依據的標準。**另外需要注意的則是對於資訊之取得、蓄積保管、處理加工、事後利用之後衍生出的人格權侵害問題，因為法官在現行法下針對各該單一具監視性質之強制處分進行判斷時，未必能夠將其與其他監視性質之強制處分結合後產生的效果納入考量。

伴隨著風險概念與看待犯罪者態度的再次轉變，監視技術與犯罪偵防領域更加緊密結合，警務與科技結合亦成為許多國家警政實施的重點。以我國內政部提出之 107 年度施政計畫(警政部分)為例，其中與監視技術相關的目標有審慎防範社會高風險族群犯罪、強化科技偵防，提升打擊犯罪量能，推動的相關計畫則有警政雲端運算發展計畫第二期－警政巨量資料分析與運用、警政發展

[129] 内藤 大海(2016)，〈総合的監視に関する予備的考察：ドイツの議論状況の概観を通じて〉，《熊本法学》，Vol.136，頁 158-159。

[130] 内藤 大海，前揭註 129，頁 166。此為德國聯邦普通法院第三刑事部 2001 年 1 月 24 日判決之部分內容節錄，由筆者轉譯為中文。

[131] 舉例來說，筆者每日搭乘同一班公車通勤，固定在台灣科技大學下車，刷的悠遊卡則是台灣大學的學生證，並且固定步行前往法學院霖澤館。這幾個能透過監視與資料收集得到的資訊，分別單純來看可能未必對筆者的人格檔案產生何種影響，但若將三者結合分析後，便可合理做出筆者就讀於台灣大學法律系此一結論。這一例子雖然未必足夠精確，因為若能直接觀察學生證亦可得到同樣結論，但或許能夠說明對不同方面的資訊進行收集而後整合之後，所可能得到的分析結果將會超出個別資訊本身這一點。

doi:10.6342/NTU201900452

方案第二期(通訊監察系統建置計畫)、建置新世代行動網路 App 偵查相關系統中程計畫、資安旗艦計畫－預防暨打擊科技犯罪精進刑事科技能量計畫[132]等。就各該計畫的具體內容來說，目前主要集中被用以協助偵蒐犯罪的系統與個人資料蒐集[133]以及通訊監察強化[134]較有關連。通訊監察的目標在於強化對行動電話位置的定位，以及電腦 IP 的追蹤與使用者身分分析[135]。這些計畫的目標，乃是試圖將傳統的「通訊監察」工作，擴大為「數位偵查」工作領域，並且提升科學辦案效能[136]。該等系統之建置計畫在法律授權下進行，警方調閱資料也受到通訊監察保障法之管制，但仍不可諱言地帶來侵害人民隱私的疑慮。

科技與警務的結合，固然在協助警方偵辦特定類型案件例如毒品買賣之中有良好效果，但必須注意的是這些系統所留下的空白空間。借助系統能夠調取電腦的 IP 與使用者資料，則進一步的通訊內容、網路瀏覽紀錄也無多少技術門檻可言。對於行動電話能夠進行模糊的定位，如果結合行動電話本身安裝的應用程式，取得更多個人資料亦非難事。這點在前述中國針對新疆所進行的社會監控實驗中已然可以看出端倪。

---

[132] 參照我國內政部 107 年度施政計畫，警政部分之描述。我國內政部 107 年及 108 年施政計畫，取自: https://www.moi.gov.tw/chi/chi_public/policy.aspx?policy_code=02&type=info，最後瀏覽日期 2019.01.11。

[133] 如警政發展方案第二期 (104-107 年)，頁 11 提及「有線電視多媒體監偵系統」及「台灣大哥大與遠傳電信 IP 多媒體核心網路監偵系統」刻正建置中，啟用後案件程序進入系統化管理，作業時間縮短為電子投單審核後即時上線，且對於各類依法申請通訊監察案件，能提供檢、警、憲、調、海巡、廉政、移民等各執法機關監察資料，有效打擊犯罪。資料取自：我國警政發展方案(第二期)(107 年作業計畫)，網址為：http://117.56.91.94/KMPublic/readdocument.aspx?documentId=279751，最終瀏覽日期：2018.01.11。

[134] 如警政發展方案第二期 (104-107 年)，頁 18 提及，建置國際 NGN 新建交換機通訊監察系統，有效打擊跨境犯罪，確保國家安全，維持社會秩序；升級第一代 M 化偵查網路系統，提升 3G 行動通訊目標定位追蹤功能，強化全國各地刑案偵辦效率及緊急狀況之即時處置；建置 IP 通聯調閱系統，迅速獲得犯罪者個人資料，提升偵查效率，前揭註 133。

[135]如警政發展方案第二期 (104-107 年)，頁 41 提及，偵查人員偵查所得的 IP 地址，透過本系統可迅速獲得使用者使用該 IP 上網之地點(IP 實體地點定位功能)，以及該 IP 之「使用者身分」，如姓名、身分證或手機號碼等相關資訊(亦即個化分析功能)，作為進一步偵查辦案或通訊監察之基礎，前揭註 133。

[136]警政發展方案第二期 (104-107 年)，頁 53，前揭註 133。

doi:10.6342/NTU201900452

第四節 規範內化的放棄

第一項 控制社會

在監視技術與犯罪控制的結合之下，個體在這些系統之中逐漸被定位為「潛在危險源」，且系統具有藉由對於各種預設危險要素的計算，具體得出每個個體的風險，並且依照風險的高低採取不同的行動的能力。此即前所提及的，個體識別、定性、差別待遇之流程。在以扼殺風險為目標的社會之中，對於個體進行的控制模式從以空間為基礎的規訓社會轉變成以「調整」為基礎的控制社會，並且帶來規範意義的改變與個體自我關注的放棄。此時被認為重要的是，如何扼殺對於社會來說的「風險」，而個體對於規範的認知則不再重要，重要的是個體是否能夠被順利的調整並且減少對社會的風險。

組成控制社會的技法邏輯，依照 Deleuze 的說法[137]，應是調整(modulation)而非鑄模/同一化(molds)。這一個重要的技法差異，**亦揭示出了從「規訓社會」轉向「控制社會」的過程**。規訓社會中的同一化技法，在權力藉由空間的配置以及結構設計所進行的社會控制之中能夠被觀察到，這些結構的設計(例如圓形監獄、學校、軍營、工廠)如同鑄模一般，固定住其中的物件(即個體)並將其琢磨成固化且定型的狀態，其運作的具體方式則透過集中管理、空間的分配、時間安排上的規律等方式進行，並且依賴著物理空間進行。在 Foucault 所提出的規訓社會概念之中，其鑄模之模具或者說所要達成的目標便是所謂的個體(individual)。在本文前述章節所分析的全景敞視主義之中，便是藉由結構的設計以及存在於自我以及結構之中的監視目光，導引出自我對自我的審查與反省，並藉此讓個體逐漸往規訓的目標同一化。此時的監視視線如同負責加熱鐵漿的火源，將個體融化並促使其融入鑄模的形狀之中。在規訓社會的概念之中存在著兩個二元對立的結構，即標示出個體存在的烙印(signature)以及標示出個體在群體中所處的位置之數字或計算資訊的指示(indicates)[138]。規訓作用的方式是將這些個體在空間上組合起來，並使每個個體的個性依循著空間的規則同一化，此時權力對個體的分化和聚集是在同一個時空下產生作用的。需注意的是此時使用的數字概念是用以在群體中標示出個體，與後續控制社會概念下將個體轉換成資訊與數據的資訊人格概念(data double)並不相同。簡單來說，規訓社會下個體仍然是個體，只是以數字代表。但在控制社會之中，數據與資訊化的人格在某種程度上已經可以取代個體的存在，各種社會機制的運作亦經常是以這些數據為目標。

[137] Gilles Deleuze (1992), Postscript on the Societies of Control, *October,* Vol. 59, p.5.

[138] Gilles Deleuze，前揭註 137，p.5。

doi:10.6342/NTU201900452

相對的在控制社會的概念之下，Deleuze 所指的調整(modulation)之運作方式則不同。以科學的用語來說，調整是以一種波狀的形式對於人格進行可變動的控制，具體作用的方式則是透過數據的調控。Bogard 指出，這一調整並不是直接作用在個體，而是藉由「震盪(oscillation)」的方式，以使個體驅向(trends)或傾向(tendential)特定的具有統計學上意義之活動[139]。其中一種調整的型態，便是統計學式控制，此種型態基於生產頻率的調整、足夠的小樣本以及標準差而建立。統計學式的控制並不需要配置空間結構，而是依賴數據與資訊的計算及追蹤(例如資料挖掘技術)。將這些數據與遠程的控制手法結合之後，特定的生產過程之管制並不需要將對象聚集在特定場所便可進行。介面與介面之間的連接依賴數據化的評價機制，個體與其他介面的連接必須在這些評價的前提之下進行，或者可以說代碼與代碼之間的連接，必須在符碼之下以通行口令進行。**此時遂行控制的不再是空間結構，而是通行口令與符碼的編譯**。簡單來說，資訊科技所構成的虛擬空間以及統計學是控制所帶來的結果，使得欲達成特定控制目的之結構設計不再受限於物理環境，而能夠透過對程式碼進行編碼之方式進行。再進一步引申，資訊社會中構成虛擬空間的底層基礎，便是由數據組合而成的程式碼，因此掌握對這些編碼進行調整權力者便能在虛擬空間中實現控制此一虛擬結構之目標。Deleuze 指出，在控制社會之中，重要的不再是規訓社會用以控制與調節的口號標語(watchwords)、數字與烙印。控制社會的主角是符碼/編碼(code)以及通行口令(password)[140]。

在 Deleuze 所發展的控制社會概念之下，代表個體的符碼如何編譯以及個體與介面之間的連接是否需要透過通行口令、通行口令如何設計等問題便成為進行社會控制的重要關鍵。此處所謂的個體即是生活在資訊社會中的人類，介面則是該個體與其他個體或其他系統所用以連接的媒介。舉例來說，個體與國家政府之間藉由稅收的繳納、社會保險、健康保險的加入、國民戶籍制度之設立、駕照之考取登記、房屋地政之登記等等方式與國家政府進行連接。此時在系統之中必須存在著代表個體的編碼，此一編碼必須是政府所能讀取(且通常亦是由政府所設計)，個體則需要透過通行口令連接到介面、系統之中。通行口令的形式事實上並無須拘束在帳號密碼之形式。但使用在資訊社會之中習以為常的輸入帳號密碼之方式有助於理解 Deleuze 在控制社會概念之中所進行的詮釋。簡單來說，個體需要藉由通行口令的輸入向系統證明個體正是系統中所留存之編碼所指代之個體。此一流程看似簡單易行，但事實上經過了對個體進行編碼、系統保存編碼、個體提交通行口令、系統確認並且對編碼再評價或對個

[139] William Bogard (2012). Simulation and post-panopticism. In Kirstie Ball, Kevin D. Haggerty and David Lyon(Eds.). *Routledge Handbook of Surveillance Studies* (p.32).

