電腦詐欺行為之刑法規範

蔡蕙芳*

目　次

* 中興大學財經法律學系助理教授；台灣大學法學博士。

中文關鍵詞：電腦詐欺、電腦詐欺罪、詐欺罪、自動櫃員機之濫用、電腦操縱、資料、資訊、輸入操縱、程式操縱、義大利香腸術、特洛伊木馬術、輸出操縱、硬體操縱
Key Words：ATM Abuse, computer fraud, computer fraud offense, fraud, computer-manipulation, data, input-manipulation, information, program-manipulation, Salami technique, Trojan technique, output-manipulation, hardware-manipulation

中文摘要

1997 年 10 月，電腦詐欺行為之刑事立法，包括：刑法第三百三十九條之一不正使用收費設備罪、刑法第三百三十九條之二不正利用付款設備取財得利罪與刑法第三百三十九條之三不正利用電腦取財得利罪（又稱電腦詐欺罪）正式施行。本文主要研究對象是刑法第三百三十九條之二與刑法第三百三十九條之三，目的在提供解釋與適用上述電腦詐欺刑罰規定之參考。由於德國刑法上有相類似之電腦詐欺罪立法例，本文首先將介紹與分析德國立法、學說見解與法院實務上處理方式。接著，參考我國學者之意見，針對刑法第三百三十九條之二與刑法第三百三十九條之三進行構成要件分析。藉由我國與德國立法例之比較，闡明我國立法上之得失。最後，本文將針對現行條文提出評論與修正建議。

Abstract

In October, 1997, three computer fraud provisions as the amendments to the Taiwan Penal Code began to come into force. The purpose of this Article is to provide a fundamental understanding of the purpose and application of two of these provisions.

The Article will begin with an introduction of the German legal doctrine, academic opinions and court decisions in the field of computer fraud. Next, it will provide a more complete analysis of the wording of the computer fraud statutes by reference to the opinions of our scholars. Finally, the Article proposes recommendations for future amendments to the computer fraud statutes.

壹、基本問題：法律漏洞填補與立法規劃

電腦發明與普及所帶來的問題，最早為自動化機器濫用。最初的主要行為類型是利用偽造硬幣或其他金屬片從自動販賣機取得貨品。在此情形下，適用傳統竊盜罪來處罰並無問題。而當濫用行為的對象轉變成自動提款機時，法律的適用問題逐漸成為關注的焦點。通常而言，在以下的案例中，傳統竊盜罪之適用可能會出現困難，亦即，當行為人以偷來之他人卡片配合正確密碼而提領現金時，一切的過程皆符合程式預定的步驟進行，但由於自動提款機並未如自動販賣機一般，事前設有附條件之持有與所有權移轉之意思決定，因此行為人之行為是否構成竊盜罪構成要件中破壞持有之取走行為（Wegnahme）便產生爭議[1]。即使利用自動櫃員機取款的情形，可適用竊盜罪，然更多情形是通過自動櫃員機之自動轉帳功能而清償如電話費、水費、信用卡等債務，或將他人戶頭之存款轉帳至自己戶頭，在此情形下，行為人自始至終皆未取得現金，屬於竊盜罪與侵占罪之取得犯構成要件所無

[1] Lenckner, Computerkriminalität und Vermögensdelikte, 1981, S. 25.

法掌握的利得犯，只能轉向依據詐欺罪等利得犯構成要件來加以規範。然而，因電腦在社會生活領域中形成新的意思形成與財產處分系統與傳統人之意思決定與財產上處分行為有所不同，故在適用詐欺罪時也產生疑問。

進而言之，以電腦為中心之意思形成與財產處分系統的特色是所有重要的決定都由電腦完成；除了讓電腦運作的程式與資料，是由程式設計者與銀行客戶輸入外，在整個意思形成過程中皆無人的介入，其交易的結帳不經過人的判斷作用而由機器自動化處理完成[2]。因此，如果利用電腦操縱（Computermanipulation）來影響電腦資料處理之結果，而獲得財產上利益，在適用詐欺罪的構成要件上將有困難。主要的原因在於，傳統詐欺罪的構成要件之一為行為人「施行詐術」而使被害人陷於「錯誤」。而依據德國刑法通說，「錯誤」是與人有關之心理事實，與錯誤相對應之「施行詐術」必然也僅限於對人想法的影響，然這些特徵在電腦操縱自動化處理過程中都不存在。雖有少數說主張，電腦是人類在分工原則下，將有關資訊與意思決定過程委由電腦自行處理，故在分工架構下，人可以透過電腦而發生錯誤。換言之，每一個電腦處理後面都會有一個使用者，因此是可以把錯誤歸屬於某個人，但此項少數見解不為通說所採，因此，在電腦操縱情形中存在處罰上漏洞[3]。儘管在涉及電腦（或自動化）操縱的案例中，並非完全不能適用傳統詐欺罪，只要其中過程有人的介入，仍可適用詐欺罪。但正如有些學者所指出者，怎可將行為之處罰繫諸於偶然因素[4]。特別是，現在人類事務自動化程度越來越高，許多

---

[2] Cramer, in: Schönke-Schröder, StGB, 25. Aufl. 1997, § 263 a Rdnr.6; Tröndle/Fischer, StGB, 49. Aufl. 1997, § 263 a Rdnr.6.

[3] Lenckner, Computerkriminalität und Vermögensdelikte, 1981, S. 26.

[4] Tiedemann, JZ 86, 869.

發生過的案件中都沒有人為的介入，因此不能據以來適用詐欺罪。故就此點而言，實有立法的必要性[5]。

為了彌補上述詐欺罪處罰上漏洞，刑法上出現了新的罪名：電腦詐欺罪（Computerbetrug, computer fraud）。電腦詐欺罪不是以電腦（包括其內之電腦資料）為攻擊對象或行為客體，而是以資料或電腦作為行為的工具[6]。電腦詐欺罪所要規範者為最終獲得財產上利益之行為，而電腦或資料只是行為的工具。因此，在電腦詐欺罪中，電腦或資料不是電腦詐欺罪所要保護的法益[7]。此外，電腦詐欺罪的規定是模仿傳統刑法詐欺罪之構成要件，期能藉以掌握那些不涉入人的檢驗決定，完全以自動化方式進行自動資料處理與財產上處分，因而不能滿足詐欺罪圍繞在對人的欺騙與造成錯誤等特徵的財產侵害行為。

基於以上敘述可知，在創造新的構成要件時，電腦詐欺罪之構成要件設計與傳統詐欺罪在犯罪結構與價值（犯罪非價）上須具有等值性。此外，在犯罪體系之安排上，因為財產的處分不是由陷於錯誤的人作成，就是由電腦等自動設備所為，因此，在詐欺罪與電腦詐欺罪兩者間有構成要件排他性的關係；亦即，在處理事務之過程中，如有人的介入，而能被認為被欺騙，仍依原來之詐欺罪處罰。至於電腦詐欺罪與其他既有保護相同財產法益之財產犯罪間之關係，應將電腦詐欺罪以補充性構成要件看待。所謂補充性構成要件就是具有備位性質之構成要件，它必定是在主

---

[5] Lenckner, Computerkriminalität und Vermögensdelikte, 1981, § 265a.

[6] Schultz, Computerkriminalität, 1992, S.99.

[7] 利用電腦操縱而取得財產上利益是電腦詐欺罪與其他種電腦犯罪類型相比較最重要的特色。電腦詐欺罪以外以電腦犯罪稱之犯罪，通常都是與資料保護有關。舉例而言，證據上重要電腦資料不法製作、電腦資料不法取得或洩漏、電腦資料不法破壞等，這些電腦犯罪類型都是與資料保護有關。

要規範（基本構成要件或基本條款）無法適用於某一值得處罰的行為而形成法律漏洞時方才介入。如果基本條款實現，依據「基本條款排除補充條款」原則，當然不再適用備位之補充性構成要件。事實上，立法例上採取修正刑法方式，在傳統犯罪體系中，加入新的電腦犯罪條文之立法用意應即在此。此一立場保留原來刑法分則內財產犯之結構，亦即，竊盜罪、侵占罪等優先於電腦詐欺罪之適用[8]。

1997 年 10 月 6 日起，與電腦詐欺行為有關之刑法規範，刑法第三百三十九條之一、刑法第三百三十九條之二與刑法第三百三十九條之三開始施行[9]。本文之研究對象為刑法第三百三十九條之二與刑法第三百三十九條之三之相關問題，目的在提供解釋與適用之參考。由於德國刑法上也有相類似之電腦犯罪立法例，故本文首先將介紹與分析德國立法、學說見解與法院實務上處理方式[10]，接著，並參考我國學者意見針對刑法第三百三十九條之二與刑法第三百三十九條之三進行構成要件分析。至於刑法第三百三十九條之一，由於性質上與前述兩條條文有所差異，將在另一

---

8 以上所述僅屬本文見解，對此問題，我國學界的立場，將在本文第參部分有關我國立法例與學說之介紹中詳細說明。

9 在本次立法之前，我國實務之立場是認為對機器可以構成詐欺罪，不過，自從這三條條文立法通過後，台灣高等法院暨所屬法院九十年座談會表示：「在以機器為對象之情形，--無所謂受欺罔至生錯誤之情形，是行為人對機器所為類似詐欺行為，並不該當於刑法第三百三十九條所規範之「詐術行為」，為彌補此一漏洞刑法乃於1997年10月增訂第三百三十九條之一、第三百三十九條之二、第三百三十九條之三，規範對機器以不正行為取得不法財物、利益之行為。據此，在前開刑法增訂公布後，對機器之不正行為，應無再適用刑法第三百三十九條之餘地。」參見，台灣高等法院暨所屬法院九十年座談會彙編（九十一年七月），頁414-24。

10 雖然我國刑法第三百三十九條之三是參考日本刑法第二百四十六條之二，但由於資料缺乏與個人能力，無法給予完整呈現，故在此省略日本立法之介紹。僅在第三部分討論我國立法條文之某些問題上，引用日本見解。

篇文章討論。而為清楚呈現兩個立法例之差異，本文採取的論述方式是將德國立法例與我國立法例分別並立，捨棄以介紹我國立法例為主，而穿插德國立法例為參考之論述方式。本文期能藉由我國與德國立法例之比較，進而闡明我國立法上之得失。文末，將提出現行不足之觀點，並針對現行條文提出修正建議。

貳、德國電腦詐欺罪規範之介紹

一、德國刑法第二百六十三條 a 電腦詐欺罪

㈠條文內容之預覽與介紹

德國刑法第二百六十三條 a[11]是依據經驗上已出現之行為型態與具財產損害性之電腦操縱特質，以例示的方法規定數種行為類型：一.編制不正確的程式；二.使用不正確或不完整資料；三.無權使用資料；並包括一項概括規定之行為，即：其他無權影響資料處理過程的行為[12]。由本構成要件可知，最重要的概念為「資料」。不過，立法者並未針對構成要件中之「資料」為定義，也沒有指出本構成要件中之「資料」即為德國刑法第二百零二條 a 第二項所定義之電腦資料。按，德國刑法第二百零二條 a 第二項規定，「第一項（電腦資料無權探知罪）所述的資料係指以電子、

---

[11] 德國刑法第二百六十三條a第一項與第二項之規定分別為：「意圖為自己或第三人不法利益，以編制不正確的程式，或使用不正確或不完整資料，無權使用資料，或其他無權影響資料處理過程的行為，影響資料處理程序的結果，因而造成他人財產之損害者，處五年以下有期徒刑。」「刑法第二百六十三條第二款至第五款亦適用於本條。」

[12] Cramer, in: Schönke-Schröder, StGB, 25. Aufl., § 263 a Rdnr.6; Tröndle/Fischer, StGB, 49. Aufl.,1997, § 263 a Rdnr.6.

磁性或其他不能直接感覺的方式被儲存或傳送的資料。」就此項定義而言，一方面限定資料的電子等形式，一方面亦侷限於已被儲存或被傳送中之資料。有德國學者指出，立法者並未指引適用德國刑法第二百零二條 a 第二項有關資料之定義之原因應該在於，立法者認為，從資料輸入階段開始，資料便有受到保護之必要性；故本構成要件中之「資料」概念比德國刑法第二百零二條 a 第二項之資料概念為寬。

此外，在理解資料時必須伴隨相對應之構成要件行為。首先，本條第一項第二段之「使用不正確或不完整資料」中之「使用」概念，由於指涉輸入行為，所以，被輸入電腦內部之資料型態必然為「代碼形式」。再者，依據通說見解，本條第一項第三段之「無權使用資料」之「使用」概念與第二段相同，皆被理解為「輸入」，所以不涉及代碼形式資料，無法滿足「無權使用資料」構成要件。承上述，由於「使用」概念是以輸入資料為前提，因此在清光賭博遊戲機內現金（Leerspielen von Glückspielautomaten）之案例中，行為人利用違法取得程式資料之特殊知識來操作機器按鈕，此按鈕行為本身並未輸入任何資料進入電腦系統中，故不構成「無權使用資料」，而必須依據下一段之「其他無權影響資料處理過程」之網羅性構成要件來處罰[13]。但亦有採廣義解釋者，將「無權使用資料」之「使用」理解的更廣，除了包括「輸入」外，還包括「利用」。依此以論，行為人所使用之資料即不必侷限於代碼形式（數位形式），尚可包含解碼後之資料[14]。類似看法，例如 Bay 高等法院在遊戲機濫用判決中曾主張，行為人取得遊戲機內電腦程式的運作程序資料，並使

[13] Wessels/Hillenkamp, BT/2 § 13 VI 2 Rdnr. 613.
[14] Tiedemann, in: LK, 11. Aufl. 1998, § 263 a Rdnr. 41.

用此等資料而得以在事先算出適當時點按鈕，進而在短時間贏得機器內所有現金，此種行為即構成「無權使用資料」[15]。

對以上爭論，有學者指出，從目的論解釋而言，立法者所要掌握的新型財產侵害型態是影響電腦處理過程之電腦操縱，因此構成要件中之「資料」並非沒有限制的條件，至少必須呈現出電腦所能「理解」的資訊。因此在解釋構成要件之「資料」概念時，必須對「資料」為如下之理解：「資料」是紀錄事實的記號，「資訊」是資料所表達或至少是資料所呈現出之事實，此外從構成要件「影響資料處理程序之結果」可以導出，使用資料必須是以電腦為對象，讓電腦「理解」。因此，可得出以下的結論：「資料」是被轉譯成代碼的資訊（kodierte Informationen），當「資訊」從可見形式被轉譯成可供機器處理之代碼形式時，「資訊」即成為「資料」[16]。

依據上段敘述可知，資訊是來自於資料之解讀，資訊是被呈現出來的東西，其存在的型態並不重要，因此，德國實務上所爭論，「資料」是否必須被固化在資料載體上之問題[17]，對解釋「資料」概念而言，並不重要。再者，在面對電腦「使用」資料時，資料並不須以「代碼形式」存在。以前述之案例為例，行為人雖然已知悉遊戲機運作程式之知識，而得以在特定時點按下按鈕，贏得機器內之現金，但行為人在行為前仍須先將程式內容印出

---

[15] NJW 1991, 438, 440.