[140] Gilles Deleuze，前揭註 137，p.5。

doi:10.6342/NTU201900452

體進行回應之程序。在這些程序中有許多與監視技術有所連結的環節。例如對於個體的編碼完整度仰賴著藉由監視技術達成的資訊收集，保存編碼與評價則涉及了資訊收集的蓄積與處理，提交通行口令與差別待遇的過程則是「個體辨識」以及分類、區別對待之手法。

值得注意的是，Deleuze 指出在規訓社會中此一定型的過程是可以隨著鑄模的改變(例如從學校到軍營、從軍營到工廠的過程)而重新開始的[141]。原因在於規訓社會的規訓過程是藉由封閉場所中的封閉規則所達成，而一旦規訓的場域發生變化，個體便需要重新適應新的規則與規訓過程。亦即，規訓社會的規訓手法以空間作為依歸，連結到圓形監獄模型中「可視性的創造」。圓形監獄中的視線雖然是不確定的視線，但仍具有著實體與依賴空間的性質(因為囚犯必須要意識到其有著被看的可能性)。但在其接下來提出的控制社會概念之中，對於空間性的要求已然消失。因為在控制社會之中藉由符碼與通行口令對個體進行的調整在死亡之前並沒有終止的一天。

第二項 編碼與虛擬空間

虛擬空間中超越距離的數據收集能力以及前述資訊化人格之問題結合之後，規範意義在監視場域之中逐漸消融。在控制社會的概念之下，對於個體而言，規訓、自我關注等概念重要性大為下降。個體所應當依循的是這些經過數據化的資料以及進行資料收集、監視的行為所引起的「震盪」，以及震盪背後存在的符碼。這些符碼的性質與規則不同，規則是明確而依歸於空間中的具體場所，符碼卻是隱晦的潛藏在每一次數值定義的決定以及資訊的數值化過程與回饋過程之中。此一回饋過程有時能夠被個體所知悉，有時會不經過通知便被處理完畢，端視掌握了數據化的定義機制者以及具有連接數據之權限(或者說，通行口令)者之決定。個體在普遍能夠接收數據的社會環境之中，會根據所獲得的這些數據化的資訊反饋調整自己的行為，但此一反饋的來源可以是多樣化的、隱晦的甚至是乾脆被隱藏起來避免個體產生反饋的[142]。

新型態的監視技術能夠對應到「警戒」型的風險處理。此種風險處理的目標，是篩選出潛在的危險因子，並且在事前擊潰危險因子。如同許多政府所宣揚的口號一般，藉由事前防犯以換取安心、安全的社會。但實際上，採取這樣的行動代表政策施行者「迴避」內在的統治，將主體和思想視為行為與機率，

[141] Gilles Deleuze，前揭註 137，p.5。

[142] 原因可能在於調控或編碼所需。具體例子例如秘密進行的通訊監察必須避免讓收集對象知悉、消費偏好的收集最好避免個體知悉後導致收集到的消費偏好失真等。

doi:10.6342/NTU201900452

以犯罪的徵兆與可能性取代犯罪的成因與虛無的自由意志。如果風險因素決定一個人是否會在特定情境之下犯罪，則近代刑法對於自由意志與理性的預設便是一片虛無。如果犯罪的可能性能夠且應該藉由演算法得出，演算法藉由風險與偏差行為的預估作為素材，以程式或 AI 進行運算，經過危險評估的犯罪者似乎就只能被定位為系統中不應該存在的 bug。但不同於電腦中的程式碼依循著數字與規律進行，現實中所進行的編碼雖然仍依賴著電腦技術，其**編碼的過程與依循的規律卻具有著不確定性，而具體的內容通常也不是受編碼支配者所能得知[143]。**對於編碼的控制者而言，最優良的演算法過程應當如同一個完整但計算過程不透明的函數，僅需要知道投入何種因子產生何種結果，對於演算法本身之運作則無須加以理解。如此一來只需要**透過因子與結果的調控，便能夠輕鬆達成控制社會的目標。**在難以描繪模範人類形象的社會之中，這樣的作法會成為較有效率統治社會的手段。因為**與其透過教育教化每個國民的精神與思想，不如直接以監控與差別待遇的方式掌握人民的行動進而規制其逸脫行為。**而事實上，也有國家已經開始試驗類似的政策，藉由網路與身體裝置達成的完全控制結構，似乎已經逐漸轉變為現實。

中國的社會信用點數評分制度即為一個嘗試的例子。這也是與本文在後續章節希望討論的一種虛構系統類似的模型。亦即**以安全作為目的，以監視技術作為基礎，以風險因素的設定做為危險因子之定義標準，以預測未來可能性作為運作方式，以演算法所得結果作為差別待遇基準之系統。**社會信用點數制度在許多方面類似於此系統的模型。尤其與監視理論重疊的部分便是「對個人資料的收集，以及以此為基礎進行的演算與差別待遇。」這一連串的過程正符合本章節所處理的，自規訓社會轉向控制社會時所依賴的 code 與 password 此一過程。對於介面與輸出進行的調控在社會信用點數評分之中所表現的型式，則是在社會福利的支給、大眾交通運輸工具的使用等方面。系統的設計上並不需要強迫個體採取何種行動，只需要**對特定因子給予不利益，並且對特定因子給予優待即可。個體藉由遵守特定因子，迴避其他因子，以試圖在介面與介面之中取得更好的待遇，並且追求「體制之內的幸福[144]」。**

從規訓社會往控制社會轉變的過程之中，規範似乎逐漸消融在數據與編碼

[143] 受編碼支配者僅能知道甚麼行為可能帶來甚麼後果，亦即何種因子丟入演算法之後會出現何種運算結果，對於背後的價值觀以及系統運作方式皆無法從演算法之結果中理解。

[144] 如果以一種戲謔的說法來說，體制之外的幸福，將會成為邪惡的因子。因此個體應當成為體制內的良民。此時監視技術可以用來篩選每個個體所具備的善良因子與邪惡因子，當然何為善良何為邪惡就交給「Big Brother」來決定。

doi:10.6342/NTU201900452

之中。與其使每一個個體認知規則、關注自我以追求善[145]，不如直接以收集資料進行風險預測以及編碼的方式對個體進行調整，並且藉由結構的設計來使得個體在「有限的自由意志」之下進行系統所允許的選擇。當然此時發展生活風格(life style)的潛在可能性便被消磨殆盡，因為這些潛在可能性通常難以在系統的範圍之中存在。

第四章 法律的論述與對抗

第一節 個人資料的保護

第一項 概論

本文的研究脈絡試圖要分析監視社會中監視技術的更新與社會控制的連結，而法律是否能夠成為對抗監視社會的其中一種可能性，便成為問題。在前面的章節所提及的數據化控制社會以及大數據、監視社會的浪潮之中，就法律作為其中一種對抗的工具成效如何、法學者對於隱私權與資料收集問題，以及所採取的對抗監視社會之手法等等問題，以下先進行簡單的整理。

監視技術與被監視的對象最直接的關聯，經常來自於個人資料的收集與使用。如同前面章節所提到的，監視技術與資料處理的技術持續發展的狀況下，個人資料的收集與使用門檻持續降低，而監視技術之中除了視線的存在之外，另一個角度即是**對於資訊人格的穿透。**因此許多針對監視進行的抵抗論述會從個人資料保護的角度著手，使用「隱私權」、「被遺忘的自由」等論述作為對抗的手段。亦即以強化個人資料的保護來對抗「監視社會」的意象以及監視者所試圖進行的控制，同時將「人格發展自由」與監視技術進行連結，認為生活在被監視的狀況之下會難以自由的發展個人的生活風格。

因此針對監視社會持續發展的現況，法學家在許多面向提出措施加以對抗，試圖在民主與法治的框架之下面對監視的目光。以我國來說，在憲法層面上，隱私權的地位持續深化，除了釋字 585 號賦予其基本權地位之外，釋字 689 號亦明確將使用科技與監控設備可能造成的侵害納入隱私權此一重要基本

[145] 不可諱言的是，針對真理或者說善進行設定本身已然存在「預設定義」之風險，權力的壓迫極有可能自行定義自身後在真理之名下正當化自身。迴避此一問題的方法便是訴諸「對自我的認知」以及「成就生活風格的潛在可能性」兩個概念。亦即，雖不定義善，但保障每個人均能藉由自我關注以認知自我，並且均保障個體追求善的潛在可能性。

doi:10.6342/NTU201900452

權的範圍之中。但須注意的是，雖然隱私權已上升到基本權之高度，對此一基本權之保護亦非絕對，如釋字 603 號即表明仍得在必要之情況下依憲法第 23 條對資訊隱私權做出限制。除此之外亦可參照歐盟所推行之 OECD 個人資料保護原則導出**以「告知、同意」為核心的個人資料保護建置**。在近期發展上，為了對應這些個人資料的收集所可能導致的風險，歐盟正在推行一般資料保護規定(GDPR)，我國也正在進行資通安全管理法草案及相關子法的研議。以 GDPR 為例，其核心重點在於使個人資料的用途、收集範圍等等公開透明化，並且要求處理個人資料的組織訂定作業流程，並且加強處理這些資料時的資訊安全，違者則處以巨額罰款，藉此試圖提高歐盟成員的個人資料安全。本文認為其所昭示的方向即公開透明、資訊安全控管等等，固然符合隱私權之價值，亦值得肯定。但實際上，GDPR 的規定的出現也**代表了監控與針對個人的資料收集已經滲透到社會的各個領域之中，實際上已經難以阻止資料的收集，而似乎只能試圖從監視系統的後端(即資料保存、使用等方面)進行管控。**