[16] Tiedemann, in: LK,11. Aufl. 1998, § 263 a Rdnr. 20f.

[17] 例如，Köln高等法院在違反授權契約之超出授權範圍使用他人合法卡片是否構成「無權使用資料」的判決中表示，當事人所輸入之提款數字由於並沒有將資訊編成二進位碼代碼與固定在資料載體上，故並非「無權使用資料」。參見，NJW 1992, 125, 127.

來，再經由逆向之解譯程序（entkodierten）[18]轉成可理解的形式，最後才能理解程式設計者的意思，得知在何種條件下機器會大量送出現金。依據前段所提出之見解，將程式列印出來的行為，雖使資料喪失「代碼」的形式，卻不會影響「使用」資料之判斷。程式為資料，設計者的意思便為「資訊」，而解譯程序是為了得到有關程式資料的資訊。有了資訊，行為人的按鈕行為，等於在增加輸贏機率一事上對電腦下指令，此即「使用」了儲存在電腦內之「資料」，因此行為人的行為構成「使用」「資料」[19]。

至於本條第一項第四段「其他無權影響資料處理過程」之「資料處理過程」應包含所有技術性過程，亦即，依據程式而進行的資料處理與傳遞處理結果之過程。立法者在立法理由中與學者在說明「資料處理過程」概念時，都強調此必須是財產上重要的資料處理過程[20]；德國學者也舉例，即使保險箱或收費站之電子檢測裝置，具有所謂資料處理過程，但行為人藉由資料操縱行為僅取得取走保險箱之物或得以通行之可能性，並非進行了財產上的處分，故無法符合本罪之構成要件[21]。至於販賣貨物機器的機械過程，也不屬第二百六十三條 a 之「資料處理」[22]，因此，使用技術而從自動販賣機取物，因其中間過程並未涉及資料操縱與資料處理程序之影響，所以不受本條規範，亦非依據第二百六十五

---

[18] 解譯是把由一系列零與一所組成的數列譯成能夠被閱讀與理解的程式（或稱明碼）。例如，將每個子程式中的零與一譯成組合語言，再簡化為簡單C語言。在通常情況下，程式是被編譯，而不是被解譯。當程式從原始碼（code）經過編譯器進行編譯後轉成機器可執行的代碼後，就沒有必要逆轉這一過程。很多商業軟體還禁止用戶從事解譯程式行為，以防止拷貝或修改。

[19] Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 21.

[20] Cramer, in: Schönke-Schröder, StGB, 25. Aufl. 1997, § 263 a Rdnr.23; Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 65.

[21] Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 65.

[22] Günther, in: SKStGB, 5. Aufl. 1996, § 263 a Rdnr. 8.

條a，而僅得依據第二百四十二條竊盜罪處斷。

㈡客觀不法構成要件

1.構成要件行為

⑴編制不正確程式

「編制不正確程式」此構成要件是要來規範「程式操縱」（Programm-Manipulation）[23]。依據德國通說之見解，由於「程式」屬於「資料」概念，因此「編制不正確程式」可被包含在本條下一款「使用不正確資料」的概念中[24]，亦即，可以被「輸入操縱」所涵蓋。由此可知，本構成要件之功用僅在進一步澄清說明，因程式操縱行為較難被發現，且程式操縱所產生的效果具持續性與重複性，因此立法者特別另立獨立構成要件，以強調其危險性[25]。

既然第二百六十三條a的「資料」概念較廣，所以行為人編制不正確程式過程中必然已經實現輸入虛偽資料行為。由此可知，此種構成要件的設計導致一行為同時觸犯本法第一項第一段與第二段之構成要件，依據「特別條款排除一般條款」原則，適用屬於特別條款之第一段構成要件行為[26]。又行為人編制不正確程式行為會使所輸入之正確資料被以不正確程序進行資料處理，同時亦將構成同條項第四段之「其他無權影響資料處理過

---

[23] Tröndle/Fischer, StGB, 49. Aufl. 1999, § 263 a Rdnr.6. Lackner/Kühl, StGB, 23. Aufl. 1999. § 263 a Anm. 4. .

[24] Tröndle/Fischer, StGB, 49. Aufl., 1999, § 263 a Rdnr.6. Lackner/Kühl, StGB, 23. Aufl. 1999, § 263 a Rdnr.6.

[25] Tiedemann, JZ 86, 869; Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 27.

[26] Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 27.

程」，然由於「其他無權影響資料處理過程」屬於補充性質之構成要件，僅為備位規範，當主要規範可以被適用時，依據「基本條款排除補充條款」原則，逕行適用第一段基本條款之構成要件即可[27]。

本構成要件所描述之程式操縱行為，包括以下兩種情形：自最初編制程式時便已開始，以及對原來既存正確程式的修改，使電腦未按既定程式，而是依後來附加的功能運作[28]。再者，本構成要件所指之程式種類並無限制，包括應用程式、作業程式、以人類所能懂語言所寫之原始程式（Quell-programme）與機器語言之的目的程式（Maschinenprogramme）[29]。又雖構成要件僅提及「程式編制（編寫）」，但也包括程式之「置入」或「插入」，所以，構成要件中「編制」一詞可包含「編寫」、「置入」或「插入」程式等行為。總括而言，本構成要件之行為方式可包括以下幾種：行為人先編制某個程式，並將之置入或插入原系統；更改或刪除已存程式中的某些程序（步驟或指令）；在既存程式中添加額外的程序（步驟或指令）或透過分流繞過既有程式，致使輸入的資料未被以程式設計者預設的方式處理；或在未更改既存程式的演算程序下，取代原有的演算程序[30]。

就如何理解程式是否「不正確」，德國學說有數種說法可供參考：

主觀說採取主觀正確性概念，認為不正確的程式編制是指違

---

[27] Cramer, in: Schönke-Schröder, StGB, 25. Aufl. 1997, § 263 a Rdnr.6

[28] Günther, in: SKStGB, 5. Aufl. 1996, § 263 a Rdnr. 14; Lackner/Kühl, StGB, 23. Aufl. 1999, § 263 a Rdnr. 6.

[29] 一般而言，寫程式之過程是先以人類所能懂語言所寫之原始程式，然後再轉換成機器能懂的目的程式。

[30] Cramer, StGB, 47. Aufl. 1995, § 263 a Rdnr. 6.

反程式處分權人之意思。一般而言，正確與否之解釋乃依據是否與事實（Wahrheit）相符合，與事實不相符者即為不正確。在此構成要件中，事實是採主觀解釋，亦即將事實理解成程式設計工作委託者或使用者（系統經營者，並非客戶）的意思，而採此說之學者亦導出以下適用結果：如果行為人置入一段他所編制的程式，即使電腦因此運作出不正確的結果，但若此符合資料處理設備所有人的意思，則未滿足本條的構成要件[31]。德國立法者當初即採此說，因為此正可符合傳統詐欺罪之解釋。傳統詐欺罪是經由行為人實行詐術行為而使得被害人做出違反處分權利人真正的意思決定[32]。

目前德國通說是採客觀正確性之立場。客觀說並非從傳統詐欺罪之觀點解釋正確性概念，而係採「詐欺相似性」（更正確說法是「財產保護觀點」），主張判斷是否屬於「編制不正確的程式」時，應重視處理相關當事人關係（例如，銀行之客戶）所進行的資料處理結果，而非編寫的程式運作是否偏離系統使用者或程式使用權人之意思。程式編制的不正確亦非依據程式（系統）處分權人的意思，而是取決於，行為人所編制的程式是否能取代原定從相關當事人關係導出的資料處理工作[33]。因此，決定正確性之標準在於資料處理系統之處理工作內容。舉例而言，信用卡機構關於利息資料處理之計算程式客觀上是否準確地被計算[34]。

進而言之，客觀說認為本構成要件所要保護者，應是參與資料處理程序者之財產，而非存在於程式上的財產處分權；因此，

---

31 Samson, in: SKStGB, 5. Aufl. 1994, § 263 a Rdnr. 5.

32 BT Drucks. 10/318, S.20 , Tiedemann in: LK, 11. Aufl. § 263 a Rdnr. 29.

33 Tröndle/Fischer, StGB, 49. Aufl. 1999. § 263 a Rdnr.6; Lackner/Kühl, StGB, 23. Aufl. 1999, § 263 a Rdnr. 7.

34 Günther, in: SKStGB, 5. Aufl. 1996, § 263 a Rdnr. 14.

標準應該在於必須被完成的工作。重點在於行為人所編制之程式是否符合資料處理當時預設的目的，而也能產生客觀上相符合該資料處理之結果。據此而論，如果雇主自己所編制之程式讓程式在計算員工工資時得出少於員工實際所給付勞務之應得者，即可被認為構成「編制不正確程式」[35]；又依據客觀說，程式處分權人或系統經營者皆可能構成本罪。值得一提者，有學者對正確性採取限縮立場，主張程式內的工作指令必須是與詐欺有關之事實，當此程式運作時，會得出內容不正確之資料處理結果，亦即唯有當電腦「被騙了」(täuscht)，方能被認為是「編制不正確程式」。據此以論，若程式設計師違反系統經營者之意思而改正會使第三人產生不利益之錯誤程式，將不構成本罪[36]。

此外，依據德國學者的見解，適用本構成要件的典型案例為計算程式被操縱而使計算過程中所產生的餘額被移入行為人的戶頭[37]。因此，一般所稱的撒拉姆法或義大利香腸術（Salami technique）[38]與特洛伊木馬術（Trojan horse technique）[39]便可被本構成要件所掌握。

---

35 Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 30f.

36 Tröndle, StGB, 47. Aufl. 1995, § 263 a Rdnr.6.

37 Carstein, Computerbetrug （§ 263 a StGB）, JurPC Web-Dok. 189/1999, Abs.20.

38 撒拉姆法或義大利香腸術(Salami technique)是指行為人所編制與置入的程式，具備有以下的功能：將客戶帳目計算上所多出的利息尾數移入（轉到）某個帳戶（可能是自己的帳戶或虛設的帳戶）。雖然金額很小，但日積月累，積少成多而累積成一筆大數目。

39 特洛伊木馬術(Trojan horse)是在原有電腦系統中，秘密地插入一個自編的程式，而能執行特定功能。例如，虛增應付利息，並將此虛增款項自動移轉到某個帳戶。

(2)使用不正確或不完整資料

「使用不正確或不完整資料」此一構成要件之重要性不僅是要來規範最經常發生之「輸入操縱」，而且此構成要件行為之設計與傳統詐欺罪之施行詐術行為最具對稱性[40]。儘管與傳統詐欺罪有對稱性，但為了與傳統詐欺罪相區別，立法者選用了不同的立法語言。

首先，本構成要件中之「資料」是對應於傳統詐欺罪構成要件中虛偽之「事實」(Tatsachen)[41]。再者，構成要件中之「資料」並不如刑法第二百零二條 a 一般，僅限於無法直接感覺的電腦資料，尚可包括未被儲存在電腦內的資料[42]。「使用不正確或不完整資料」之「使用」涵義，是指將資料「輸入」以供資料處理的行為[43]。此處之資料處理並不以已經在運作為前提，行為人亦可經由中斷資料處理程序後重新啟動而實施本構成要件行為[44]。「使用」行為包括行為人在輸入程序中，以直接方式，自行輸入不正確或不完整資料，亦包括以間接方式讓不知情的工作人員輸入[45]。

其次，德國立法例上（主要是指在詐欺罪中之資訊（事實）是否正確）所使用的「正確」與「不正確」，是指對於事實狀態的呈現是否符合事實；如果主張確實符合事實，則該事實呈現為

---

[40] Tiedemann, JZ 86, 869; Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 32. Günther, in: SKStGB, § 263 a Rdnr. 3; Cramer, in: Schönke-Schröder, StGB, 25. Aufl., 1997, § 263 a Rdnr. 7.

[41] Günther, in: SKStGB, 5. Aufl. 1996, § 263 a Rdnr. 2.

[42] Cramer, StGB, 47. Auflage 1995, § 263 a Rdnr. 7.

[43] Cramer, in: Schönke-Schröder, StGB, 25. Aufl., § 263 a Rdnr.7; Tiedemann in: LK, 11.Aufl. 1998. § 263 a Rdnr. 32.

[44] Günther, in: SKStGB, 5. Aufl. 1996, § 263 a Rdnr. 23. Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 32.

[45] Günther, in: SKStGB, 5. Aufl. 1996, § 263 a Rdnr.4; Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 36.

「正確」；反之，若主張並不符合事實，則該事實之呈現為「不正確」[46]。又透過資料所呈現出之資訊，如果是與事實狀態不符合，則必然為不實（falsch）[47]。依據德國學者之說明，同於其他詐欺罪之立場，正確性概念是採客觀解釋與所依據的事實認定；預測、價值判斷等，唯有成為事實基礎時，才能列入考慮[48]。至於另一構成要件「使用不完整資料」是指資料無法讓人對事實狀態有充足的認識[49]，特別是藉由省略重要事實狀態，而扭曲事實狀態之意義[50]。再者，區分使用不完整資料與不作為之基本原則為：積極作為，亦即，隱匿部分資料，以致使資料所呈現之事實狀態成為不完全；而不作為則是以完整資料輸入為前提之說法[51]。

然在有些案例中，可能產生以下的難題爭論：濫用卡片行為是否構成「使用不正確資料」？有鑑於此，「無權使用資料」構成要件便產生。就目前德國刑法通說而論，此種型態的行為是依據「無權使用資料」構成要件來規範[52]。因此，有學者指出正確與否之問題必須與下一段「無權使用資料」的認定相區別，於「無權使用資料」行為中，判斷正確與否的標準，並非採所謂「詐欺相似性」而是「電腦特定性」，亦即，電腦未按原來程式設定而回應資料與資訊[53]。

---

[46] Günther, in: SKStGB, 5. Aufl. 1998, § 263 a Rdnr.3.
[47] Hilgendorf, JuS 1997, 131.
[48] Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 33.
[49] Cramer, in: Schönke-Schröder, StGB, 25. Aufl. 1997, § 263 a Rdnr.6.
[50] Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 34.
[51] Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 34.
[52] Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 35.
[53] Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 35.

(3)無權使用資料

「無權使用資料」此一構成要件所引起的爭議最多。此一構成要件也是在立法過程的最後階段才被放入本罪之構成要件中，其中原因便是實務在無權使用資料等相關問題的立場尚未明確[54]。

在前文討論資料概念時，曾論及「使用」一語之涵義，此問題的答案將影響下一個構成要件的適用範圍。如果「使用不正確或不完整資料」與「無權使用資料」一樣，都是指資料輸入行為，則後一種構成要件「其他無權影響資料處理過程」便具網羅性功能，用來掌握不涉及資料輸入的情形。目前，依據多數說見解，「無權使用資料」之「使用」亦是以資料輸入為前提[55]。

由於銀行自動櫃員機系統是以卡片與密碼來從事存取控制，在未獲授權下使用他人卡片與密碼時，由於這兩項資料都是系統運作的基礎，因此，自電腦系統設計本身的觀點而言，行為人使用的資料是客觀上正確的資料[56]。再者，由於未獲授權而輸入密碼與送入卡片，可被認為是無權使用資料之行為。基於以上之理由，立法者在立法理由中表示，引進德國刑法第二百六十三條 a 中之「無權使用資料」，期能規範冒用偷來卡片（伴隨密碼使用）之無權使用他人卡片與密碼而濫用自動提款機的行為[57]。

在「無權使用資料」構成要件中，「無權」的概念最引起爭議。有學說認為「無權」一詞之規定已違反罪刑法定原則之罪刑

---

[54] 關於德國刑法第二百六十三條a立法前自動櫃員機濫用行為相關問題爭議，請參見下文貳、三、（一）本文。

[55] Tiedemann in: LK, 11. Aufl. 1998. § 263 a Rdnr. 41.

[56] Tiedemann in: LK, 11. Aufl. 1998. § 263 a Rdnr. 40.

[57] BT-Dr 10/5058, S.30.

明確性原則。然而聯邦最高法院則採不同意見。聯邦最高法院援引用學者的主張[58]，認為「無權使用資料」此類一般性條款在刑法內處處可見，只要法官解釋時，透過行為必須與詐欺罪在結構上與不法價值方面具有等值性，同時參考針對本條所做成之判決，以足夠可預見的方式來限縮本構成要件之適用範圍，即不違反罪刑明確性原則[59]。

究竟何種行為才是構成要件所指的「無權」（ unbefugt）？依據學說與實務之見解，可歸納為以下三種：

(A)依據字義性解釋，認為「無權」使用資料是就違反權利人意思所為之使用；此說又被稱為主觀解釋方法。

(B)採取「詐欺相似性」解釋方法（die betrugsnähe Auslegung）或「詐欺特殊性」解釋方法（die betrugsspezifische Auslegung），而主張在無權使用資料行為中，必須存在一個「詐欺等值」行為。

(C)採取「電腦特定性」解釋方法（die computerspezifische Auslegung），僅從電腦處理過程觀點來判斷是否構成無權使用資料。

依據前述之主觀解釋方法，判斷行為人之行為是否構成「無權使用資料」，必須以是否違反契約之觀點而討論；而是否違反契約要看法益持有人（資料處理設備之經營者或設置者）事實上之意思或推測之意思。採主觀解釋方法之學者以 Mitsch 與 Bühler 為代表。Mitsch 認為，由於電腦詐欺罪所保護之法益是個人財產法益，因此在判斷「無權使用資料」問題上，法益持有人主觀之

---

[58] Lackner/ Kühl, StGB, 21. Aufl. 1999, § 263 a Rdnr. 2 .

[59] BGHSt 38, 120=NJW 1992, 445.

意思便居於關鍵性地位[60]。Bühler 主張，只要是在未取得資料處分權人同意而使用資料，便屬「無權使用資料」。因此，應該確定者為資料權利人之期望範疇（Erwartungshorizont）[61]。1994 年聯邦最高法院判決（BGHSt. 40, 334）便引用學者 Mitsch 與 Bühler 所提出之主觀解釋方法來判斷是否構成「無權使用資料」。

針對主觀解釋方法存有反對之見解。有學者即指出，主觀解釋方法所採之契約違反觀點有其缺點。此說將電腦詐欺罪內涵轉成純粹依據契約關係決定，這似乎不妥；故應採詐欺特殊性解釋方法[62]。此外，拒絕採用主觀解釋方法之學者，也認為單純違反民法上契約是不能建立刑法第二百六十三條 a 之可罰性。再者，如果採主觀說，顯然已將「無權使用資料」之構成要件放寬，使本罪所能掌握的情形，不僅包括那些與傳統詐欺罪相對應而應處罰之電腦操縱行為，尚及於不具應刑罰性的行為。例如，使用自己的密碼超額提款，此即係違反用戶與銀行間契約之違約行為；又或者，將自己卡片交給他人而他人從卡片持有人之戶頭逾額提款。

回到上引第二說，該說之基本主張是採取「詐欺相似性」解釋方法，要求行為人必須施行與欺騙行為結構上相似或不法內涵等值的行為[63]。1991 年 11 月 22 日聯邦最高法院（BGHSt 38, 120）之判決已使用「詐欺特殊性」一詞[64]。依此而論，在使用偽卡或偷來卡片時，由於行為人明知自己缺乏合法權限，並非合法權利人，在面對銀行員時，必須冒用合法權利人身份始能進行冒領，

---

60 Mitsch JZ, 1994 883f.
61 Bühler, MDR, 1991, 16.
62 Wessels/Hillenkamp, BT 2 § 13 VI 2 Rdnr. 609.
63 Lampe, JR 1988, 437.
64 BGH 38, 120=NJW 1992,445.

此必然已經是一種實施詐術行為。所以，適用電腦詐欺罪者為使用偽卡之無權利人者[65]；某個欺騙行為，如果對人施行時不會構成詐欺，第二百六十三條 a 便被排除而不適用。據此，第二百六十三條 a 僅包括那些缺乏對於人智力影響，與因此影響導致錯誤決定的案例，此即所謂「假設上相似性的涵攝需求」（ein änliches hypothetisches Subsumtionserfordernis）；此一概念也被適用在德國刑法第二六九條之偽造證據上重要電腦資料罪[66]。

第三說所主張之「電腦特性」解釋方法認為，要認定某個資料使用行為是否構成無權使用資料，必須取決於電腦資料處理系統之經營者，是否已經將反對此種資料使用行為之意思，表達於程式設計中；亦即，在設計程式時，是否已經將這種行為考慮在內[67]。對於電腦特定性解釋方法所提出之批評，可歸納為以下兩點。首先，如果採用此種解釋，將使本段之無權使用資料構成要件行為與前段之使用不正確資料行為之功能相重疊。舉例而言，假設電腦程式設計有辨識濫用行為之模組（Mißbrauchserkennungsmodule），並針對使用權限一事做出提問，而行為人又做出「有」權限之回答，那麼即可被認為已構成前段使用不正確資料之構成要件行為。此外，電腦特性解釋方法會使無權使用資料構成要件之適用範圍過於狹隘，亦使立法者明示要處罰的無權利者（偷卡者）濫用自動櫃員機之行為成為不可罰[68]。

---

[65] Günther, in: SKStGB, 5. Aufl. 1996, § 263 a Rdnr. 17; Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 48f.; Wessels/Hillenkamp, BT 2 § 13 VI 2 Rdnr. 60.

[66] Cramer, in: Schönke-Schröder, StGB, 25. Aufl., 1997, § 263 a Rdnr.2. Günther, in: SKStGB, 5. Aufl. 1996, § 263 a Rdnr. 17.

[67] Achenbach, JR 94, 295.

[68] Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 45.

(4)其他無權影響資料處理過程行為

「其他無權影響資料處理過程行為」之構成要件是為了規範前述行為以外，而尚未被知曉的操縱技術[69]。在最初的立法草案中，此網羅性構成要件並未被列入，但立法者考慮到將來若出現法條未規定的新操縱技術時，將因缺少網羅性構成要件，而形成不罰行為，因此，促使德國立法者參考奧地利刑法的規定，設計此一構成要件。

從「其他」(sonst)一詞可明白本構成要件屬於網羅性的構成要件，可用以規範不屬於輸入操縱之鍵盤操縱[70]與輸出操縱。輸出操縱的行為，如阻止資料之印出等[71]。此外，此構成要件亦可用來規範極少出現之硬體操縱，亦即透過硬體而影響資料處理過程的行為。雖大部分學者都認為本構成要件包括硬體操縱，然須先釐清之問題是，硬體操縱是否包含以暴力透過硬體操縱而影響資料處理過程的行為。例如，行為人拔掉資料處理機器的主電源插頭，使尚未被儲存的資料消失，以致於影響資料處理過程；或者，行為人對磁碟片製造煙霧致使電腦無法讀取載於其上的資

---

[69] Günther, in: SKStGB, 5.Aufl. 1996, § 263 a Rdnr. 21.

[70] 按，鍵盤操縱是指在資料輸入過程沒有人為的操作介入，電腦處理器處理的是正確的數值，但當電腦正在處理時，行為人從鍵盤為不正確的操作，使電腦產生不正確的電腦數值，最後與輸入操縱、程式操縱的情形相同，讓電腦輸出不正確的電腦數值。鍵盤操縱之所以不被列入輸入操縱範圍是因為此種類型專門用來與一般終端機輸入操縱相區別。一般的終端機是具備處理與儲存資料功能之個人電腦。即使不與主電腦連線，也能獨立處理資料。但有一種終端機只包含螢幕與鍵盤兩部分，而沒有儲存、計算與儲存資料的能力，常見於大型電腦系統（mainframe computer）之主控台（console），所連接之終端機只作為顯示資料與輸入資料之用。

[71] Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 62; Cramer, in: Schönke-Schröder, StGB, 25. Aufl., 1997, § 263 a Rdnr.5. Lackner/Kühl, StGB, 23. Aufl. 1999, § 263 a Rdnr. 15.

料等。有學者指出，受本構成要件規範之造成資料處理過程不正確運作之硬體操縱行為，都具有造成物毀損之特色，但與德國刑法第二百六十五條 a 的詐騙自動機器給付罪所不同者，乃是詐騙自動機器給付罪因受限於構成要件行為「詐騙」一詞之故，須排除暴力行為；而本構成要件「影響資料處理過程」，則利用「無權」來限制其適用的範圍[72]，故係採取較寬的解釋立場。

就事實而論，在適用本構成要件時，所面臨的最困難點仍係「無權」一詞的涵蓋範圍。有些學者認為所採之標準應同於第三段之「無權使用資料」，要求在價值與結構上須對稱於詐欺罪之欺騙行為。舉例而言，影響須使資料處理過程發生錯誤，繼而致使資料處理結果成為不正確[73]。雖有學者主張必須具備詐欺相似性，但為避免被批評違反構成要件明確性原則，故採限制解釋方法，將本構成要件行為限制於沒有「使用」資料，但卻可以「無權」影響資料處理過程的行為類型，例如以詐欺相似性或欺騙特殊性方式，運作資料處理過程，並造成結果[74]。或者，有學者主張，為了達成限制解釋目的，應與第一段與第二段之「編制不正確程式」與「使用不正確資料」相配合，將此種影響限制在，在輸入正確資料條件下，進行不正確資料處理[75]。

綜合分析德國學者對「其他無權影響資料處理過程行為」構成要件之解釋可知，本款所稱之無權影響資料處理過程之行為，基本上是排除前述三種足以影響資料處理過程的行為，亦即，排除資料的程式、輸入操縱或使用。但較有爭議者是，有學者認為唯有具詐欺相似性或詐欺特殊性的無權行為，才與詐欺行為等

---

[72] Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 62.
[73] Günther, in: SKStGB, 5. Aufl. 1996, § 263 a Rdnr. 22.
[74] Lackner/Kühl, StGB, 23. Aufl. 1999, § 263 a Rdnr. 15.
[75] Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 63.

值，亦方能構成本構成要件行為[76]。對此項主張，有學者提出不同意見，認為如此的主張與本條第一項第一段「編制不正確程式」中涉及「不正確」概念的解釋一樣，都是想像性的。就事實而言，如欲影響人類思維與意思決定過程，除了對之提供不正確資料外，其餘方法皆與欺騙無關，如過度疲勞、酩酊大醉等。相同的道理，在影響電腦處理過程之情形，亦不限於具備詐欺相似性或詐欺特殊性之行為，方能構成[77]。

2.構成要件結果

經由上述四種型態行為的實行，所產生者為「影響資料處理程序之結果」與「財產上損害」。茲分別說明如下：

(1)影響資料處理程序之結果

首先，「影響資料處理程序之結果」之「影響」是否必須以已經在進行中的資料處理程序為前提？舉例而言，在使用卡片提款的案例中，是否在使用卡片提款時，方才啟動銀行主機資料處理過程？事實上，構成要件所規定之資料處理程序並不以已經在運作為前提，行為人尚可藉由對資料處理程序的中斷或啟動而產生影響[78]。資料處理程序之結果之影響，也可指行為人為達到「其他的結果」而使用特定方法啟動因果歷程。此處所指之「其他的結果」，如提款機向權利人為給付[79]。

依據立法者之設計可知，「影響資料處理程序之結果」是用

---

[76] Lackner, StGB, 21. Aufl. 1995, § 263 a Rdnr.15.

[77] Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 26.

[78] Günther, in: SKStGB, 5 Aufl. 1996, § 263 a Rdnr. 23.

[79] Cramer,in: Schönke-Schröder, StGB, 25. Aufl. 1997, § 263 a Rdnr.6; Dreher-Tröndle, StGB, 45. Aufl., § 263 a Rdnr.6.

來取代傳統詐欺罪之「陷於錯誤」與「因錯誤所產生之財產處分」。因為經由構成要件所指出之行為方式，諸如，編制不正確程式、使用不正確或不完整資料等，在技術上必然會導致「錯誤」結果的產生，因此符合傳統詐欺罪所要求之「財產上處分行為」。不過，有刑法學者指出，不管就哲學上本體論（ontologisch）或價值論（wertungsmäßig）而言，兩者概念並不相同[80]。詳而言之，在以人為對象的詐欺行為，必須被欺騙者在行為人所實施詐術誤導下，得出錯誤的意思表示；但在電腦詐欺罪之構成要件「影響資料處理程序之結果」中，被影響之資料處理結果並不一定是「不實」的結果。又就上述第三種「無權使用資料」與第四種「其他無權影響資料處理過程」兩種構成要件行為而論，這些行為僅啟動「正確」資料處理程序[81]。至於所謂的「影響」，是指在這些行為介入後，資料處理程序之結果與在沒有介入下、完全依據原先程式設計之處理程序之結果，有所不同[82]。

再者，受影響之資料處理程序結果是指中間結果而言[83]。在此，必須強調的是，影響資料處理程序結果之行為並不以直接引起財產上處分為必要。換言之，財產上處分行為是電腦處理後之結果，亦即，資料處理後直接引起財產上之損害結果[84]，並不直接取決於行為人之輸入資料等行為[85]。此等「直接性」便是詐欺罪與竊盜罪之區別所在。因此若缺少電腦之處分行為，僅構成竊盜罪而已。換言之，竊盜罪之行為人必須自己從事導致持有移轉

---

80 Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 26.