個人資料收集與監視社會的構成，不再只有國家政府能參與。銀行、電信業者、社群軟體、社交與購物網站、網路服務供應商等等群體亦都構成監視社會的一環，且早已融入資訊社會的生活之中，而形成了另類的「Big Brother」。不同的點在於，「Big Brother」的意象是獨裁而極權的，但**近代監視社會中的組織經常以一種有利於大眾的、柔軟的形態出現[146]。**並且其中有些服務確實透過個人資料的收集以及對於用戶使用習慣的監視而提供許多便利的服務。本文認為，GDPR 制度的推行或許能夠在個人資料的收集此一領域中起到一定的嚇阻與使得監視機制公開透明化的效果，但其他的監視技術領域是否能夠同樣以法制化[147]的方式，以類似的作業準則來進行公開透明化的作業，則有許多待解決的課題。例如涉及刑事偵查時，警方針對監視器所收集的畫面如何分析使用、法官進行量刑調查時對於被告的個人資料收集、福利政策層面的監視問題、甚

[146] 需注意的是，從 Haggerty 的聚合體概念與 Deleuze 對於控制社會中的 code 與 password 等概念之詮釋來看，在資訊社會之中掌握數據編譯權限以及網路底層協議傳輸過程的這些組織，其所能達成的控制未必真的少於「Big Brother」。而其所能控制的範圍，隨著社會功能逐漸資訊化，更加地擴展。舉例來說，假設薪資、稅賦、社會保險、福利給付等基本的福利國家功能均依賴資訊設備以儲存、紀錄、使用，那掌握了收集資訊權限與通行口令權限者其所能達成的控制便更加深入。

[147]除了以法律制度化進行抵抗之外，另外一個可能性，則是區塊鏈技術的引入。區塊鏈技術最重要的特點，是其採取去中心化的儲存資料方式來建立資料庫。由於資料分散儲存在各個訊息節點，採用這種技術儲存的個人資料可以降低資訊被集中儲存導致的風險，且區塊鏈難以被特定組織或團體所掌握，或許將成為反制監視浪潮的重要工具。但不可否認的是，區塊鏈技術仍在發展中，能否在個人資料的管理上應用，尚有許多疑問有待解決。

doi:10.6342/NTU201900452

至是人臉辨識系統的應用等等。以下先處理法律針對個人資料收集部分主要使用的隱私權論述以及具體應用時所採取的制度。

第二項 取得面向控制

試圖對個人資料進行保護時，首先被法學者考慮到的是針對資料取得面向進行的法律管制[148]。以我國來說，大法官釋字 585 號解釋明文將「個人資料之自主控制」納入憲法第二十二條隱私權之保障範疇中。釋字 603 號進一步闡明，個人自主控制個人資料之資訊隱私權之內涵旨在「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。」在此脈絡發展下，資訊隱私權之保障係以「告知、同意」作為保障核心。亦及，在收集個人資料的時候，原則上必須告知其個人資料可能之用途，並且取得「真摯之同意」，此權利即為個人資料自主權。

個人資料自主權在實踐有以下的困難[149]，其一是當事人無意義的同意。此問題的原因來自於當事人對於個人資料使用條款內容的不了解，以及個人資料提供與特定服務的綁定。例如智慧型手機中 APP 的使用、網路服務供應商對瀏覽紀錄進行的收集等等。其二是隱私與社會利益之間的取捨問題，以及利用資料對個體來說可以帶來的好處。除了在醫療、教育方面的個人資料使用之外，在犯罪偵查領域，個人資料的收集與使用也經常能夠協助犯罪的預防與偵查。在這些利益的支撐以及適當的法律授權之下，繞過個人的同意進行資料收集之情形亦屬常見[150]。為了因應這些當事人資料自主權資料實踐上的困難，歐盟便透過一般資料保護規定(GDPR)之規定強化對於資料取得面向之控制。歐盟模式具體之內容為:1.**當事人同意的強化**，必須要是「任何特定且經告知後的自主表示，表明資料主體同意使用其個人資料。」2.**告知事項的擴張與圖形化標準資訊政策**，藉由將告知事項擴大以及將使用資料之範圍與風險以圖形表達之方式確保當事人知悉自己的資料將被如何使用。3.**對大數據與物聯網的妥協**(資料最小化儲存原則的放寬、科學研究目的資料儲存的放寬、合法收集資料的放寬、資料假名化、去識別化[151]等等。) 論者認為[152]，歐盟個資命令雖然仍秉持著以

[148] 劉定基(2017)，〈大數據與物聯網時代的個人資料自主權〉，《憲政時代》，第 42 卷第 3 期，頁 274。比較法與個人資料自主權之緣起則可參照頁 270 以下之整理。

[149] 劉定基，前揭註 148，頁 274-279。

[150] 最為明顯的例子即是在通訊保障及監察法授權之下所進行的通訊偵查。

[151] 此一發展在監視影像的處理上亦有類似的系統被提出，即透過程式的處理，將被附帶拍攝到監視影像中的第三人加以隱藏或模糊化，並且搭配解碼權限之限定與紀錄之方式避免對於被附帶拍攝到影像中的第三人其隱私權造成侵害。另可參考前揭註 33、38 之文獻。

[152] 劉定基，前揭註 148，頁 288。

doi:10.6342/NTU201900452

個人資料自主權為基礎架構之法律體系，甚至在個資命令中進一步強化了作為個人自主權基石的「當事人同意」定義並且擴大告知事項等，試圖回應自主權在實踐上的種種困難，但也在大數據的浪潮之下在個人資料保存期限、利用墓地等方面作出了妥協。在許多例外狀況以及法律授權的資料收集可能性之下，當事人資料自主權的保障究竟是否能夠落實尚有待觀察。

第三項 使用面向控制

針對資料取得進行管制之方向，在資訊社會中面臨前所提及的諸多困難。因此有論者認為應該轉向解決較有可能實際對資料提供者產生侵害的資料使用問題。在資訊社會之中，個人的資訊隨時隨地被收集或者被洩漏，試圖強化使用者自主的意義並且從源頭管制資料取得的手法，反而有可能導致管制目標均集中在「同意的有效性」以及「告知事項是否明確」等等細節上。而這些針對「資料的取得」所進行的管控，在許多的狀況下會成為虛無飄渺的管制措施，因為資料的收集在實務上幾乎都是合法而正當的原因。而真正的問題應該是資料的傳輸與使用遠遠脫離了當事人所能控制的範圍，且許多資料最終的應用狀況早已超出了收集當時所預設的應用範圍。因此與其將資源耗費在通常難以阻擋的資料收集階段，不如將重點擺在資料使用面向上的控制[153]。

使用控制與風險評估之新模式，其目標在於重視「資料使用」的環節，而對於蒐集資料的同意與否以及同意有效性之認定則放寬檢驗的標準。接著以資料外洩所造成之損害風險評估來取代資料自主權的地位。亦即關注的重點，是著重在評估個人資料的洩漏究竟對於當事人可能造成何等之損害，以及資料的使用是否可能對當事人之人格發展自由造成傷害。若資料的使用確實對當事人有害，使用這些資料取得的利益又是否能夠在憲法與法律的要求之下通過利益衡量。亦即不再針對資料之取得進行控管，而是集中在後續對於資料之使用是否超出當事人授權範圍，以及是否對當事人造成損害等部分。

採用此一模式的優點在於將關注的焦點集中在較有可能直接對當事人帶來不利益的資料使用面向，迴避掉使用者無效同意與不謹慎同意的問題，並且藉由確實進行利益衡量來有效達成管制資料使用之目的。如同論者所說，採用此一取向進行管制確實較單純針對資料取得部分之管制來得有實行可能性，但若結合本文前述監視社會之現況看來，資料持續蓄積以及多重資料交互使用之後所可能造成的損害是否能夠單純以法律加以對抗，便有可能產生疑問。最主要的問題仍然會回到「位於虛擬空間之資料收集與儲存」與「資料收集客體」之

153 劉定基，前揭註 148，頁 290。

doi:10.6342/NTU201900452

間的距離問題。

第四項 極限

不論採取何種面向作為法律面對監視社會中個人資料收集問題之解決手法，問題仍然在於最終的實踐層面。使用面向控制針對的階段主要在資料已經被收集、蓄積在資料庫之後的使用。對於在資料庫中被保存的資料則以防止外洩做為主要的應對方式，而無法阻止資料被收集。而受限於資料庫難以接觸的性質，藉由法律進行規定作為解決的手法，固然能夠在某種程度上控制住資料的流動。但電腦資料庫本身以及收集資料的行為與法律、資料被收集的客體之距離等特性，皆由於虛擬空間之存在性質而產生了兩個特殊的現象。即資料收集的簡便易行，以及資料使用的不透明。具體來說，資料庫端可以輕鬆連接到負責資料收集的終端，但是不具有連接資料庫權限的人要連接到資料庫卻十分困難。即便在使用面向上要求資料收集者必須要透明公開，一般人仍然難以理解構築資料庫的程式碼，亦無法自行連接到儲存個人資料的資料庫。要完全阻止處在虛擬空間中的資料不洩漏或被移作他用似乎不太可能。且實際上即使採用同意面向的手法嚴格要求告知與真摯同意，資料提供者有時仍然無法預測到大量資料被儲存、分析、利用之後可能帶來的結果。