81 Lackner-Kühl, StGB, 23. Aufl.,§ 263 a Anm. 22.

82 Cramer, in: Schönke-Schröder, StGB, 25. Aufl. 1997, § 263 a Rdnr.22; Tiedemann in:, LK, 11. Aufl. 1998, § 263 a Rdnr. 26.

83 Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 26, 65.

84 Tiedemann, JZ 86, 869.

85 Tiedemann, JZ 86, 869; Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 26.

之行為，例如，當行為人藉由無權使用密碼而打開自動化門鎖之際，僅取得進入之可能性，行為人尚須從事持有移轉行為方構成竊盜罪[86]。

承上所述，「影響資料處理程序之結果」構成要件之功能在於代替傳統詐欺罪中之「錯誤」與「財產上處分」，電腦詐欺罪即是以此要件和詐欺罪、竊盜罪相區別；其與詐欺罪相同者乃是，兩者皆為「自我損害犯」（Selbstschädigungsdelikte）[87]。

⑵財產上損害

依德國通說之見解，電腦詐欺罪之「財產上損害」與傳統詐欺罪相同，皆無須造成實害，僅須形成財產上之具體危險即可[88]。進而言之，當發生財產上實害或具體危險時即屬既遂；又終了時是指最後財產利益取得之時[89]，均與詐欺罪之判斷相同。再者，在傳統詐欺罪之架構下，行為人希望取得之利益與被害人（不一定要是受騙者）財產上所發生之損害間須具有「內容相等」（Stoffgleichheit）之關係[90]。易言之，財產上處分行為將同時在一方產生「損害」，另一方產生「得利」，其損害與得利間具有對等關係[91]。據此而論，在電腦詐欺之情形，符合「內容相等」之

---

[86] Samson, in: SKStGB, 5. Aufl. 1994, § 263 a Rdnr. 13.

[87] Günther, in: SKStGB, 5. Aufl. 1996, § 263 a Rdnr. 24.

[88] Tröndle/Fischer, StGB, 49. Aufl. 1999, § 263 a Rdnr.11; Lackner-Kühl, StGB, 23. Aufl.1999,§ 263 a Rdnr . 18.

[89] Cramer, in: Schönke-Schröder, StGB, 25. Aufl., 1997, § 263 a Rdnr. 38; Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 77.

[90] 「內容對等」一詞之翻譯，參見黃榮堅，「刑法題解—關於詐欺等財產犯罪」，收錄於氏著，《刑法問題與利益思考》，1995年6月初版，頁96；林東茂，「詐欺罪的財產損害」，警大法學論集第三期，頁200。

[91] Cramer, in: Schönke-Schröder, StGB, 25. Aufl. 1997, § 263 Rdnr. 53; Tröndle-Fischer, StGB, 49. Aufl. 1999, § 263 Rdnr. 39.

要件為，行為人須希望被操縱之電腦資料處理結果導致財產上損害；若行為人僅希望藉由上述的幾種操縱行為，對電腦硬體與軟體造成損害，則此情形並不符合上述之要求；又為了消除損害，讓電腦重新運作所支出之費用，由於並非行為人所取得之利益，因此亦不符合上述之要求[92]。

由電腦所進行之財產上處分行為，並不當然涉及電腦系統經營者之財產；在某些情形下，可能涉及第三人之財產處分，而使第三人受有損失；依據通說之見解，若符合適用詐欺罪時所建立之基本原則與標準，例如，財產處分者與受損者間因具有密切關係，則電腦詐欺罪仍有三角詐欺（Dreieckscomputerbetrug）之適用；其若不具學說上所提出之密切關係要件，則屬於竊盜罪或其他類型之他人損害犯罪之間接正犯。

有學者認為電腦詐欺行為本身就是以三角詐欺型態為基本結構[93]，據此可另以「電腦三角詐欺」一詞與「通常三角詐欺」相區別；然其所產生的問題是：僅在少數案件中，電腦經營者本身會是受損者，此時從事處分行為之電腦與電腦經營者（受損者）間，具有通說所要求處分者與受損者間之密切關係。但在大多數電腦詐欺之案例中，皆係受程式支配之電腦損害了第三人（銀行客戶）利益，因此，很難去建構銀行電腦與銀行客戶間的密切關係，故有學者建議在電腦詐欺下應該放棄傳統三角詐欺所建立之一般原則。如行為人影響銀行所有之資料處理設備，以致於客戶受有財產上損害，在此種情形下，須放棄傳統詐欺罪為了使財產上處分行為歸屬於財產權人所發展之「立場理論」（Lagertheorie）

---

92 Tröndle-Fischer, StGB, 49. Aufl. 1999, § 263 a Rdnr. 11; Lackner-Kühl, StGB, 23. Aufl.1999,§ 263 a Rdnr . 25.

93 Mitsch, Jus 1998, 314.

[94]。因銀行的資料處理設備不可能是受騙者，故不必去探討處分者與受損者間是否具備密切關係，行為人只須直接依據德國刑法第二百六十三條 a 處罰[95]。此外，屬於得適用傳統理論之案例為，當出現系統經營者被騙得情況時，舉例而言，行為人欺騙系統經營者而讓他設計錯誤程式以致於造成銀行客戶損害，並使自己得利。此情形即屬通常三角詐欺類型，可以依據德國刑法第二百六十三條處罰，因受騙之系統經營者與銀行客戶間具有通說所要求處分者與受損者間之密切關係[96]。

但亦有學者不認為電腦詐欺為三角詐欺。假設是銀行行員對假裝為合法持卡人支付之情形，他是銀行代表，而銀行對客戶帳戶內金錢有處分權；因此，他與銀行、銀行與銀行客戶都有密切關係。在此情形，銀行地位就是傳統詐欺罪之受騙者與財產處分者。這種關係不會因為付款自動化因素而受影響；又若將行員改成電腦，不同於行員是銀行之代表，電腦是系統經營者（銀行）之助手，電腦對客戶帳戶內金錢之處分應該視為經營者之處分行為，此處分行為雖非由財產權人所為，但可因為處分者（銀行）與受損者（客戶）間具有上述密切關係而認為是自我損害行為[97]。因此，可以認定電腦所進行的處分行為屬於詐欺罪構成要件之處分行為，故符合傳統詐欺罪之要件，亦同時符合電腦詐欺之解釋上要求。

最後，在傳統詐欺罪，施行詐術行為具有作為（虛構事實）

---

[94] 「立場理論」一詞之翻譯是引用林東茂教授之翻譯，參閱，林東茂，「詐欺或竊盜-一個案例的檢討」，刑事法雜誌，第43卷第2期，頁54。

[95] Haft, Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG), NStZ 1987, 8.

[96] Bühler, Ein Versuch, Computerkriminellen das Handwerk zu legen: Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität, MDR 1987, 449, 451.

[97] Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 71.

與不作為（隱瞞真相）兩種方式，故在電腦詐欺罪中，其亦有可能以不作為方式構成本罪。舉例言之，經營者或其他保證人（例如長官）知悉輸入資料人員(例如下屬)輸入不正確資料時容忍而不制止，以致影響資料處理過程，進而造成財產上損害[98]。

㈢主觀不法構成要件

在電腦詐欺罪之故意在於，行為人認識並希望「因」被無權操縱之資料處理程序之結果「而」取得不法利益。但如果行為人誤認自己是有權進行資料操縱，則屬於構成要件錯誤[99]。又除了電腦詐欺行為之故意外，尚須具備特別主觀不法構成要件之「意圖為自己或第三人取得不法利益」。

二、相關條文間之關係

㈠電腦詐欺罪與詐欺罪之關係

德國刑法第二百六十三條a電腦詐欺罪與德國刑法第二百六十三條傳統詐欺罪無論在結構上或價值上均具有等值性，二者間有構成要件排他性的關係。因為財產的支配不是由陷於錯誤的人作成，就是由電腦等自動設備所為[100]。因此，依據立法者之意思與學說，在適用上基於漏洞填補之性質，若當中過程有人的意思決定介入，而能被認為被欺騙，則電腦因只基於工具的地位，仍適用原來詐欺罪處罰，電腦詐欺罪因而無適用之餘地[101]。舉例言

---

98 Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 64.

99 Lackner/Kühl, StGB, 23. Aufl. 1999, § 263 a Anm. 24.

100 Samson, in: SKStGB, 5. Aufl. 1994, § 263 a Rdnr. 5.

101 Lackner/Kühl, StGB, 23. Aufl.1999, § 263 a Anm. 28; Günther, in: SKStGB, 5.

之，行為人偽造支票，欺騙具有處分權限之銀行行員，並讓該行員使用電腦進行資料處理，則此案例適用詐欺罪。再依據學說之見解，倘資料處理結果，對行為人而言，僅屬於施行詐術之工具，則僅構成詐欺罪[102]。又在所謂的「輸出操縱」中，若行為人影響電腦輸出物，則由於有人為的介入，所以不會構成電腦詐欺罪[103]。

㈡電腦詐欺罪與竊盜罪、侵占罪之關係

如上文所述，本罪與詐欺罪間具有構成要件排他關係，但本罪與竊盜罪、侵占罪之關係為何？討論此問題之實益在於回答，當一行為同時可以適用電腦詐欺罪與竊盜罪或侵占罪時，應該如何競合的問題。

在此須先說明者，本罪之立法目的在於彌補可罰性漏洞。例如，在濫用卡片提款的案例中，由於德國實務上多數說認為使用偽卡或偷來之真卡從自動櫃員機冒領現金的行為，並不構成竊盜罪，因此存在可罰性漏洞。至於是否構成侵占罪，在這些法院中仍有爭議。但大多數學者卻不贊同實務見解，認為電腦詐欺罪立法之實用性有限。除了有些學者不區分偽卡或無權取得之真卡，而主張冒領均構成竊盜罪外，另有學者認為，如果使用偽卡，則構成竊盜罪，而使用真卡，由於卡片與密碼都是在符合通常規則下使用，並不構成竊盜罪。因此，才有所謂處罰上漏洞必須藉助德國刑法第二百六十三條 a 來填補[104]。

不管如何，認為無權使用卡片（偽卡或真卡）於自動櫃員機

Aufl. 1996, § 263 a Rdnr. 24. Tiedemann in: LK, § 263 a Rdnr. 17.

102 Wessels/Hillenkamp, BT/2 § 13 VI 2 Rdnr 603.

103 Tiedemann, JZ 86, 869.

104 Otto, Zum Bankautomatenmißbrauch nach Inkrafttreten des 2. WiKG, JR 1987, 225.

冒領現金行為構成竊盜罪之學者都採取這樣立場：在本罪通過後，可以依據電腦詐欺罪論處，但在本罪立法前，已有竊盜罪或侵占罪（請參閱下文之說明）作為規範基礎。這不會因為本罪之立法而受影響[105]。由於可以同時適用電腦詐欺罪、竊盜罪或侵占罪，如何處理上述條文間之競合關係，便成為學說討論之重點。

關於上段所提出之問題，存在以下幾種不同立場。第一說主張，本罪與竊盜罪之關係類似於詐欺罪與竊盜罪之排他性擇一關係。傳統詐欺罪與竊盜罪的分界線在於：在詐欺罪，行為人所造成之財物或利益上損害，是來自被害人自己瑕疵之意思決定與處分行為，學說上稱為「自我損害犯」（Selbstschädigungsdelikte）；而在竊盜罪中，被害人之財物損害是來行為人之竊取行為，屬於「他人損害犯」（Fremdschädigungsdelikte），因此，兩者間有排他關係。又因詐欺罪與竊盜罪有排他性關係，故與詐欺罪同屬同一類型之電腦詐欺罪，亦如同詐欺罪一樣與竊盜罪間具有排他關係。而就區分竊盜罪與電腦詐欺罪之方法而論，仍承襲傳統之「他人損害犯」或「自我損害犯」標準，因此兩者具有排他性擇一關係[106]。

第二說認為，本罪乃竊盜罪或侵占罪之特別規範，故排斥竊盜罪或侵占罪之適用，德國聯邦最高法院刑事庭（BGH, Urteil vom 22.11.1991）即採本說。同時亦有學者指出，在濫用卡片取得現金之案例中，本罪之立法史已清楚呈現出此立場[107]。

此處之特別規範係指立法者特別針對電腦濫用而立法，對於

---

105 Ranft, Der Bankomatenmißbrauch, wistra 1987, 84.

106 參閱 Günther, in: SKStGB, 5. Aufl. 1996, § 263 a Rdnr. 24. Tiedemann in: LK, 11.Aufl. 1998 § 263 a Rdnr. 65.Wessels/Hillenkamp, BT/2 § 14 I 1 Rdnr. 613. Ranft, Der Bankomatenmißbrauch, wistra 1987, 84.

107 Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 17, 84.

刑法分則中那些保護所有權與其他財產利益之構成要件（例如竊盜罪與侵占罪）而言，屬於特別規定；至於沒有電腦針對性之其他財產犯罪構成要件，則應該被電腦詐欺罪所排除，無須適用。因此，學說上認為電腦詐欺罪對竊盜罪與侵占罪而言，係屬於特別條款，因此電腦詐欺罪構成要件優先於竊盜罪與侵占罪構成要件之適用[108]。

第三說認為，本罪被設計來彌補法律漏洞，性質上屬於居於補充性質之網羅構成要件[109]。如果採用本說而認為本構成要件屬於補充地位之網羅構成要件，則無法如同第二說一樣，能夠排除諸如刑法第二百四十二條竊盜罪與刑法第二百四十六條侵占罪等包含取得犯構成要件（Zueignungstatbestande）之「所有犯」（Eigentumsdelikte）適用。採此說之學者引用聯邦最高法院在討論第二百三十九條 a 與第二百三十九條 b 效力範圍時，所曾表示過之立場：除非立法者確實有此意思，否則僅是與情況有關之特別規範不能改變刑法分則之原來結構。因此，主張此說之學者認為，聯邦最高法院所揭示之此原則亦應可適用於德國刑法第二百六十三條 a。據此以論，為避免改變刑法分則財產犯罪之基本結構，仍應以傳統罪名之適用為優先，僅是當竊盜罪或侵占罪無法適用時，再以次要地位進行補充，避免法律漏洞產生。再者，本罪較竊盜罪與侵占罪，有較高的法定刑，因此，若將電腦詐欺罪視為補充規範，僅用來網羅不能被傳統詐欺罪所處罰之行為，而不使負有任務去加重處罰竊盜行為或侵占行為的話，將較能符合

---

108 Ranft, Zur "betrugsnahen" Auslegung des 263 a StGB, NJW 1994, 2576; Cramer, in: Schönke-Schröder, StGB, 25. Aufl. 1997, § 263 a Rdnr. 26; Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 17, 84.

109 Ranft, NJW 1994, 2577.

法治國人民權利保障之精神[110]。

㈢電腦詐欺罪與背信罪之關係

有學者認為德國刑法第二百六十三條a應該被立法者置於背信罪章中，沒有如此作的原因在於，德國刑法第二百六十三條 a 所規範的事實關係並不能完全由背信罪所掌握，所以仍須另行設立新的法條。因此，當本身沒有擁有事務決定權的下層職員從事本條所規定的行為時，便無法適用背信罪，僅得以第二百六十三條 a 規範。

㈣電腦詐欺罪與偽造技術紀錄罪

1969 年德國刑法加入刑法第二百六十八條有關偽造技術紀錄的特別構成要件。歷來通說之見解皆認為，經由程式不當操作而被改變之電腦程式並非第二百六十八條所規定的「技術的紀錄」。至於輸入的不當操作行為亦不能適用德國刑法第二百六十八條第三項之「行為人在製作紀錄過程中進行干擾，影響紀錄結果者，視同製造不真實之技術紀錄。」易言之，輸入的不正操作行為並非德國刑法第二百六十八條第三項所要求之「經由紀錄過程中的妨害作用而影響紀錄的結果」的行為。所以，在為取得財物或得利而為電腦操縱之領域，並無適用德國刑法第二百六十八條之餘地。

三、個別類型行為之討論

與本條適用有關之案例，共計有以下幾種類型：㈠自動櫃員

---

[110] Ranft, Der Bankomatenmißbrauch, wistra 1987, 84.

機濫用。㈡賭博性遊戲機之濫用。㈢視訊資訊系統濫用。茲於下說明之。

㈠自動櫃員機之濫用

使用正確資料提領現金的行為，在刑法上究應如何評價，在本罪立法前，德國實務上並無一致見解。在早期，有些地方法院認為此類型為可構成竊盜罪；而有些法院（包括聯邦最高法院）卻認為不能構成竊盜罪。然在新法修正後，德國刑法第二百六十三條 a 的適用問題，開始在實務上產生熱烈討論。茲於下文分別就以下之四種類型行為說明之。

1.使用偷來的原始卡片提款

在德國刑法第二百六十三條 a 制定後，德國聯邦最高法院刑事庭 1987 年 12 月 16 日針對自動提款機濫用案件所為之第一則判決（BGHSt 35, 152），即是針對使用合法提款卡提領現金的行為。該案之事實為：被告竊取其兄之提款卡，且在得知該卡片之密碼下，使用這張卡片提走 5100 馬克。但因之後便予以返還卡片，故不具永久性剝奪卡片持有之意圖。

聯邦最高法院認為，被告的行為對卡片本身和所提領的現金而言，皆不構成竊盜罪[111]，但卻可認為構成侵占罪。此判決雖然

---

[111] 聯邦最高法院認為，從自動櫃員機提走他人存款的整個行為過程不能被評價成「他人持有破壞」之竊取行為。使用偷來的真卡可以啟動機器之運作（達到符合原來設定功能運作之條件），在此同時，也完成財產移轉。因程式運作所導致之現金送出，可視為金融機構「同意」喪失對現金之持有。由於不存在持有之破壞，被告並非竊取銀行之金錢。只要一切都是在符合機器預設功能下，現金就會被「交付」給卡片使用者。此「交付」之性質不會因為卡片是由無權使用者使用而被認為不存在。「交付」與「竊取」是相對立，如果是「交付」，就不是「竊取」。聯邦最高法院因此否定竊

是本法通過後所形成，然因行為發生在施行前，故並未針對刑法第二百六十三條 a 之電腦詐欺罪的適用問題進行討論。不過，學說上普遍都針對此種案例類型進行討論。

採取主觀解釋論者認為，行為人之行為因違反權利者之意思，亦即，違反原卡片合法持有人之意思而使用卡片[112]，或者，因違反與銀行間之契約條件而可認為違反銀行意思[113]，而構成無權使用資料之電腦詐欺罪。又如果依據詐欺特定性解釋可以為以下的說明：當行為人面對銀行行員時需要從事詐術行為，亦即，行為人提示卡片時必須冒用他人名義，並且也必須對卡片不屬於行為人一事進行欺騙，因此，在合法使用卡片權限上存在一個可得推知之詐術行為[114]。再者，由於電腦是透過輸入正確（真的）卡片與附隨於該張卡片之密碼來確認身份同一性與權限，故如何運用電腦特定性解釋方法，始能達成當初立法者希望處罰這種類型行為（使用偷來真卡）之目的，可能有些疑問[115]。

2.使用偽造卡片提款

德國刑法第二百六十三條 a 制定後，德國聯邦最高法院刑事庭關於自動提款機濫用案件所為之第二則判決（BGHSt 38, 120）即是針對使用偽造的提款卡提領現金行為所為。聯邦最高法院認為，只要符合機器預設之功能運作而取走現金，此一過程即不能被評價為「他人持有之破壞」，因此不構成竊盜罪[116]，亦非侵占

盜罪的成立。

112 Hilgendorf, Jus 97, 134.

113 Maurach/Maiwald, BT/1 § 41 Rdnr. 233.

114 Meier, JuS 1992, 119.

115 Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 49.

116 德國聯邦最高法院認為，被取走現金的帳戶對銀行是有存款債權，而且該

罪[117]，行為人應被論以刑法第二百六十三條 a 之電腦詐欺罪。

該案例的概要事實如下：被告利用自製機器在銀行的自動櫃員機上側錄許多他人的銀行帳戶與密碼資料，並將這些資料轉錄到空白卡片以製造提款卡；最後，使用這些提款卡提走他人帳戶內的存款，總計大約為 14 萬馬克。可能是因為自動櫃員機內並不具備對使用虛假卡片行為作出反應的安全系統，又或是因為系統本身有瑕疵，使行為人能在自動櫃員機仍保持運作下，成功地將錢提走。審理本案之地方法院判處被告犯加重竊盜罪、電腦詐欺罪與偽造證據性電腦資料罪；該案被告不服提起上訴，要求法院廢棄有關竊盜罪部分的判決。最後，聯邦最高法院判決廢棄下級審關於加重竊盜罪之判決，認為使用偽造的提款卡從自動櫃員機提走金錢，應成立刑法第二百六十三條 a 之電腦詐欺罪而非竊盜罪或侵占罪。在此僅就聯邦最高法院就電腦犯罪部分之判決說

偽造的卡片也被銀行接受，所以該行為人是在符合程式預設功能的運作下，使用自動櫃員機，並因此使得現金持有狀態產生變化。前述之促使持有移轉之過程確實是來自物之持有人當時的決定(程式決定)。透過機器內部的電腦程式所設定的標準，以代替人去審查操作機器之人是否有權去提領現金。所以，取得現金行為不構成他人持有之破壞。再者，聯邦最高法院表示，是否構成「交付」現金，被儲存在提款卡上磁條內的資料(正確的資料)是決定性的關鍵。即使被告使用的卡片不是銀行發行的而是被告自己複製，不會改變法院在符合機器預設功能運作這一點上之認定。參見，BGHSt 38, 120=NJW 1992, 445.

[117] 德國聯邦最高法院援引學者Lackner見解而表示，侵占罪之成立以行為人在取得行為前已持有，或取得行為同時持有或占有他人之物即可（「小範圍糾正解釋」（kleine Berichtigete Auslegung））。在本案例中，當行為人實施電腦詐欺罪之構成要件行為時就已經將現金據為己有。之後不可能再有重複之據為己有行為，而有適用侵占罪之餘地。因此，不構成侵占罪。對此部分，學者之批評主要是認為，行為人並沒有重複取得問題，而是在取得現款之同時，完成了電腦詐欺罪與侵占罪之構成要件。依據目前通說見解，此行為構成侵占罪，不過由於電腦詐欺罪為特別規範，因此，不必適用侵占罪。參見，BGHSt 38, 120=NJW 1992, 445.Cramer, in: Schönke-Schröder, StGB, 25. Aufl. 1997, § 263 a Rdnr.41.

明：

此一判決是採用「詐欺相似性」或「詐欺特殊性」解釋下所產生的結果。首先，將自動櫃員機假設成自然人，機器因把偽卡當成真卡，在此影響下決定支付，因此，滿足了傳統詐欺罪所需要的構成要件。聯邦最高法院認為，行為人讓機器做成「不正確決定」，而此不正確決定讓行為人得以取走現金；並因機器做了不正確決定，因此，構成「詐欺」。法院並表示，立法者將新的規定引入刑法就是希望使用新的電腦詐欺罪條文去掌握於自動櫃員機上濫用歐洲支票卡之行為，特別是，無權使用他人密碼之濫用自動櫃員機行為[118]。

由以上所述可知，採取客觀解釋立場的聯邦最高法院認為，假設面對行員提款時，行為人必須就自己是擁有權限一事進行欺騙，那麼，行為人使用偽造卡片提款行為已構成無權使用資料之電腦詐欺罪。此外，由於使用偽造卡片已違反銀行與帳戶所有人之意思，故此種案例類型若採主觀解釋方法，仍可肯定構成無權使用資料之電腦詐欺罪。然在此案例中，若係附隨在程式中的安全設置失效或有瑕疵，從電腦特定性之觀點而論，是否構成無權使用資料之電腦詐欺罪，可能較有疑問[119]。

3.使用自己卡片溢領

使用自己卡片溢領的行為，在電腦詐欺罪條文施行後，是否構成電腦詐欺罪，則有爭議。實務上存有數則上級法院的判決；舉例言之，1987 年 Stuttgart 高等法院採取主觀說而主張，合法卡片持有人若溢領，因超過銀行所授與之額度，明顯已違反契約，

---

[118] BGHSt 38, 120=NJW 1992, 446.

[119] Tiedemann in: LK, 11. Aufl. 1998, § 263 a Rdnr. 48.

構成電腦詐欺罪之構成要件「無權使用資料」。行為人因違反與被害人間的內部限制條件，故行為人的行為已然是違約[120]。

學說上，贊同使用自己卡片溢領行為構成「無權使用資料」者為通說[121]。學說上討論此一問題時，多採取詐欺相似性解釋方法而主張，使用自己的卡片超額提款，因存有與傳統詐欺罪相對應之施行詐術行為，亦即，倘若銀行行員在場，在支付前必然會先檢驗帳戶狀況，此時便不會發生金錢支付超過預定額度的情況，因此，此時行為人需要一個可得推知之詐術行為，來隱瞞戶頭不足額的情形，故有一個與施行詐術等值的行為存在。然須注意的是，亦有學者認為，在面對銀行行員超過額度之提款，行為人有可能沒有施行詐術。相同道理，合法持卡人超出銀行所授權之範圍，違反與銀行間之契約而超過預定額度之溢領行為並非實施詐騙行為[122]。可能要檢討的是否可以適用背信罪構成要件。不過，在適用上也有些困難，因為行為人與被害人之間通常都沒有法律行為而有處理事務之關係[123]。此外，因為歐洲支票卡之雙重功能，可用於提款與開立支票，因此，也有學說主張可以適用德國刑法第二百六十六條 b 支票卡或信用卡濫用罪[124]。

---

120 OLG Stuttgart, 23.11. 1987-3 Ss 389/87= NJW 1988, 981.

121 Maurach/Maiwald, BT/1 § 41 Rdnr 233. Günther, in: SKStGB, 5.Aufl. 1996, § 263 a Rdnr. 19. Cramer, in: Schönke-Schröder, StGB, 25. Aufl., 1997 § 263 a Rdnr. 19; Tröndle-Fischer, StGB, 49. Aufl. 1999, § 263 a Rdnr.6.

122 Günther, in: SKStGB, 5 Aufl.1996, § 263 a Rdnr. 19. Cramer, in: Schönke-Schröder, StGB, 25. Aufl., 1997, § 263 a Rdnr. 19; Tröndle-Fischer, StGB, 49. Aufl., 1999, § 263 a Rdnr.6.

123 Günther, in: SKStGB, 5. Aufl. 1996, § 263 a Rdnr. 19. Cramer, in: Schönke-Schröder, StGB, 25. Aufl. 1997, § 263 a Rdnr. 19

124 關於德國刑法第二百六十六條b支票卡或信用卡濫用罪之討論，本文擬於另一篇文章介紹在此略過對此問題之討論。

4.超出授權溢領

1991 年 Köln 高等法院針對以下案例，作成構成電腦詐欺罪之判決。本案例事實摘要如下：卡片之合法持有人甲將他的卡片交給乙並且告知密碼，以便讓乙能夠從自動櫃員機提款。後來乙又在未得甲同意下從他的戶頭提領現金。修法前之解決方法是將此情形類比於使用偷來的卡片提款。由於一切遵照程序，依據實務向來所採之符合功能設定即未違反意思或未得同意而取走現金之立場，不構成竊盜罪。自本法修正通過後，Köln 高等法院認為不構成電腦詐欺罪，而應以背信罪論處。

Köln 高等法院採取「詐欺相似性」或「詐欺特殊性」解釋，認為行為人並沒有施行與詐術等值之行為，因此，不構成電腦詐欺罪。在此判決中，法院表示，交付第三人卡片與告知密碼雖已經違反與銀行間之契約，但此契約違反行為尚未達「無權」使用。此種行為並未具有詐術之非價性，因為行為人並未對外假裝出自己是有權限者。再者，契約之所以禁止將卡片交給他人使用，目的在於禁止濫用卡片，但並不禁止卡片持有人以合法方式透過第三人從自己戶頭領錢。在本案中，由於取得卡片是來自於合法持卡人移轉，就外部關係而言，被授與權限是有效的，因此，當行為人面對銀行職員時並不需要去以可得推知之詐術行為去欺騙職員，使他誤信在內部關係也是有權限的[125]。

針對前述法院之判決，有學者提出不贊同意見而表示，在此類案件中，如果對無權使用之判斷採取主觀意義，取決於卡片與密碼之使用是否違反自動櫃員機設置者事實上存在或推測的意

[125] OLG Köln, 9.7. 1991-Ss 624/90= NJW 92, 126f. Günther, in: SKStGB, 5 Aufl. 1996, § 263 a Rdnr. 19. Cramer, in: Schönke-Schröder, StGB, 25. Aufl. 1997, § 263 a Rdnr. 19; Tröndle-Fischer, StGB, 49. Aufl.1999, § 263 a Rdnr.6.