另一個問題是，以法律來做為對於監視的限制，事實上亦是從另外一個角度強化了監視結構的穩固，處於法律控制之下的監視技術與個人資料收集得以在此一框架之下發展，並且取得正當性。當然在現代國家體系之下，個人如果要在社會生活，自然無法避免隱私權的部分放棄。且大部分情況下由國家所發動的監視並不會以特定個人為目標，由企業所發動的監視則未必會對個人造成損害，因此對於一般群眾來說以有限的個人隱私之犧牲換取國家福利之提供、更安定之社會控制、有利於個體之服務等等狀況似乎並非不能接受。但於此仍需要注意的是這些資料的蓄積背後所隱藏的危險性。亦即，資料在不被使用的時候看似無害，一旦將散布各地的資料組合起來之後搭配演算法與差別待遇之手法，將有可能創造出無法抵擋之控制系統。中國大陸於新疆所採行之社會控制實驗以及社會信用評點制度即是現今值得觀察之標的。其最終內藏的危險，誠如 Deleuze 所言，仍是在於對於 code 與 password 之控制。不論是將個體排除於系統之外，或是對個體進行差別待遇，均有可能對個體帶來嚴重的損害。

第二節 犯罪控制與結構論

doi:10.6342/NTU201900452

第一項 規範意義的轉變

第一款 刑事政策與犯罪控制的觀點轉變

Lessig 認為制約人的行動的四種手段是法規範、社會規範、市場、結構。而這幾種不同規範手段相互之間的作用便決定了規制的最終效果[154]。以法規範來說，在罪刑法定主義之想法出現之後，對於犯罪的想像亦開始與法規範相連結，並且將自由意志、理性與懲罰之預設作為對於犯罪者與犯罪行為之回應。但此一將犯罪者與法規範、自由意志、理性預設等因素掛鉤的想像，在刑事政策與犯罪控制近代的觀點轉變之下有所變化。

近代刑事政策學者經常這樣描述近代的刑事政策:「從以包攝與結合為基調的社會轉移到以分離與排除為基調的社會[155]。」此即包攝結合/分離排除模型。亦即刑事政策的本質在於如何回應犯罪行為，針對犯罪者所採取的路徑則可以拆分為將犯罪者重新接納回社會的路徑，以及將犯罪者分離排除於社會之外的路徑此兩種角度進行觀察。而從包攝到排除的轉換，則可以從刑事政策各時期思想的發展歷程中觀察到。以下先簡述各時期出現的觀點轉變，再說明監視技術做為技術手段以及結構此兩種不同角色在各個時期中產生的相互作用。

1.應報路徑[156]

犯罪被視為惡害，為了對應此一惡害必須加以懲罰。此一路徑對應到古典刑法的應報思想，而在近代加入了對犯罪者理性意志的要求，因此不再單純以懲罰對應犯罪的惡害。

2.矯正路徑

此一路徑又被稱為醫療模式。將犯罪現象視為個人的疾病，並且以矯正犯罪者、使其順利的回歸社會做為目標。具體的手段有藉由刑罰達成的教育、社會內處遇、治療等方式。

---

154 松尾 陽(2017)，「法とアーキテクチャ」研究のインターフェース—代替性・正当性・正統性という三つの課題，載於松尾 陽(編)，《アーキテクチャと法：法学のアーキテクチュアルな転回？》，頁 11-12，弘文堂。

155 此概念主要由 Jock Young 加以發展，參見松尾 陽(2013)，防犯アーキペラゴ序説—包摂と排除の交錯とはざま—，載於仲正 昌樹(編)，《「法」における「主体」の問題》，頁 88-89，御茶の水書房。之整理。在此一轉變的過程中，以病理、醫療模式理解作為基礎的新古典犯罪學派逐漸式微，社會對於犯罪者所採取的態度也轉向以排斥為主流想法。

156 以下路徑之內容整理自松尾 陽，前揭註 155，頁 90-91。

doi:10.6342/NTU201900452

3.構造路徑
此一路徑將犯罪視為社會構造的疾病，而這些疾病是因貧困導致的結構問題、教育制度的失敗等等原因引起的現象。因此處理犯罪的方法應該是將這些社會構造的因素排除，例如充實社會保險制度以及完善教育體制等。

4.排除路徑
此一路徑以從社會中排除犯罪的危險因子為目標。亦即特定出未來可能有犯罪危險的個體，並且將這些個體從社會中隔離。

5.環境路徑
此一路徑以減少誘發犯罪的環境為目標，以構築可能對犯罪之實行造成妨害之環境等方法來預防犯罪[157]。並連結到本文前面章節所分析的環境犯罪學理論以及後面將提到的結構論問題。

近代犯罪學與刑事政策對於犯罪之理解，經常綜合採取上述路徑的想法。以大略的方法進行分類的話，可以將矯正與構造路徑分類為「包攝型社會」，將應報、排除、環境路徑分類為「排除型社會」。前面提及的從「包攝型社會」轉換到「排除型社會」的描述，便是從此一歷程的發展特徵中觀察得出。此一轉換的原因可能在於人民的「對於安全、安心的欲求」。七零年代以來，刑事政策幾個重要的轉折點如下。首先環境路徑隨著環境犯罪學的發展逐漸抬頭，應報路徑下的懲罰要求逐漸再生，治療與矯正路徑逐漸衰退，轉為以自社會中排除犯罪者為核心。處罰的早期化及嚴罰化在對於安全的要求之下逐漸被認可，被害者學在刑事政策中逐漸佔有一席之地等等[158]。本文認為從這些趨勢看來，似乎揭示了為了追求社會的安全而「排除犯罪者」這一核心思想，逐漸取代了以往以使犯罪者回歸社會做為目標的政策取向。

在此背景下論者在這裡進一步將這些犯罪學路徑區分為犯罪原因論與犯罪機會論兩個類型。其內容如下：犯罪原因論試圖從結構、矯治構造來對犯罪原因進行治療，犯罪機會論則以消滅犯罪的機會與風險做為防止犯罪的手法。其中結構與矯治路徑或者說犯罪原因論的發展，主要起因於福利國家的制度構成之中。福利國家的機制雖然內藏著確保勞動力與軍事力的機能，但其設定的理想仍然是全體市民的權利實質平等之實踐。在此目標之下，除了藉由社會福利

[157] 具體方法例如日本於 2003 年犯罪對策內閣會議所提出的「犯罪に強い社会の実現のための行動計画」、各地方自治團體制定的「安全、安心まちづくり条例」等，其政策目標在於直接的、間接的以調整環境之方式妨礙犯罪的實行。

[158] 松尾 陽，前揭註 155，頁 88。

doi:10.6342/NTU201900452

的給付來減少貧富差距之外，同時為了確保稅收與勞動力的來源，因此必須要建立人與人之間的社會連帶。因此可以說在福利國家之中，社會的包攝(亦即社會連帶的重新建立)被作為其設定的理想。因此矯正路徑試圖將犯罪者與犯罪行動連結的因子加以特定，並且以摘除此一因子之方式，重新將犯罪者包攝回由不具有這些犯罪因子的正常人所構成的社會之中，此一手法便可以被劃分到包攝模型中[159]。

構造路徑則藉由社會保護網的構築，以解決經常被認為是犯罪原因的貧窮問題，並藉此試圖將貧窮者與富有者統合在福利社會之中。將這些犯罪原因論觀點下的路徑與福利國家連結起來的概念，則被稱為刑罰福利主義。相對於此，排除型社會通常是價值觀已經多樣化發展的社會，在此類社會之中正常與異常的區別已經變得曖昧不清，取而代之的是社會行動與「風險」概念的結合[160]，此時的課題則是刑事政策如何應對日常生活行為所潛藏的風險[161]，例如破窗理論與零容忍政策、三振法案等等皆是對應到排除型社會的政策。這些政策注重在環境的調控、入監獄服刑人數的提高、增加排除於社會之外的人數等方向，因此可以將這些政策所依循的排除路徑與環境路徑等納入排除型社會之中。在這兩個較為簡單的二分概念[162]之下，本文接著試圖分析「排除」之概念與新形態監視作為環境結構以及作為排除手法的兩種可能性。

第二款 結構與監視技術做為犯罪的影響因素

近代的監視社會之中，犯罪被視為風險，且能夠透過監視技術達成一定的

159 松尾 陽，前揭註 155，頁 92。

160 主要原因在於多樣化的價值體系、生產模式逐漸脫離對勞力的依賴、居住環境轉變為都市、個體與個體之間的社會連帶變為薄弱等因素影響。在近代社會之中，較難找到如同神權、軍權時期呈現的對於真理與善的單一理解，也因此產生了對於行為之判斷轉而以機率與風險加以量化的想法。

161 整理自松尾 陽，前揭註 155，頁 93。

162 論者指出事實上包攝與排除路徑之間有許多模糊的地帶存在，例如針對環境的設計來使得有意圖進行犯罪者受到阻礙，看似是排除掉具犯罪風險者，但也可以看做是包攝不會受到這些結構影響的「善良的市民」。針對犯罪原因論的論述看似是試圖將犯罪者包攝回社會之中，但也可以解釋為忽視掉了「犯罪作為日常生活的延長」此一性質，而在理想的個人形象之下排除掉現實的個人。因為瘋狂與正常的界線，並不是理性的預設所能夠切分。日常生活與犯罪的距離並不如一般人所想像的遙遠。最終應該要注意的，是包攝與排除中間存在的間隙如何分配，以及刑事政策在這之中的調控如何進行。參照松尾 陽，前揭註 155，頁 95 以下。

doi:10.6342/NTU201900452

控制。此時犯罪者是否有理性意志並非考量的重點。對於社會來說有害/有利才是觀測的重心。監視技術在刑事政策與犯罪領域中扮演的角色主要有二。首先，依照 Lyon 所提出的 social sorting 概念來看，監視技術本身能夠有效做為對人口進行控制以及分類的輔助技術。監視影像中出現的偏差行為，會使得被監視的對象被貼上偏差者之標籤。此即前述監視帶來的其中一種分類效用，以及對於未來危險之評估作用。另一方面監視系統的設置本身將成為存在於社會中的結構，對於其所監視的對象所進行之自我決定以及行為將有可能產生影響，同時監視技術與所得到的資料亦能作為是否對個體進行差別待遇的區分基準。需釐清的是，欲影響對象的自我決定一般而言必須要使對象認知到監視系統的存在，具體的模型例如前述圓形監獄概念所揭示的，藉由監視視線之創造進而影響個體自我決定的運作方式。但監視視線作為結構的另一個運作方式，則是使得對象在潛意識中決定採取何種行動，亦即與環境犯罪學路徑與結構論之連結。

監視技術作為能夠與各種領域交錯的手法，與「結構」的概念密切相關。結構的設計在社會中一直有重要的意義，而自圓形監獄的模型中結構與控制手法的結合被明確的描寫出來之後，控制之目標與結構設計的關聯亦更加凸顯。結構論(architecture)原本是從資訊社會的發展之中衍生的新概念，其作為構成資訊領域的底層基本結構，有可能藉由對其所進行的設計與調節，在不透明的狀況下制約個人的自由。除了傳統意義上以物理結構進行的控制之外，資訊社會之中構成虛擬空間的程式碼編碼(CODE[163])問題也被提出。在結構論的想法之中，技術、物理的結構、虛擬空間的底層編碼，會如同自然環境一般影響個體的自我決定。

但與自然環境不同的是，人為的結構具有被創設、被調整的可能，並且能夠影響到個體的自由意志，這也是環境犯罪學路徑所用以說明其應對犯罪策略之基礎。而能夠作為結構的一種類型看待的「技術」，亦非單純供人類使用的道具而已。此時人與這些技術的關係產生了改變，但法律的設定卻未必能夠及時的與之對應。論者並指出「**許多人的直觀的認為……，技術僅只是用以補足我們的實存之單純中立性質之道具，……技術會形成我們的行為以及世界經驗，並且以此一方式與我們生活的型式主動的有所關聯**[164]。」例如車輛對於生活範圍的擴展、電話與網路對於通訊範圍的擴張，建築結構的設計以及可視性的創造等等。這些對於結構進行的設計以及技術的發展，事實上影響了個體在這些

[163] 此處的 code 並非德勒茲在闡述控制社會時所使用的符碼概念，而是用以描述組成虛擬空間基盤的程式碼。當然兩者之間在概念上仍有相通之處。

[164] 稻谷龍彥(2017)，〈技術の道徳化と刑事法規制〉，載於松尾 陽(編)，《アーキテクチャと法：法学のアーキテクチュアルな転回？》，頁 94，弘文堂。翻譯為筆者自行翻譯。

doi:10.6342/NTU201900452

結構之中基於其自由意志所進行的決定。論者在此指出一個道德上的難題，亦即超音波對於母體內胎兒狀態的判定問題，以說明自由意志必然受到環境以及構成環境的技術影響之狀況。「若將自由意志與自律性作為人類的本質的話，並且以只有人類能成為道德評價對象的人類中心主義作為準據的話，對於此種超音波檢查儀器的評價便變得十分困難。因為如果以技術為基礎的人工物成為了引導人類判斷的準據的話，此時之判斷早已不是基於自由意志的自律判斷了[165]。」當然，對於此一說法仍可做出反論，因為若認為人能依照自由意志進行理性判斷，此時的理性判斷仍須依賴感官對於自然環境的接收與反饋作為理性判斷之基礎。此時究竟賴以判斷之基礎究竟是自然環境或是人工技術，並非重點。重點是自由意志在這之中究竟扮演多種要的角色。若從此一想法延伸，在結構與技術的影響之下自由意志究竟還殘餘下多少，自律性此時存不存在，便是需要釐清的問題。論者進一步指出，此時對自律性存在的多寡若欲進行規範評價，「由於人類並不存在一種本質，基於正確人類形象所進行的道德評價，最終僅僅剩下要求一個標準化的人類形象存在之意義而已，並不具有其他的意義[166]。」亦即，要求一個正確的人類形象存在，其實最終都會變成特定價值觀的再次創設甚至壓迫，事實上難以藉此真正取得一個良善、正確的人類形象。

本文認為在結論上來說，必須要承認的點是人類在本質上是可塑的，可以接受環境影響，並且具有有限的自律性。僅僅由腦海中的思考所構成的絕對理性無法存在，我們的感官以及基於這些感官所形成的存在方式極有可能因為與事物、技術的關聯而產生改變。連結到環境犯罪學的想法而言，便能藉此以結構設計之方式或者對環境進行調控之方式影響犯罪者的自由意志進而防止犯罪發生。在環境能夠影響人類決定的前提下，基於此設定出法益、安全、社會利益、危險等等概念並且以環境調整的方式對試圖對個體加諸影響。此一方式能夠結合監視技術與個人資料收集等等手法，更加深入的控制風險的發生。亦即，藉由前述對法益、安全等定義之創設，導出一個完美的良善人形象之後，藉由監視技術的收集時刻檢查社會中的個體是否符合此一形象，並且對不符合

[165] 稻谷龍彥，前揭註 164，頁 99。翻譯為筆者自行翻譯。對於胎兒狀態的判定，依循肉眼並無法達成，勢必需要透過超音波儀器此一技術。因此對於胎兒狀況的判斷事實上無法直接純由人類的自由意志達成，而必然受到技術的介入。本文認為論者在此的主張是認為絕對理性與完全的自由意志並不存在，人在進行判斷時必然是會受到環境影響的生物。

[166] 對於理性的預設不得不受到環境因素以及結構、技術因素的汙染，因此實在難以存在。此時所謂的自律性，充其量僅只是論述者心中所建立的一個標準化的理想人類形象。此時由被標準化的人類所構成的，沒有摩擦，不存在自律性也不存在創造性的「透明的社群」問題便產生。此一問題由 Foucault 指摘，此時所謂的自律性其實僅只是與理想人類形象所進行的對比而已。所謂的社群也只是個體試著往人類形象不停地切割、鎔鑄自身。詳細可參照稻谷龍彥，前揭註 164，頁 100。翻譯為筆者自行翻譯。

doi:10.6342/NTU201900452

該形象的個體加以差別待遇，以此確保所謂的社會利益。正如同日本內閣府的政策構想，藉由更加全面的監視，在偏差行為發生之前便加以阻止。但若以此預設作為刑法介入、或者刑事政策介入之基礎，將有可能在不知不覺中將既存的社會秩序無意識的轉換為「良善的社會秩序」並且強制加諸在個體之上，又由於刑罰的嚴重性使得此一手法造成的影響特別的劇烈，因此具有極大的破壞自由意志前提之風險。此時個體將被迫依照此一良善社會秩序生活。這一點在監視技術對於危險因素的預測之中亦有可類比之處。這一論述並不代表防治犯罪的想法有錯誤，而是從個體所具有的「潛在可能性」之觀點切入。設定「危險」概念之後，實踐這些危險的犯罪之行為固然對於社會有害，且必須要加以應對，但如果應對的方式是抹消掉存在於有限的自由意志與自律性中存在的潛在可能性，則此一應對方式將與「自律」、「共生」之社會漸行漸遠。

第三款 以安全為絕對價值的政策可能性

基於本文至今所進行的監視社會相關之論述，或許可以設定一個虛構的政策系統作為供檢討的對象。亦即以**安全作為目的**[167]**，以監視技術作為基礎，以風險因素的設定做為危險因子之定義標準，以預測未來可能性作為運作方式，以演算法所得結果作為差別待遇基準，並且試圖在事前預防風險發生之系統**。此一系統的每一步驟在監視社會之理論上與技術上均有達成之可能，並且能夠用以作為預防犯罪的一種備選政策[168]。在此種政策的實行之中，只要危險因子的設定足夠準確，便有可能藉助於資訊設備達成完全的控制，並且有助於達成防止犯罪發生的目標。日本內閣所提出的「イノベーション２５[169]」此一戰略

[167] 當然亦有可能潛藏統治、優生、勞動力確保、人口管理、經濟考量等等多樣化目的。

[168] 例如於我國縣市首長選舉中曾經被提出作為政見的政策，國民黨籍台北市長候選人丁守中今（13）日舉辦婦幼安全記者會，會中提出運用大數據、GIS 資料庫算出犯罪熱點及模式，加強設置數位監視器、警力巡邏，及見警率，用智慧科技打擊犯罪。不過因丁守中表示獨居、人際關係差、失業、單身男子易犯罪，應有效監測並加強查訪，此舉言論亦被人質疑是否歧視單身男性，對此丁守中強調這不是歧視，只是反應數據資料。新聞內容節錄自台灣好新聞 (2018.08.13)，〈丁守中：獨居、人際關係差、失業、單身男子易犯罪　應有效監測、加強查訪〉，http://www.taiwanhot.net/?p=611865，最後瀏覽日期 2019.01.11。該政策所設定之目標，即是將單身、獨居、失業男子設定為危險因子，並且試圖推動更完全覆蓋公共空間的監視配置，預測這些標的未來的犯罪危險性，並且以大數據統計與風險預測作為正當性基礎之系統。

[169] 詳細內容在本文研究動機部分有簡略提及，另可參照日本內閣府官方網頁，イノベーション２５之說明，取自：https://www.cao.go.jp/innovation/，最後瀏覽日期 2019.01.11。具體來說，最

doi:10.6342/NTU201900452

構想中，亦使用了類似的概念，亦即透過對於偏差行為的定義以及監控與身體裝置所進行的事前預測，試圖扼殺犯罪風險於無形。在技術層面來說，若能夠設置足夠多的身體裝置，以及在公共場所建置足夠完備且與網際網路連線之監視網路，在搭配影像辨識技術與危險源預測技術的情況下，完全有可能建置出類似的系統。且中國大陸政府亦已經在新疆進行類似的政策試行[170]。