思。據此以論，將卡片交給第三人使用已經違反持卡人與銀行間所訂立之定型化契約，亦即違反銀行經營者之意思[126]。行為人違反與被害人間之內部限制條件，因此，行為人的行為已經是違約。據此，則行為人之行為構成「無權使用資料」[127]。

㈡賭博性遊戲機之濫用

在第二次經濟犯罪對策法制定前，德國所發生之賭博性遊戲機器之攻擊型態，屬於相對上簡單的方式。對賭博性遊戲機器之影響，如果是以狡猾方式，從機器內取出現金，通常被論以竊盜罪。現代電腦技術使手段精緻化成為可能，此亦使刑事審判工作變得更加困難。從已發生的案例中可知，行為人先無權取得遊戲機器程式，之後利用已經被無權下載到磁碟片上之程式，輔以電腦，而得以算出何時啟動遊戲機之機率按鈕，可以有較高的贏率，並藉以取得現金。刑法上如何評價此類行為，雖在不同法院間產生爭議，但一致性的看法是，關於所贏得之現金，既不構成德國刑法第二百四十二條竊盜罪，亦不構成德國刑法第二百四十六條侵占罪，且無德國刑法第二百六十五條 a 之詐騙自動機器給付罪之適用。理由與濫用自動櫃員機之情形類似，不構成竊盜罪的理由在於，行為人取走現金已符合機器所設定之條件，並未構成違反機器設置者之意思。又排除適用侵占罪的理由在於遊戲者取得的現金是直接來自於機器，因此不具備侵占自己所持有之他人之物要件。

各法院間之爭議主要在如何適用德國刑法第二百六十三條 a 電腦詐欺罪。關於法院間之爭議，可引述以下幾則判決作為參

---

[126] BGHSt 40,335; Hilgendorf, Jus 97, 132.

[127] Maurach/Maiwald, BT/1 § 41 Rdnr 233.

考。以 1990 年 Bay 高等法院之判決為例，法院認為操作遊戲機之機率按鈕可構成刑法第二百六十三條 a 第一項第三段之「無權使用資料」或第一項第四段之「無權影響資料處理過程」。法院認為行為人之行為構成「無權」的理由在於，機器之設置者同意行為人進行遊戲的前提是遊戲者並不知悉遊戲機內運作程式。而知道程式資訊之行為人已超越事實上或可推測意思之同意範圍，因此行為人之行為屬於「無權」。

此外，1994 年聯邦最高法院判決（BGHSt. 40, 334f）曾引用學者 Mitsch 與 Bühler 所提出之主觀理論來判斷是否構成「無權使用」。法院表示：「由於電腦詐欺罪與詐欺罪所保護之法益皆為個人財產法益，因此在判斷此問題上，法益持有人之主觀意思便居於關鍵性地位；只要有合理根據，同時又在外在可見的範疇內，則法益持有人之期望範疇是不能不被列入考慮的。在本案中，遊戲者在機器上所從事之行為，並未得遊戲機經營者明示、默示之同意，或者，可得推知之同意，故將構成無權使用。而是否符合上述條件，尚須依據各案例事實，斟酌相關利益。」[128]法院接著表示「由於遊戲者使用經由違法方式取得之程式，因此，此項遊戲行為並不符合遊戲機器設置者的意思。」[129]

至於認為應該檢驗「無權影響資料處理過程」此構成要件的學者，也針對構成要件內之「無權」一詞提出，必須援引詐欺相似性解釋來作為解釋依據。就上述之行為而言，行為人對遊戲機器之影響是屬於「無權」。無論如何，該程式資料是無權取得，因此負有向遊戲經營者保證人之說明義務，遊戲者之沈默因此具

[128] BGHSt 40, 335=NJW 1995, 670.
[129] BGHSt 40, 335=NJW 1995, 670.

有欺騙非價性[130]。

㈢視訊系統服務之濫用類型

自 1984 年開始，德國聯邦郵政局開始在全德國境內提供可視圖文服務（Bildschirmtext-System; Btx-system, Videotel），銀行可藉由此套系統提供電子銀行服務，客戶只要在自己家庭的設備（將電視或個人電腦）做一些相應的改裝或利用放置在公共場所的終端機，即可透過電話線路以會話方式與銀行通訊，並享受銀行的各種服務。由於費用便宜，所以此套系統的主要使用者為公司客戶，而通常個人用戶可藉由操作此套系統來定貨。實務上所發生透過視訊圖文服務進行電腦詐欺有以下兩種類型：

1.電話銀行

電話銀行（Telebanking im Btx-system）是指架構在視訊與資訊系統的銀行服務，亦即，透過電話線與電視，並非純粹語音服務。若是藉由網路，情形仍係相同，僅電話銀行成為網路銀行。

德國所發生濫用視訊資訊系統的案例主要是行為人在視訊與資訊系統內，使用他人的個人密碼與交易密碼或連線密碼（Transaktionsnummer, TAN）來進行無權的轉帳或匯款行為。依據學說之見解（並有法院採納[131]），此種情形與無權使用他人銀行卡與密碼案例相類似，因此也必須先區分內部關係之權利濫用與外部關係之權利濫用；而唯有當匯款行為違反視訊資訊系統參與者的意思時，方能適用第二百六十三條 a；若行為人係使用卡片與其附屬密碼，將錢匯入自己戶頭，此行為僅違反與銀行間的

---

[130] Wessels/Hillenkamp, BT/2 § 13 VI 2 Rdnr 613.

[131] Zweibruecken StV 93, 196.

契約約定，但未違反視訊資訊系統參與者的意思，不能適用第二百六十三條 a。若適用第二百六十三條 a，則無異於將刑法擴張而至保護密碼之占有[132]。

2.視訊資訊服務

在德國，參加視訊資訊系統的會員可以在自己的電腦終端機取得資訊或其他種類的視訊服務。此類服務係由業者經營，雖有些是可免費使用，但大多數必須付費方能使用。此外，業者尚須付費給提供電訊通信服務的電話公司。使用者必須經過兩道身份確認手續：個別的連線密碼與個人的識別密碼，才能進入視訊與資訊系統。

實務上曾出現的身份確認程序上之濫用行為如下：行為人以違法方式取得他人的連線密碼與個人識別密碼，並假冒會員身份使用視訊資訊系統[133]。此情形究應如何適用第二百六十三條 a「無權使用資料」之構成要件？此問題之回答，可以參考德國法院在以下案例中所提出之見解：某案被告冒用前妻名義，登錄某視訊資訊系統取得資訊服務，並在三個月內累積了二千三百五十九馬克的費用，最後他卻無能力支付這筆費用。第一審地方法院認為，被告從最初便已經知道他並無能力去支付這筆費用，因此應論以第二百六十三條 a 之電腦詐欺罪；然而，Zweibrücken 高等法院對第一審法院之此項判決提出以下疑問：如果現在認為違反契約之無權使用密碼行為可構成電腦詐欺罪，那麼將產生以下的結果：許多不具詐欺罪不法內涵的行為都將構成電腦詐欺罪。Zweibrücken 高等法院之主要觀點在於提出以「與詐欺罪相對應

---

132 Cramer,in: Schönke-Schröder, StGB, 25. Aufl. 1997, § 263 a Rdnr.20.

133 Schultz, Computerkriminalität, 1992, S.11f, 19ff.

的情狀」（亦即，相同行為對自然人施行也構成詐欺）為解釋規則，認為唯有當法院肯定該行為具備詐欺犯罪行為所特有之不法內涵時，方能被視為刑事可罰，亦才能構成「無權」使用資料，被論以電腦詐欺罪。在本案中，Zweibrücken 高等法院對這種違反契約之無權使用視訊服務之行為是否具有前述與詐欺罪相符合的情狀，存有疑問。同時，法院進一步表示，違反契約之使用自己密碼，也不具有上述之要求，其理由係：電腦僅審查「形式上權限」－密碼的正確與否，因此，電腦不可能「被騙」[134]。

參、我國刑法第三百三十九條之二與之三

一、刑法第三百三十九條之二不正利用自動付款設備取財得利罪

㈠條文內容之預覽與介紹

第三百三十九條之二的立法目的，在規範不正使用自動付款設備而取得不法利益之濫用行為。而在涉及自動付款設備案例中，本構成要件一方面彌補竊盜罪以物取得為要件之處罰上漏洞，另一方面亦彌補詐欺罪以人為前提之處罰上漏洞。

茲於下分析將第三百三十九條之二[135]第一項不正利用付款

---

134 OLG Zweibruecken,wistra 1993, 323.

135 第三百三十九條之二第一項與第二項規定分別為「意圖為自己或第三人不法之所有，以不正方法由自動付款設備取得他人之物者，處三年以下有期徒刑、拘役或一萬元以下罰金。」「以前項方法得財產上不法之利益或使第三人得之者，亦同。」

設備取財罪與第二項不正利用付款設備得利罪之不法構成要件。首先是客觀不法構成要件包括：1.自動付款設備。2.他人之物。3.不正方法取得。其次是主觀不法構成要件：1. 取物故意（第一項）或得利故意（第二項）。2.不法所有意圖（第一項）或不法得利意圖（第二項）。本文將於下參考我國學說之討論，依序檢驗上述之構成要件：

㈡客觀不法構成要件

首先說明本構成要件解釋與適用上最重要之「不正方法」概念。究竟本罪構成要件規定之「以不正方法由自動付款設備取得」之「不正方法」所指為何？甘添貴教授認為本罪之構成要件「不正方法」應採限縮解釋，指類似於詐欺之不正當方法，亦即，在正常使用自動付款設備的範圍內相類似[136]，林山田教授亦採取相詐欺相似性的解釋方法[137]。

必須一提者為，黃榮堅教授對本罪之構成要件「不正方法」的解釋，似乎採機器設置者意思之主觀說（雖然亦曾提及詐欺相類似性概念）。黃教授認為，凡是違背發卡人與自動櫃員機設置目的範圍之提款方式，即屬「不正方法」。據此以論，如果有人使用偽造或變造之提款卡，責任歸屬並不係真正持卡人，而係銀行。基於如此的法律利害關係，銀行對自動櫃員機之利用，當然會關心提款卡是否係偽造或變造，所以會構成「不正方法」[138]。至於使用竊取、撿來或利用委託保管卡片來提款，或者超出他人

---

136 甘添貴，《體系刑法各論（第二卷）》，2000年4月初版，頁326。

137 林山田，《刑法各罪論（上冊）》，2002年3月修訂三版一刷，頁427。

138 黃榮堅，「刑法增修後的電腦犯罪問題」，收錄於氏著，《刑罰的極限》，2000年4月元照初版第二刷，頁318-319。

委託提款額度而提款，因銀行在民事關係上可因不具備重大過失而免責，因此銀行並不在乎領款人是否權利人或者是否逾越授權，亦即非屬本罪之「不正方法」[139]。這樣的結論與林山田教授所主張者幾乎相同，依據林山田教授之見解，以偽造或變造提款卡經由自動付款機提款，構成本罪，但若以竊取、侵占或拾獲他人提款卡而由自動付款機中提款，則非屬本罪之不正方法[140]。

甘添貴教授與林山田教授所提出之詐欺相似性解釋方法，應是源於解釋德國刑法第二百六十三條 a 電腦詐欺罪之「無權使用資料」（此特別為解決提款卡濫用行為所增設），而為了彰顯電腦詐欺罪與詐欺罪不法內涵的等值性與平行結構，必須以詐欺罪的內涵來解釋。亦即，雖然對人之詐欺與電腦詐欺兩種行為之外觀與型態有所不同，但電腦詐欺罪必須具備詐欺罪之內涵方可。雖然我國刑法與德國刑法中有關電腦詐欺行為的規範有所不同，亦即，德國並未針對自動付款設備之濫用行為另立如我國刑法第三百三十九條之二的獨立規範，但德國是以刑法第二百六十三條 a 的電腦詐欺罪來規範所有電腦詐欺濫用行為。鑑於自動付款設備之濫用亦屬於電腦詐欺行為，我國刑法第三百三十九條之二應為平行於德國刑法第二百六十三條 a 的電腦詐欺罪。基於以上所述，本文認為德國實務與學說所主張之「詐欺相似性」對刑法第三百三十九條之二「不正方法」的解釋，頗有參考價值。

據此以論，「不正方法」應是指以類似於詐欺的方法操縱自動付款設備的電腦資料處理過程。換言之，必須設想行為是否類似於在面對自然人時，所為之施行詐術行為；此處的「詐欺性」與傳統詐欺罪之詐欺之差別應僅在於對象是自然人還是機器。本

---

139 同前註。

140 林山田，前揭書（註137），頁427。

文認為，不管使用不法方式取得（偷竊、侵占）之真卡或偽造之假卡，其所輸入的資料皆為正確，亦即，與銀行系統所設定或儲存之密碼、帳戶資料相符[141]，但卻係無權使用。此種無權使用他人資料（帳號與密碼資料），亦即一般所稱之「冒用」或「盜用」。當行為人面對行員進行冒用時，必須冒稱自己是合法權利人而讓行員產生錯誤，可以被認為是施行詐術，在適用詐欺相似性的解釋原則下，而屬於「不正方法」。

此外，在適用本構成要件時，必須注意尚有與卡片濫用無關之經由自動付款設備取得他人之物的情形。舉例而言，行為人先以一比三的代價，向他人購買偽鈔，之後，他順利將偽鈔存入無人銀行的自動櫃員機中，帳款入帳之後，再迅速到其他櫃員機，以提款卡領出真鈔。此由自動付款設備取得現金之行為方式是否構成本罪「不正方法」？若依上述詐欺相似性方法檢驗，答案應為肯定。由以上說明可知，本罪之「不正方法」之構成並不以卡片濫用為前提。

㈢主觀不法構成要件

本罪之主觀不法構成要件，除了包括不正使用自動付款設備取物故意（第一項）或不正使用自動付款設備得利故意（第二項）。不正使用自動付款設備取物或得利故意必須是行為人對於他人自動付款設備有所認識，並進而決意使用不正方法由自動付款設備取物或得利。如果行為人取得自動付款設備因機械故障而自動送出之現金，則不構成本罪之故意，至多只能成立刑法第三