此一想像中的系統，**固然有可能藉由監視技術的完備，辨識出所謂的「危險個體」，並且在風險實現之前及早採取行動以避免損害發生。**但其所存在的危險性正如同許多監視理論的學者所指出，**在於危險因子設定與演算法之間可能產生的落差，以及對於自由意志與潛在可能性的剝奪。**首先在定義危險因子的部分，以本文註 151 中所提及的政策為例，此一政策所瞄準的對象(獨居、人際關係差、失業、單身男子)正暴露出了對於所謂「高風險犯罪因子」定義的困難，**即便在大量的數據支撐之下，一個人無論有著怎樣的特質，其未來是否會犯罪仍然是未知數。**如若將對於行為的未來選擇，化約成犯罪的風險與機率，並且藉此作為訪查甚至加以實行監控的正當化理由，毋寧是否定了這些人對於未來進行選擇的潛在可能性。而風險因子的定義也代表了「排除型社會」之傾向，**監視技術在此時會成為用以進行差別待遇的有力工具。亦即，設定了「優良市民」標準之後，以大量的監視技術分辨出不符合優良市民定義之個體，並且將其貼上風險標籤並且進行未來預測以作為差別待遇之正當化理由。**在這一連串過程之中，定義被創制，演算法被掩蓋，差別待遇的正當化標準被訴諸於「數據的完備與系統的準確性」。此一作法其實便是將「Big Brother」的意象換上「社會安全」的外皮，重新發展出全面的監視社會。

本文認為，若社會共識已然清楚理解到監視技術內藏的風險以及潛在可能性被抹滅所帶來的意義，則選擇此類型控制政策作為社會安全調控的方法亦無可厚非。但此類控制政策極可能成為人格自由之發展停滯以及民主社會崩潰之開端，而社會安全是否值得犧牲這些代價換取，亦有待商榷。

第二項 安全與隱私

第一款 安全與隱私

值得注意的是在「伊野辺家の 1 日」中兒童身上裝設的身體裝置與治安防護網路的連線，以及身體裝置與醫療系統的連線這兩個構想，可以從中看出物聯網、監視網路、未來預測等特性。

[170] 此一系統在實行上尚能與其他方面的控制系統進行結合，例如對刀具進行實名化與購買登記、對於個人在網路上的發言進行追蹤以及敏感詞彙偵測等等。

doi:10.6342/NTU201900452

刑事政策的導向逐漸轉向事前的預測與預防。而想要更精確的達成此一目標，有賴於對於社會中各種資料的收集。人民的基本權此時雖然被保障，但此一保障並非絕對，國家仍然可以在一定的條件之下，合法的侵害人民的基本權。在此前提之下，隱私與安全事實上僅僅是天秤兩端的砝碼。甚至對許多國民來說，犧牲掉部分的隱私來換取似乎更能保護社會安全的刑事政策是筆划算的交易。例如在我國道路上廣設的監視器、公共場合中私人設置的監視器、行車紀錄器的普及等趨勢看來便已經呈現出此一傾向。例如經常被用來強化監視行為的抗辯：「不做虧心事不怕鬼上門(I've got nothing to hide) [171]」即是例子之一。此一抗辯普遍存在於針對社會安全之政策輿論之中，通常的說法是只要我不犯法，根本不害怕國家進行監視，因此不如就讓國家監視並且交換來社會的安全。在此一論述之下，個體犧牲部分隱私換來全體社會的安全似乎變得具有足夠的正當性，畢竟對於所謂的「良民」來說並不需要擔心國家的監視之眼。但**此一論述忽略了監視系統創建者所掌握的對危險因子定義之能力，亦忽略了系統與演算法在預測時發生誤判的風險。亦即，選擇以隱私換取安全時，上需要考慮這些誤判危險，以及國家或系統建置者對於「良善」與差別待遇標準的定義。**

自近代的監視理論逐漸發展以來，論者在對抗監視的路徑如同前面所述，經常採取隱私權、人格發展自由、對國家權力的抑制等等觀點切入來做為對抗的論點。如《一九八四》與 Foucault 的全景敞視主義，皆帶有與這些角度有關的譬喻性質。**加上一般民眾「不欲被看見」的隱私權此一基本權的連結，似乎在對抗監視的論理之中具有一定的說服力。**亦即，監視網路與科技，必須要在尊重隱私的前提之下，小心的進行，並且維護每個人民的人格發展。其呈現出的光譜，是將監視帶來的安全、效率對比於個體的隱私、人格發展等權利來進行衡量。**但實際上，監視技術的發展下產生的許多特性，使得此一對立是否能夠繼續作為對抗監視發展的論述產生疑問。**隱私權事實上經常被個體自我放棄、或是為了更重要的利益被犧牲。而這一點與個人資料收集之現況有關。

第二款 監視技術與資料收集

現代監視技術下進行的資料收集狀況，有幾個特點。第一個特點是現代社會下由**其他組織保有資料的普遍狀況以及透過交出個人資料可以為個體帶來的「利益」。**在現代社會之中，由於資訊科技導致的社會運作方式改變，個人事實上無法避免其他組織握有自己的資料。舉例而言，如果要申辦手機門號，必然需要提供個人資料給電信業者。而駕照、納稅、健康保險、國民年金等等制

[171] Solove, Daniel J. (2007), 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy, *San Diego Law Review*, Vol. 44, p. 748-749; *GWU Law School Public Law Research Paper,* No. 289.

doi:10.6342/NTU201900452

度，在建構社會生活的同時，也收集著每個國民的資料。某程度上來說，現代社會的人早已接受了將資料交給其他組織使用的事實。而實際上，這些個人資料的收集與使用也確實在不同的領域提供人民益處，例如醫療病歷的雲端化、網路服務提供者對使用者體驗的優化改善等等。

第二個特點，則是**監視所收集的資料其處理過程的晦暗不明。**如前文提及，網路與電腦技術的發展使得透過監視所收集到的個人資料的整合、編輯、傳播變得十分快速，資料可以以極快的速度在不同的組織之間流動、甚至進行再製以及虛擬人格的描繪。而這些資料的處理過程隱藏在肉眼不可見的以電腦技術與網路為基礎之虛擬空間中。因此，對於人類而言，要使用肉眼來追蹤個人資料的流向十分困難。即便個人也能夠透過資訊設備來連接上網路，但這些資料的處理通常會經過加密，大部分情形下並非個人能夠連接。也因此對於個人資料的流動與外洩的狀況，個人的反應通常不若涉及身體、財產等等標的的犯罪那般明顯。舉例來說，如果一個人走在路上時錢包被搶，此一破壞財產法秩序的行為對於個體、社會來說明顯可見，且亦易於促使個人馬上對其做出追訴的反應。但相對的，個人資料，究竟被儲存在何處，以及是否有逾越授權範圍的使用，對於一般民眾來說通常難以得知，即便各國皆針對個人資料以法律、條約等等規定加以保護，**個人對於自身資料的流向仍然幾乎處在無法干涉的狀態。**如同本文前面所述，資料的流出在當下未必會對個人造成顯著性的損害，在損害難以直接被觀察到的情況下，個人對於個人資料的敏感度經常抱持相對較為漠然的態度。但以提供資訊為代價得來的服務，以及監視器的設置帶來的安全感，卻是相對容易被人類所感知。此時監視系統能夠帶來的好處似乎在衡量上便能掩蓋過其可能存在的風險。

第三個特點，則是**個人經常對於資料收集的意涵不甚了解。**除了強制提供資料給政府的情形以外，其他組織在現行法下若要對個人資料進行收集，仍必須要經過被收集者的同意才能進行。以我國來說，在現行個人資料保護法的要求之下，非政府組織要收集個人資訊便必須要符合該法所訂條件，並且得當事人之明確同意。但實際上這種同意，在網路介面上面呈現的樣態，通常是在申辦特定網站會員、或加入特定網路服務(最明顯的例子以社群網路來說例如 Facebook、Google，以購物網站來說例如 Amazon)時，包含在使用者協議之中。而此類協議通常會加入概括同意收集、使用資料，甚至得交給第三方組織使用之條款。從個人資料保護法的前提來看，這些同意仍然被承認是有效的。當然，使用模糊語句包裝個人資料收集範圍的服務提供者亦屬常見，但相對於以個人資料換取服務後所能取得的利益來說，大部分的群眾在理解到其資料的用途之前，通常不會對這樣的授權有太大的排斥心理。但是這些使用者未必真的明確體認到自己到底授權了哪些資料的使用，即便這些情報收集透過較為「柔軟」的方式進行，仍然無法免除這些個人情報洩漏的危險性。甚至理解用

doi:10.6342/NTU201900452

途之後仍然會為了便利的服務而提供資料。如 Facebook 近年來產生的個人資料外洩爭議、以及中國大陸對微信進行的言論審查等等。另一個特殊的現象，是人們雖然宣稱其重視個人的隱私，但其行動卻很少反應這一點。對於在社會生活過程中散播出去的個人資訊，很少關心其流向、用途，其原因可能在於，資訊的流動並非個人可以直接感知，所造成的侵害也非明顯可見。

弔詭的問題便在這裡產生。我們都承認隱私權對於人格發展的重要性，但隱私權在某一些社會功能需求的推動之下，經常會被個人選擇犧牲。基於隱私、人格發展脈絡而對監視技術進行的批評似乎漸漸失去其力道。例如 Facebook 所帶來的社交、自我表現、社群連繫功能，購物網站帶來的在家購物體驗、搜尋引擎收集資訊的便利性等等，許多人樂於交出個人資料換取這些好處，這本來無可厚非，但卻進一步帶來在「同意」與「福利」之下，資料被濫用的可能性。若真有濫用的情況發生，如果處理個人資料的組織內部選擇隱瞞濫用情況，除非有願意冒風險告發的員工存在，否則幾乎難以被社會所察覺。而這些以柔軟的型態出現的監視系統，相對來說更容易被社會所接受。畢竟提供個人的 GPS 定位資訊給地圖 APP 的供應商，聽起來並沒有「Big Brother」此一在背後控制你的思想與行為這樣的意象可怕。這一點便是本文所說的，監視與資料收集的「柔軟」態樣。當然，**在國家系統中，監視與資料收集便不一定需要柔軟的進行，而國民事實上也很難自國家系統中掙脫。**