---

141 存款戶在開辦金融卡時，先由銀行發給一組預定密碼，再請存款戶到自動櫃員機（ATM）或用電話銀行變更密碼，其中沒有人員介入，經過變更後之密碼，並非儲存在金融卡，而是儲存在主機內。當顧客進行交易行為時，直接由 ATM 終端系統與銀行的主機確認密碼。

百三十七條侵占脫離持有物罪[142]。此外，構成本罪還需要大多數財產犯罪所要求之特別之主觀不法構成要件，如不法所有意圖（第一項）或不法得利意圖（第二項）。

二、刑法第三百三十九條之三不正利用電腦取財得利罪

㈠條文內容之預覽與介紹

在進入構成要件分析之前，必須先對本構成要件之結構為分析。現行第三百三十九條之三第一項與第二項之規定分別為「意圖為自己或第三人不法之所有，以不正方法將虛偽資料或不正指令輸入電腦或其相關設備，製作財產權之得喪、變更紀錄，而取得他人財產者，處……。」「以前項方法得財產上不法之利益或使第三人得之者，亦同。」依據林山田教授之解釋，「不正方法係將虛偽之數位資料輸入電腦或其相關設備，或將不正指令輸入電腦或其相關設備，而製作財產權得喪變更紀錄，……。故不正方法僅以透過電腦數位資料之處理而與詐欺相類似之方法為限。」[143]由前引觀點可知，林山田教授有兩點重要見解。第一，將「不正方法」理解為具有詐欺相類似性行為。第二，「不正方法」用來修飾「輸入虛偽資料」與「輸入不正指令」。而黃榮堅教授將本罪之構成要件行為統稱為「不正輸入」亦應屬相同脈絡

[142] 參見，林山田，前揭書（註137），頁427；以及甘添貴，前揭書（註136），頁326。

[143] 林山田，評詐欺罪章中之新增三罪，月旦法學第49期，頁87。

之思維[144]。本文贊同此等的法條結構分析，茲於下進一步說明相關概念：

首先，雖然我國的立法相類似於與日本立法例[145]，但與日本立法例最大不同之處在於我國構成要件多了「不正方法」，此應為立法者有意增加之文字。當初立法者加入「不正方法」應是配合刑法第三百三十九條之一與之二，主要目的可能在使新增的三個構成要件在體系上具備完整性。再者，立法者將此三條文規定於詐欺罪章，顯然「不正方法」是與詐欺罪關連性之強調。但是，自字面涵義而論，「虛偽」資料與「不正」指令已均足以顯現詐欺等值性；再者，從詐欺罪之對應結構而言，輸入虛偽資料就是一般所稱之「輸入操縱」[146]，而「輸入不正指令」亦即「程式操縱」[147]；此兩種方式均會影響資料處理結果。目前條文將「不正方法」置於「輸入虛偽資料」或「輸入不正指令」之前，似乎屬於同義反覆之贅語。對照「以不正方法將不正指令輸入電腦或其

---

144 黃榮堅，前揭文（註138），頁323。

145 日本刑法第二百四十六條之二第一項與第二項規定分別為：「在第二百四十六條之外，對他人用於處理事務之電子計算機輸入虛偽資料或不正指令而製作出有關財產權之得喪變更之不實電磁紀錄，或將有關財產權之得喪變更之虛偽的電磁紀錄提供給他人用於處理事務，而獲得財產上不法利益或使他人獲得者，處十年以下有期徒刑。」「前項之未遂犯，罰之」。此條文之翻譯係參考，前田雅英著，董璠興譯，劉俊麟校訂，日本刑法各論，五年圖書出版公司，2000年5月初版一刷，頁254。

146 輸入操縱是指電腦在內部程式沒有被變更下，依據預先設計、按步就班的指令來處理來自外部輸入行為的數值，如果輸入的數值本身並非正確，經過處理後產生之電腦數值也是不正確的，最後產生不正確資料處理結果。參見，Sieber, Computerkriminalität und Strafrecht, 2. Aufl. 1980, S.55,61.

147 程式操縱是指在資料在輸入過程中並沒有被操縱，也就是，輸入正確資料，之後經由電腦內部的編譯器將之編譯成正確的電腦內部數值，但有可能因為程式已遭修改，電腦所進行的資料處理程序與原來應進行的資料處理程序相較，可認為是不正確的資料處理程序，最後產生不正確資料處理結果。參見Sieber, Computerkriminalität und Strafrecht, 2. Aufl. 1980, S.55,61.

相關設備」之文字結構，前述同義反覆之批評似乎更顯明確。據此而論，似乎不需以「不正方法」之構成要件作為詐欺等值性之強調。

另一方面而言，本文認為，既然「不正方法」已被立法者列為構成要件，「不正方法」之解釋仍有必要。本文將在下文所進行之構成要件分析時，以「不正方法」作為修飾「輸入虛偽資料」與「輸入不正指令」之前置詞。在此，先依前文所討論者，對刑法第三百三十九條之三構成要件為如下分析：㈠客觀不法構成要件： 1.不正輸入行為[148]：(1)電腦或其相關設備(2)輸入虛偽資料(3)輸入不正指令。 2.製作財產權得喪變更紀錄。 3.財產上損害與得利。㈡主觀不法構成要件： 1.不正利用電腦取財故意（第一項）或不正利用電腦得利故意（第二項）。 2.不法所有意圖（第一項）或不法利益意圖（第二項）。

㈡客觀不法構成要件

1.不正輸入行為

(1)電腦或其相關設備

由於本構成要件屬於詐欺罪之補充規定，立法目的在規範不涉及人，而由電腦代替人所獨立進行之自動化財產權處分之情形。因此，構成要件之「電腦或其相關設備」必須具備財產權處分之功能。舉例言之，保險箱或收費站之電子檢測裝置，即使屬

[148] 雖然構成要件並沒有出現「不正輸入」之字眼，但本文用不正輸入行為來包括構成要件所規定之「輸入虛偽資料」與「輸入不正指令」。這類似於德國詐欺罪中經常以「欺騙」（Täuschung）一詞代替構成要件所規定之行為，如「虛構事實」（durch Vorspiegelung falscher Tatsachen）與「歪曲或隱瞞事實」（durch Entstellung oder Unterdrückung wahrer Tatsachen）。

於具備資料處理能力之電腦或其相關設備，但因行為人藉由資料操縱行為僅取得取走保險箱之物或得以通行的可能性，此種電腦並不具備財產上處分之功能，所以，並非本構成要件所規定之「電腦或其相關設備」。

再者，由構成要件之「製作財產權之得喪、變更紀錄」亦可以間接推論出在適用本罪時，應將不具備財產權得喪變更紀錄功能的「電腦或其相關設備」排除在本罪的適用範圍外。此外，為配合本罪所規定之構成要件行為「輸入虛偽資料」或「輸入不正指令」，「電腦或其相關設備」必須具備人力經常介入的可能性，亦即，具備輸入（儲存）資料或程式之功能。最後，本構成要件之「電腦或其相關設備」應配合網路時代下之電腦概念，電腦不僅是可以計算，還具備藉由電腦連線而達資源分享的功能，亦即電腦與通訊的結合。

接下來將根據以上之標準來檢驗以下之設備是否為本罪所指之「電腦或其相關設備」。一般所稱之智慧卡，亦即，具有儲存與處理個人金融資料功能的晶片。由於具備處理與儲存資料功能，智慧卡也可算是本罪所稱之「電腦或其相關設備」。再者，自動販賣機（包括物或服務之給付）之硬幣辨識裝置是利用感應該硬幣的重量與形狀為判斷（此功能由晶片所執行），與家用電器（微波爐之定時器、錄影機）一樣，都是將計算、邏輯與控制之線路放在一片晶片上，由晶片完成預定之功能，而晶片上之程式為固定。與一般電腦的差別在於，自動販賣機之硬幣辨識裝置是為某個工作而設計之電腦，只能做固定工作，不能載入新的程式與資料。此種電腦在開機後立即以各種模式工作，雖不能否認此等機器設備具有資料處理功能和財產上處分之功能，但因並不具備製作財產權之得喪、變更紀錄之功能，故不在本罪之「電腦

或其相關設備」範圍內。再者，日常生活中常用的掌上型電子計算機主要是用來執行簡單的加減乘除運算，沒有複雜的介面，雖因具有可程式性與快速運算能力，不能否認具有資料處理功能，但由於並無複雜介面以允許外力介入內部資料處理程序，亦無製作財產權得喪變更紀錄之功能，故不屬於本罪之「電腦或其相關設備」。

值得討論者為卡式或 IC 公共電話與自動影印機等配合卡片使用之自動機器。使用時，影印卡或電話磁卡之餘額會顯現於機器設備上。這些機器設備具有資料計算、處理之功能，儘管機器內部不像一般電腦有內部儲存裝置，但可在卡片上進行資料之儲存，因此，這些機器設備應屬於得製作財產權得喪變更紀錄之電腦。然較有疑問者為，電信通訊設備之性質。電信通訊設備之運作[149]除了提供連線服務，進行財產上處分（給付物以外之財產上利益）外，還有通話開始與結束之紀錄，據以向顧客收費，具備製作財產權得喪變更紀錄之功能，因此，屬於本罪所規定之「電腦或其相關設備」。

⑵輸入虛偽資料

關於「輸入虛偽資料」構成要件之說明，必須藉由「輸入」概念來解釋「資料」的意義。就電腦基本原理而論，輸入的動作是使用者或周邊設備將資料傳向電腦的動作，交談式電腦一般是

[149] 電信通訊設備之運作如下：當電話使用者撥出一通長途電話時，在短短一、二秒中，電信通訊設備之資訊系統便開始辨識撥話端的電話號碼、紀錄開始通話時間、檢查發話端的設定特性或特殊服務、收集發話端的電話號碼，並且迅速決定與哪一台長途電話交換機連線、等待長途交換機的回應後再回覆發話端。

由鍵盤輸入資料，而輸入的來源是使用者與鍵盤[150]。接下來，可借用前文已提到過之「輸入操縱」的架構來增進對「輸入虛偽資料」構成要件之理解。在輸入操縱情形中，行為人希望藉由提供或傳向電腦不正確資料，而得到不正確處理結果。要讓電腦處理此資料之前提在於資料已經從外部進入電腦，更正確地說，資料已經進入電腦內部待處理區域，亦即，資料暫存之記憶體中。之後電腦會讀取記憶體中已有之指令（在此情形，不涉及程式操縱，所以指令沒有被行為人影響過）與行為人所傳向之資料，並執行這個指令所代表之計算；而經由電腦處理過所得出的不正確資料結果，即是行為人行為的結果。

因此，關於本構成要件所指之「資料」，可以為以下之說明：首先，在輸入階段，所輸入的資料型態不一定是數位形式之電磁資料。行為人藉由電腦連線所傳輸或藉由資料載體（如卡片上磁條）所輸入者必定是數位資料。至於紙本上的資料或打孔片上資料，亦屬本構成要件所指之「資料」，只是這些資料必須經過轉譯程序成數位形式資料（內碼或代碼），如此才能被電腦處理。由林山田教授針對本罪所提出之立法建議條文中強調「輸入虛偽數位資料」[151]可知，林教授所要表達之意思應該是要藉此強調所有資料，進入電腦後均轉成數位形式之電磁資料。經本文前述之說明可知，輸入時點上，原來資料有可能是紙本式資料。再者，本構成要件所規定之「輸入」包括輸入並儲存原本不存在之新資

---

150 參見，黃匡庸，二〇〇二最新電腦字典，旗標出版有限公司，2001年6月，頁431。

151 林山田教授所提之修法建議條文為「意圖為自己或第三人不法之利益，以不實或不完整之數位資料或不正指令輸入電腦或其相關設備，造成數位資料處理之錯誤結果，而取得他人之財物或財產利益或使第三人得之者，處七年以下有期徒刑」。參見，林山田，前揭書（註137），頁431。

料外，更改已存在的資料或刪除資料，亦可被認為屬於輸入行為。因更改資料係以輸入新的資料而取代舊的資料；而刪除動作則在完成後尚須進行儲存。行為人之輸入資料行為必定已經影響既有或原本應有之資料處理結果。當然，輸入也可利用不知情之工具，例如，填寫不正確資料匯款表格而讓銀行行員輸入。

再回到構成要件之「輸入虛偽資料」之「虛偽」概念。對照於前文曾介紹過之德國電腦詐欺罪立法例所使用之「使用不正確或不完整資料」構成要件，我國所規定之「輸入虛偽資料」顯得較為簡單；亦即，不區分「不正確」與「不完整」兩種情形。若參考德國法上之見解來解釋可知，本構成要件之「虛偽」應指「不符合事實」，也就是「不正確」的意義。按，符合事實為「真」或「真實」，與事實不符合為「假」或「虛假」。與實際事實存在狀態不符合之資料即可被認為是本構成要件中所稱的「虛偽資料」。

歸納言之，以下行為屬於「輸入虛偽資料」。首先，如果行為人自住家終端機入侵銀行電腦系統，直接輸入並儲存不正確的存款資料，變更原資料系統之內容，並促使電腦自動產生與事實狀態不符之紀錄。由於行為人實際上並未有存款行為，卻輸入並儲存一筆存款資料，藉此使自己在銀行紀錄上的存款餘額增高，以便進行帳戶透支或在已經沒有存款額的帳戶中提領現金。由於資料所呈現出之資訊狀態與現實不符，所以構成輸入虛偽資料。再者，在公司薪資名冊上輸入不存在的員工資料，使薪資計算系統自動匯入薪水，藉以取得不法利益。又如輸入假的供應商帳目到公司電腦中的貸方資料（債權人部分）中。此外，屬於輸入虛偽資料者還包括刪除型態，例如某出納員為了使朋友獲得財產上利益，每月從應支付會費的名冊中，刪除他朋友的資料，使得該

位朋友無須支付會費，此出納員的行為仍屬輸入虛偽的資料。

此外，前文曾論及卡式或 IC 公用電話或附有計費裝置影印機可被認為屬於本構成要件之「電腦或相關設備」，而下述之不正當使用行為則可被認為構成「輸入虛偽資料」，例如，擅自變更或增加影印卡或電話磁卡之餘額額度資料後，再持之使用於公用電話或影印機。由於卡片上之資料屬於不實的電磁資料，將卡片送入機器讓機器讀取並處理，便可認為「輸入虛偽資料」。