第三項 小結

從這幾個領域接受資訊化社會的轉變之後，可以發現數據化與資訊化帶來了深刻的影響。這些影響最主要集中在**資料使用效率提升、對於未來預測的可操作性逐漸提高、以及監視技術外觀的柔軟化等方面。**資料使用的效率提升使得收集個人資料的成本降低，更精確的個體識別也使得進行資料收集帶來的好處更多。數據化的資料能夠以演算法做為運算結構，實現自動化、大規模的風險預測系統。**監視技術的外觀則與安全、福利、便利性等柔軟的性質掛勾**，加上技術的發展使得個人與監視系統的連接更加緊密，也使個體更容易接受這些系統的調整。

第五章 結論

第一節 研究所得與限制

doi:10.6342/NTU201900452

第一項 總結

監視理論的發展伴隨資訊社會的到來，無可避免地轉入數據化、資訊化、分散化、多元化的階段。監視技術在監視聚合體的支撐之下，能夠與不同的領域接合，在不同領域中進行更精確的個體辨識、個人資料收集、以及以風險評估為目標的未來預測。其中針對犯罪預防與刑事政策領域之結合在古典的監視理論中已經存在，在引入後現代監視技術之後亦發展出了新的可能性，亦即對於未發生的犯罪、個體犯罪的機率等進行計算與預測的可能性。這些系統的運作雖然有著演算法的漏洞、資訊人格與個體的割裂等等問題，但因為其以對抗風險帶來安全作為目標，對於渴求安全的社會來說未必不能接受。在類似的系統中個體發展生活 style 的潛在可能性可能會受到剝奪，從法律出發的論述似乎未必有足夠的對抗監視社會之力道，而法律本身在某種程度上也支持監視技術的發展甚至與之合作。此時如何對抗監視社會的到來，便成為問題。

第二項 抵抗論述的可能性

後現代的監視社會之中，視線以及對個體的穿透與掃描似乎已經成為無法掙脫的塊莖狀結構。**此一結構超越了視線層次，而是以透徹的、猶如波浪持續沖刷一般的狀態存在於生活之中，並且衝擊著每一個個體。**資訊設備的使用會留下資訊足跡，交通工具的車牌與擁有者連結，持有手機的狀態下行動軌跡亦有被追蹤的可能性。這些對於監視的恐懼，一方面來自於對於獨裁與受到箝制的抗拒，另一方面則來自於人性尊嚴之保障與人格發展之自由。即使在監視理論發展之前，對於個體來說，時刻關注自己並且試圖影響行為的視線，均會讓人感到不自在，並且影響人格發展自由。在這些前提下，有許多對抗監視社會論述之可能性。以下簡單敘述各種論述上的對抗可能性，並且提出本文最後的結論。

限制、最小化監視。要求各個使用監視技術的機構或個體盡量減少監視視線的設置，或者盡量減少監視視線對個體可能帶來的損害，例如本文於法律控管部份的論述提及的，對個人資料之使用與收集進行管制之手法。但問題是，期望官僚組織與商業組織減少資料收集似乎不切實際，而即便使用法律進行限制，仍無法避免個體為了換取特定服務而主動提供資料之情況(例如網路供應商、購物網站、銀行、醫療院所)。此時問題在於，**監視技術為社會帶來的益處也同時綁定了其背後存在的系統性危險，而事實上在監視科技發展之後，已經很難再重新限制監視之發展。**如本文於前述資料取得取向之管制部分論述亦說明，資料流動與收集之浪潮已難以阻擋。因此限制與最小化監視之作法，在實行上固然能夠產生一定作用，但也同樣面對這些困難。

doi:10.6342/NTU201900452

道德論述的建立。以監視理論與監視社會的現況為中心，承認監視技術當今的發展並且試圖在之中找到一個具有道德性質的行為準則，並以此一原則作為監視進行與發動的標準，重新檢視監視社會中出現的各種問題。論者認為若能建立此一論述，其將有能夠防止系統預測失靈、錯誤的差別待遇之可能性[172]。但即便認為建立道德論述此一手法可行，其實際操作似乎仍無法脫離安全與隱私的衝突問題。且**有能力建構監視系統者，通常亦有能力掌握道德論述的解釋權力，且在近代多元價值觀之下，似乎難以對道德論述進行何種創新，實際操作上大概仍會回歸到隱私權與人格發展自由之運作。**在這些原因之下，道德論述建立大約只能作為輔助性質的對抗論述。

對 code 與結構之設計進行控管。從構成監視社會的重要基礎，即監視技術與系統運行所依賴之程式碼與演算法之建立過程，以及現實環境中監視技術的相關配置著手，以結構之設計達成限制監視社會之目標。例如要求公開演算法運算過程與系統之程式碼達成透明化、課予說明危險因子的定義與差別待遇的理由之義務等等。此一論述的問題在於，必須要結構之設計者願意接受控管或者願意變更設計才有可能達成。但正如同**官僚組織章節所提及的，組織本身難以克制對於更多個人資料的渴求，如果試圖依賴法律等對設計進行控制，亦必然會留下供國家使用的例外狀況**，例如出入境管理、國家安全等等因素便經常作為展開例外的理由。因此此一論述應屬部分可行，但仍無法掙脫國家進行的管理。且結構設計另一個問題在於，其經常潛藏於環境與編碼之中，個體未必能夠理解結構所代表的意涵。甚至在虛擬領域中，即便將程式碼與演算法公開，恐怕能夠理解其內容的個體亦屬少數。此時更重要的似乎是對各該設計者課予開示結構設計目標之義務。例如完整說明個人資料使用之流向、網頁之 Cookie 究竟紀錄何種瀏覽習慣等等。

自我關注的回歸。在個體無法脫離社會單獨存在的前提之下，似乎也僅能促使個體盡量意識到監視視線的存在以及個人資料的流通所蘊含的危險，而後在其所能控制的範圍內對自我的資料盡量實踐資料自主權。正如本文前述，在資訊社會的生活之中，與其他系統、介面的連接事實上不可避免。本文最終認為，從系統中逃脫或者整體推翻掉系統的建置、甚至邁向下一個時代等選項，均非單一個體所能達成。生活於資訊社會中的個體應當盡量理解這些系統與介面收集個人資料代表的意涵，亦**即明確了解「監視技術與系統中蘊含的危險性」，而後試圖在這些制度與系統之中掙扎或者放棄。而不論選擇掙扎、放棄、或者進行游擊戰，最重要的是試圖去認識監視社會中蘊含的危險性為何，個體**

[172] Eric Stoddart (2012). Evaluating surveillance ethically. In Kirstie Ball, Kevin D. Haggerty and David Lyon (Eds.). *Routledge Handbook of Surveillance Studies* (p.376).

doi:10.6342/NTU201900452

於這些系統中所受到的限制又為何，而後才有足夠供自身判斷是否採取行動、如何採取行動之標準，或者拓寬前幾種抵抗論述之可能性。而這些均以理解監視社會與系統的現狀為前提。在卡夫卡的《審判》中，審判的到來與判決的執行沒有解釋與理由。監視社會中的個體在演算法之下被差別待遇的過程，在某程度上可以與之類比。審判的進行與差別待遇的進行，有時候完全脫離於個體的意識與控制能力之外。當然大部分情況下監視社會的差別待遇程度並不嚴重，例如購物網站依照客戶資料區分購物傾向等狀況，與《審判》中死刑的結果即難以對比。但監視社會中終究蘊含著此一差別待遇的危險性，生活當中的個體則應當對此予以關注，並在力所能及之範圍內妥善管理個人資料。

第二節 留待未來解決的問題

個人資料的散失以及監視網路的構成，似乎使得此一權力網路越加牢不可破。更多的資訊會在無意間被記錄下來並且進行分析，在個人資料無法避免地必須提供給國家以及其他系統的情況下，監視系統的滲透似乎成為必然，亦留下許多留待探討的問題。例如由私人設置的監視設備以及私人進行的資料收集與犯罪控制是否可能產生關聯？若參照日本內閣府未來政策構想之描述，對於犯罪此一嚴重的危害，採用全面監視以在事前預防犯罪發生之政策是否可行？對於犯罪的恐懼，使得人民願意接受犯罪控制的概念、接受監視視線的存在以換取安全，並且對社會進行標記與分類而後加以進行排除。此時人民關心規範還是關心風險？法規範的意義是否被風險概念取代，新的行為規範又如何與監視技術相結合？監視技術與系統是否會促成「敵人刑法」的再臨？差別待遇之合理性是否可以完全交由演算法進行判斷？或者即便有法官介入使用類似令狀原則之方式處理可能被實行的差別待遇，此時以單純以「未來可能之風險」作為差別待遇之正當理由，是否足夠？以上問題雖然在本文的論述中或多或少有所觸及，但限於能力問題，未能於文本中進行完整處理。本文希望，藉由這些論述的提出，對於監視社會至今的發展以及未來的可能性與危險性以及面臨的問題能夠提供一些參考。

doi:10.6342/NTU201900452

參考文獻

一、中文文獻

(一)專書

Barkan, S. E. (著) (2011)，秦晨 等(譯)，《犯罪學：社會學的理解》，第四版，上海人民出版社。(原著出版年:2008 年)

Gilles Deleuze (著) (2000)，楊凱麟譯，《德勒茲論傅柯》，麥田。(原著出版年:1986 年)

法務部司法官學院(編)(2013)，《刑事政策與犯罪研究論文集〈16〉》，法務部司法官訓練所。

謝劍斌、李沛秦、閆瑋、林成龍、劉通、洪泉益、周紅飛、崔一兵(編著)(2016)，《無人監控：技術原理與應用》，佳魁。

(二)期刊論文

李榮耕(2015)，〈科技定位監控與犯罪偵查：兼論美國近年 GPS 追蹤法制及實務之發展〉，《臺大法學論叢》，第 44 卷第 3 期，頁 871-969。

張煜麟(2004)，〈台灣監視器系統作為集體逃避自由的機制？一種自由主義的觀點〉，《資訊社會研究》，第 7 期，頁 191-218。

劉定基(2017)，〈大數據與物聯網時代的個人資料自主權〉，《憲政時代》，第 4 卷第 3 期，頁 265-308。

董娟娟(2005)，〈詮釋新加坡發展的新路徑：監視社會研究的新解與展望〉，《台灣政治學刊》，第 9 卷第 2 期，頁 107-150。
http://dx.doi.org/10.6683/TPSR.200512.9(2).107-150

(三)專書論文篇章

溫哲彥(2013)，〈影像處理技術於偵查與鑑識之應用－由二維到三維空間〉，載於法務部司法官學院(編)(2013)，《刑事政策與犯罪研究論文集〈16〉》，頁 237-254。

(四)網頁資料

我國內政部 107 年及 108 年施政計畫，網址:
https://www.moi.gov.tw/chi/chi_public/policy.aspx?policy_code=02&type=info

doi:10.6342/NTU201900452

最後瀏覽日期 2019.01.11。

我國警政發展方案(第二期)(104-107 年作業計畫)，網址為：http://117.56.91.94/KMPublic/readdocument.aspx?documentId=279751，最後瀏覽日期：2019.01.11。

(五)新聞

台灣好新聞(2018.08.13)，〈丁守中：獨居、人際關係差、失業、單身男子易犯罪　應有效監測、加強查訪〉，http://www.taiwanhot.net/?p=611865，最後瀏覽日期 2019.01.11。

二、英文文獻

(一)專書

David A. Mackey & Kristine Levan (2011), *Crime Prevention*.

David Lyon (Ed.). (2002). *Surveillance as Social Sorting: Privacy, risk, and digital discrimination*.

David Lyon (Ed.). (2006). *Theorizing Surveillance: The panopticon and beyond.*

Ernesto U. Savona (2004), *Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research.*

Kevin D. Haggerty, & Richard V. Ericson (Eds.). (2006). *The New Politics of Surveillance and Visibility.*

Kirstie Ball, Kevin D. Haggerty and David Lyon(Eds.). (2012) *Routledge Handbook of Surveillance Studies*.

Michel Foucault (1995), *Discipline & Punish: The Birth of the Prison.* (Alan Sheridan, Trans.) (Original work published 1975)

Marcus Felson (2002), *Crime and Everyday Life*.

Nikolas Rose (1999), *Powers of Freedom: Reframing Political Thought.*

(二)期刊論文

Ferguson, Andrew Guthrie (2012), Predictive Policing and Reasonable Suspicion,

doi:10.6342/NTU201900452

Emory Law Journal, Vol.62, pp.259-325. Available at SSRN: https://ssrn.com/abstract=2050001

Gilles Deleuze (1992), Postscript on the Societies of Control, *October*, Vol. 59, pp.3-7.

Kevin D. Haggerty and Richard V. Ericson (2000), The surveillant assemblage, *British Journal of Sociology*, Vol. No.51 Issue No.4, pp.605-622.

Ronald V. Clarke (1995), Situational Crime Prevention, *Crime and Justice*, Vol. 19, pp. 91-150. Stable URL: https://www.jstor.org/stable/1147596

Solove, Daniel J. (2007), 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy, *San Diego Law Review*, Vol. 44, pp. 745-772; *GWU Law School Public Law Research Paper* No. 289. Available at SSRN: https://ssrn.com/abstract=998565

(三)專書論文篇章

Aaron Doyle (2006). An Alternative Current in Surveillance and Control: Broadcasting Surveillance Footage of Crimes. In Kevin D. Haggerty, & Richard V. Ericson (Eds.). *The New Politics of Surveillance and Visibility* (pp.199-224).

Christopher Dandeker (2006). Surveillance and Military Transformation. In Kevin D. Haggerty, & Richard V. Ericson (Eds.). *The New Politics of Surveillance and Visibility* (pp.225-249).

Christopher Dandeker (2007). Surveillance: basic concepts and dimensions. In Sean P. Hier & Joshua Greenberg (Eds.). *The Surveillance Studies Reader* (pp.39-51).

David Lyon (2002). Surveillance as social sorting: Computer codes and mobile bodies. In David Lyon (Ed.). *Surveillance as Social Sorting: Privacy, risk, and digital discrimination* (pp.13-30).

Eric Stoddart (2012). Evaluating surveillance ethically. In Kirstie Ball, Kevin D. Haggerty and David Lyon (Eds.). *Routledge Handbook of Surveillance Studies* (p.369-376).

John McGrath (2012), Performing surveillance. In Kirstie Ball, Kevin D. Haggerty and David Lyon (Eds.). *Routledge Handbook of Surveillance Studies* (pp.83-90).

doi:10.6342/NTU201900452

Joseph Turow (2006). Cracking the Consumer Code: Advertisers, Anxiety, and Surveillance. In Kevin D. Haggerty, & Richard V. Ericson (Eds.). *The New Politics of Surveillance and Visibility* (pp.279-307).

Kevin D. Haggerty & Richard V. Ericson (2006). The New Politics of Surveillance and Visibility. In Kevin D. Haggerty, & Richard V. Ericson (Eds.). *The New Politics of Surveillance and Visibility* (pp.3-25).

Oscar Gandy, JR (2006). Data Mining, Surveillance, and Discrimination in the Post-9/11 Environment. In Kevin D. Haggerty, & Richard V. Ericson (Eds.). *The New Politics of Surveillance and Visibility* (pp.363-384).

Oscar H. Gandy, Jr (2012). Remote sensing in the digital age. In Kirstie Ball, Kevin D. Haggerty and David Lyon(Eds.). *Routledge Handbook of Surveillance Studies* (pp.125-132).

Toni Weller (2012). The information state：An historical perspective on surveillance. In Kirstie Ball, Kevin D. Haggerty and David Lyon (Eds.). *Routledge Handbook of Surveillance Studies* (pp.57-63).

Toshimaru Ogura (2006). Electronic government and surveillance-oriented society. In David Lyon(Ed.). *Theorizing Surveillance: The panopticon and beyond* (pp.270-295).

William Bogard (2012). Simulation and post-panopticism. In Kirstie Ball, Kevin D. Haggerty and David Lyon(Eds.). *Routledge Handbook of Surveillance Studies* (pp.30-37).

(四) Working Paper

Michael McCahill & Clive Norris (2002), *CCTV in London*, Working Paper No.6. Available at http://www.urbaneye.net/results/ue_wp6.pdf

(五)網頁資料

Australian Government Department of Human Services, BasicsCard. 取自：https://www.humanservices.gov.au/individuals/services/centrelink/basicscard，最後瀏覽日期 2019.01.11。

doi:10.6342/NTU201900452

Human Rights Watch,“Eradicating Ideological Viruses” China’s Campaign of Repression Against Xinjiang’s Muslims, September 9, 2018. 取自：https://www.hrw.org/report/2018/09/09/eradicating-ideological-viruses/chinas-campaign-repression-against-xinjiangs，最後瀏覽日期 2019.01.17。

三、日文文獻

(一)專書

David Lyon(著)(2011)，田島 泰彦、小笠原 みどり(譯)，《監視スタディーズ－「見ること」「見られること」の社会理論》，岩波書店。

仲正 昌樹(編)(2013)，《「法」における「主体」の問題》，御茶の水書房。

岩井 宜子(2011)，《刑事政策》，第五版，尚学社。

松尾 陽(編)(2017)，《アーキテクチャと法：法学のアーキテクチュアルな転回？》，弘文堂。

星 周一郎(2012)，《防犯カメラと刑事手続》，弘文堂。

(二)期刊論文

小林 健人、稲村 勝樹、金田 北洋、岩村 惠市(2016)，〈プライバシ保護と犯罪防止を両立させる監視カメラシステム〉，《情報処理学会論文誌》，Vol.57 No.1，頁 172-183。

内藤 大海(2016)，〈総合的監視に関する予備的考察：ドイツの議論状況の概観を通じて〉，《熊本法学》，Vol.136，頁 157-193。

守山 正(2017)，〈犯罪予測技法の展開－近接反復被害分析を中心として－〉，《政治・経済・法律研究》，Vol.20 No.1，頁 1-31。

星 周一郎(2017)，〈犯罪の未然防止・再犯防止と情報の取扱い〉，《法学会雑誌》，58 巻 1 号，頁 59-89。

(三)專書論文篇章

松尾 陽(2017)，「法とアーキテクチャ」研究のインターフェース―代替性・正当性・正統性という三つの課題，載於松尾 陽(編)，《アーキテクチャと法：法学のアーキテクチュアルな転回？》，頁 1-31，弘文堂。

doi:10.6342/NTU201900452

松尾 陽(2013)，防犯アーキペラゴ序説—包摂と排除の交錯とはざま—，載於仲正 昌樹(編)，《「法」における「主体」の問題》，頁 87-110，御茶の水書房。

稻谷龍彦(2017)，技術の道徳化と刑事法規制，載於松尾 陽(編)，《アーキテクチャと法：法学のアーキテクチュアルな転回？》，頁 93-127，弘文堂。

(四)網頁資料

日本內閣府官方網頁，イノベーション 25 之說明，取自：https://www.cao.go.jp/innovation/，最後瀏覽日期 2019.01.11。

doi:10.6342/NTU201900452