有爭議的是，使用不法取得之他人合法卡片或使用偽造卡片而冒領存款行為，是否構成輸入虛偽資料？就德國立法例而言，由於前階段之使用卡片與密碼行為不構成「使用不正確或不完整資料」（性質上等同於我國之「輸入虛偽資料」），因此有了「無權使用資料」構成要件之產生。換言之，依據目前德國刑法通說，前述之濫用卡片冒領行為是依據「無權使用資料」來規範。顯然在德國立法例下，輸入他人合法卡片或偽卡與密碼並不構成「輸入虛偽資料」，但若依日本學說之見解，使用他人卡片與密碼屬於「輸入虛偽資料」。在我國法下，此一問題，有深入討論之必要。

本文認為，無權使用他人卡片或偽造卡片與密碼資料而取得不法利益的行為，是否構成本罪所規定之「輸入虛偽資料」，可以有以下三種解釋方法：

(A)以系統經營者主觀之明示或可得推知意思為標準

一般人到銀行提領現金，並不需要攜帶身份證。只要提出存款簿與印章，不論何人，均可提領。在自動櫃員機設計上應該也是採取相類似立場。卡片上所載用戶身份識別碼與通行碼（俗稱為密碼）是用來提供持卡人擁有合法權限之證明；是否是持卡人

本人或經合法授權，對交易相對人之銀行而言並非是交易上重要訊息。事實上，如果銀行非常在乎是否是持卡人本人或經合法授權，就必須採取更嚴格驗證程序，例如，防偽性較高之 IC 卡取代目前容易被複製之磁卡，或卡片真偽之辨識，或者利用指紋等足以鑑識人別之技術來確保持卡人為本人。從此可以推論的是，銀行只在乎是否上述兩項資料是否正確，因此，只要輸入之這兩項資料為正確，並不構成「輸入虛偽資料」。

(B)以詐欺相似性來解釋「輸入虛偽資料」

卡片上所載用戶身份識別碼與通行碼是用來提供持卡人擁有合法權限之證明。儘管行為人所輸入的資料與事先儲存在銀行主機交易系統內之合法權利者之權利認證資料相符，但如果實際上使用人並不具有合法權限，等於向電腦傳遞了不實訊息，則輸入上述資料的行為即類似於詐欺罪中之施行詐術行為。因此，不能因資料屬於正確而否認此行為已構成「輸入虛偽資料」。依上述解釋，濫用卡片冒領之類型可被納入刑法第三百三十九條之三電腦詐欺罪之規範範圍內。不過應注意者為，此種解釋與前文所介紹德國立法例上之見解明顯不同。但分析現有條文可知，我國立法例幾乎於日本立法例相同，而日本也是將此種類型行為納入「輸入虛偽資料」概念下。

(C)以電腦觀點來解釋「輸入虛偽資料」

從系統運作觀點觀察，可以將無權使用他人卡片或偽卡冒領存款之行為做如下的分析：電腦程式所設定運作的方式是認卡不認人。因此行為人必須先輸入卡片與附隨的密碼於銀行的自動提款機（其實是終端機）中，而上述資料很快便可藉由電話線或專

線傳送到銀行主機；此時銀行資料處理系統僅審查金融卡上磁條的資料與密碼資料，等到審核資料結果係正確後，才授權行為人進行進入系統中。在進入系統後，行為人必須遵行顯示於螢幕的指示，始可進行交易。例如想要提領現金，只要按適當的鍵（命令通過連線再送入主機），電腦會自動地在將提領金額記入顧客的帳戶的借方並發鈔。

從電腦觀點而論，無論使用偷來的真卡與偽造的假卡，行為人插入卡片與輸入密碼的行為應非屬輸入虛偽資料；姑且不論真卡，就製造偽卡而言，前提是須取得卡片的相關資料，才能進行卡片複製。由於行為人所輸入之資料與儲存在銀行系統內的資料相符，因此，屬於輸入正確的資料，而在之後一連串的行為中，行為人所做的僅係對銀行電腦進行「指示」，其並無任何輸入虛偽資料的行為出現。在此，必須說明的是，「指示」應與下一構成要件所使用之「不正指令」之「指令」相區別。「指示」可直接輸入，讓電腦為使用者執行一個特定工作；而「指令」則是由裝置在電腦內部之程式所組成[152]。

針對此一問題，可參考八十一年度第十一次刑庭會議決議中的一段說明：「自動付款機所按上之「提款數字」，是一種付款操作之指令，即命軟體程式依此就其所控制之自動付款系統為一定之處理，並付出與該數字相同之現款。---。所為既非輸入虛偽資料。」再者，如刑事庭會議決議所指出者，「原先儲存之資料，內容上有所變更」，與事實不符的資料（真正的權利人並沒有從事此項交易，提領金額已入帳）確已存在於銀行自動付款機軟體內，這是不能否認之事實。何況，從電腦紀錄檔中可以看到這項

---

[152] 參見，黃匡膚，前揭書（註150），頁183, 432, 680，以及，榮欽科技，最新電腦字典，松崗電腦圖書資料股份有限公司，2001年6月二版，頁3-4。

資料輸入行為（動作）之存在紀錄，但關鍵處在於，此動作的存在紀錄並不是來自於行為人之輸入行為，因為，在電腦原理中，不管動作樣態如何，所謂「輸入」之後就是數位形式資料進入暫存器，之後中央處理部分再進行處理。而「按密碼」（密碼並沒有被偽造而只是被無權使用）與「按選擇項目」這些動作，都僅能使電腦進行資料處理，以決定下一步動作，處理完畢後呈現出的資料是與事實不符者。電腦系統內所存在之虛偽資料，並不是來自於密碼、卡片上磁條所載的資料之輸入，而是一連串指令處理後之結果。由於行為人從頭到尾都沒有從事儲存行為，亦即，沒有在銀行電腦磁碟上儲存（記載）任何之意思或觀念，也沒有對「已有之程式或資訊、資料予以變更或塗去」。既然沒有儲存或變更，就不能認為有偽造或變造電磁紀錄。事實上，就銀行電腦系統而言，使用者是沒有存取權限的，僅可下指令讓電腦完成工作，而前提必須是被認證過身份者，才能讓電腦處在接收指示狀態。因此，並無任何輸入虛偽資料行為。

以上三說何者較為適當？如前文所討論，就法條結構而言，「不正方法」用來修飾緊接在後之「輸入虛偽資料」與「輸入不正指令」，而本文在解釋刑法第三百三十九條之二之「不正方法」時已採用詐欺相似性解釋，所以，此處之「不正方法」應該採取相同立場。因此，在以上三說中，似乎以第二說為適當。再者，基於提供法益完整保護之理由，本文也認為應該採取第二說。茲於下說明法益保護必要性之立場：

據以上所述可知，使用不法取得之他人真卡或偽卡冒領現金之行為，依據第一說與第三說之解釋方法，並不是本構成要件之「輸入虛偽資料」，無法依據我國刑法第三百三十九條之三論罪，但此種濫用還可以適用第三百三十九條之二不正利用付款設

備取財得利罪處罰，所以，目前針對自動櫃員機無權使用正確資料之行為尚無處罰上漏洞。但與自動櫃員機同樣面臨相類似風險者，還包括銷售點系統（Point of Sales）[153]，亦即，在使用銷售點系統可能發生無權使用他人卡片與身份識別碼等權利認證資料而取得財物或財產上利益行為。在使用這種系統時反而面臨比自動櫃員機更大風險，因為商店職員或後來客戶都可能在前次交易後接續進行；相較之下，自動櫃員機之使用者反而較能控制卡片的使用[154]。而由於銷售點系統之操作類似於自動提款機，因此也須決定無權使用他人認證資料是否構成「輸入虛偽資料」。

此外，對日漸普及之不涉及卡片使用之電子支付系統（electronic payment system）濫用行為也會形成處罰上漏洞。目前網路信用卡冒用便是最明顯的案例。在網路上以信用卡支付時，由於電子信用卡系統少了將卡片交給店員刷卡動作，因此只要鍵入卡號、身分證明字號、有效日期便可刷卡，無須出示信用卡與當事人簽名，網路上之商店再以電腦連線連至信用卡中心，要求取得授權，並由銀行代付帳款[155]。其他如在撥通電話後，依據銀行語音提示而輸入帳戶號碼與密碼，繼而選擇按鍵的電話銀

---

153 使用銷售點系統的程序，可以簡單說明如下：消費者將欲購買的商品帶到設置有銷售點系統終端機的櫃台，在不使用現金、支票或信用卡下，藉由卡片的插入終端機與鍵入個人識別碼便可進入自己在銀行開立的帳戶，接著商店輸入商店帳戶號碼、商店位置與交易額等其他的資料。電腦會自動地在將消費金額記入顧客的銀行帳戶的借方，並在商店的帳戶的貸方記入消費金額。關於此系統與電腦詐欺罪適用之討論，由於牽涉銀行、商家與持卡人三方，情況不同於自動櫃員機，故本文擬於獨立一篇文章中討論。

154 Rostoker/Rines, Computer Jurisprudence-Legal Responses to the Information Revolution, 1986, 387.

155 參見，張真誠、林祝興、江季翰編著，《擁網值錢-電子商務安全概要-安全、風險管理、控制》，松崗電腦圖書資料股份有限公司，2000年2月初版，頁812-813。

行操作行為，亦屬相類似的情形。如果行為人藉由無權使用他人認證資料，而取得財物或財產上利益，因此一過程是完全沒有人介入的自動化過程，故無法適用傳統竊盜罪與詐欺罪。顯然地，有利用第三百三十九條之三規範之必要性。

進而言之，在網路時代下，網路上的網路銀行與目前正在發展中的電子支付系統都必須經由電子閘道輸入認證工具。舉例而言，網路銀行設立後，消費者可以將個人金融資料儲存於個人電腦，隨時依據需要在網路上進行諸如，轉帳、繳費、購物付款等金融活動。但網路上銀行業務在電腦系統操作上必須藉由一定程序來確認對方身份，此即所謂認證程序。認證程序是給予每一個用戶身份識別碼，亦即帳號與俗稱為密碼之通行碼來提供身份證明[156]，因此，無權使用他人資料以取得不法利益之行為究應如何評價，仍有待明確的刑法規範。

⑶輸入不正指令

依據日本學說見解，日本刑法二百四十六條之二所規定之「不正指令」是指程式操縱[157]；而德國第二百六十三條 a 則是以「程式」（program）作為構成要件。參考上述兩個立法例後，可以將本構成要件中的「輸入不正指令」以一般所稱的「程式操縱」理解之，程式操縱將足以改變電腦內部資料處理之程序。

在電腦實務上，有關程式之理解是與指令有關。對「程式」之通常定義為「可以被電腦所執行之一連串機械碼」，而機械碼之敘述就是「指令」（instruction）。簡單的說，「程式」是可供

---

[156] 參見，張真誠、林祝興、江季翰編著，前揭書（註155），3-2, 3-3，以及黃匡庸，前揭書（註150），頁27。

[157] 參見前田雅英著，董幡興譯，劉俊麟校訂，前揭書（註145），頁254。

電腦執行之代碼化「指令」序列。有時程式也包括尚未被轉譯成機械語言（機械碼），而以各種較高階語言形式所寫成的原始程式（source program）[158]，因此在解釋本構成要件時，應該將機械語言（機械碼）與非機械語言之程式包括在內。

據上段所述可知，在使用不法取得之真卡或假卡案例中，由於輸入正確的卡片與密碼資料，而能使銀行系統處在等待下「指示」的狀態，之後行為人所為之選擇提款選項與按入提款金額，都僅是對銀行資料處理系統下「指示」，此已於前文中有所說明。雖然前引八十一年度第十次刑庭會議決議文使用「付款指令」一詞，但嚴格說來，應是「付款指示」，亦即，先指示電腦為行為人執行提款工作，之後再指示提款金額。此一連串行為便類似於，當我們要列印一份文件時，必須利用文書軟體所設計出的各種功能選項，透過鍵盤或滑鼠輸入列印的指示，CPU 收到這個指示後，知道我們要列印文件，便會將資料送到印表機，然後由印表機執行列印文件的工作。很清楚地，前引兩種情形都屬於可以直接輸入之「指示」，而非與電腦資料處理程式有關之「指令」，據此可知，濫用卡片行為不涉及刑法第三百三十九條之三「輸入不正指令」之構成要件行為。

接下來是有關「不正指令」內涵的討論。甘添貴教授參考日本學說，將「不正指令」解釋成依該電腦系統所預定之事物處理目的，所不應該給予的指令；如應存檔者，卻給予刪除的指令[159]。依據林山田教授之說法，「不正指令」是「能對電腦下達錯誤之

---

158 參見，黃匡庸，前揭書（註150），頁432, 680，以及，榮欽科技，前揭書（註152），頁3-4。

159 參見，甘添貴，前揭書（註136），頁334。

處理指令之犯罪程式」[160]。甘添貴教授之說法相當接近於德國通說所主張之依據系統所預定處理之工作來判斷程式是否屬於「不正確程式」；而林山田教授似乎以程式所得出之結果是否錯誤來從事判斷。

本文認為「不正指令」之判斷，可以參考德國立法例在「編制不正確程式」上之立場，而認為應從財產保護觀點出發，著重資料處理之結果，對相關利害關係人而言，是否是正確被完成之工作。據此以論，與系統設計不符（不相容）的指令當然構成「不正指令」。至於電腦系統相容的程式操縱，例如，運用已存在之工作指令而支配（影響）資料處理的過程，只要最後得出之結果並非正確工作處理，並屬影響利害關係人之不正確的結果，即使是與系統程式相容，仍屬「不正指令」。

歸納而言，「輸入」不正指令之「輸入」可分為二種。第一種為原來程式的修改。修改也包括程式之刪除。第二種為在原來的程式中插入新的指令[161]。此外，「輸入」並不限於無權使用人在系統運作後所為之前述二種輸入不正指令行為[162]，若屬於電腦尚未正式運作前，設計電腦程式之工程師在電腦程式中，秘密地增加或預設能在中途改變的指令，亦可被認為屬於輸入不正指令。

最後，行為人行為有可能涉及輸入虛偽資料與不正指令行為。舉例而言，行為人先侵入郵局電腦主機系統，以甲之名義，開設帳戶；過數日後，復侵入該電腦主機，輸入指令，將以存戶

---

[160] 參見，林山田，前揭文（註143），頁87。

[161] 同前註。

[162] 參見，甘添貴，前揭書（註136），頁338。

之利息，設定成自動轉入甲之戶頭[163]。

2.製作財產權的得喪變更紀錄

「製作財產權之得喪、變更紀錄」此構成要件的功能是代替傳統詐欺罪下人之「陷於錯誤」與「財產上處分」。電腦本身依賴儲存在內部之資料或它所處理之資料獨力完成法律上之處分行為，其中並沒有任何人之介入，因此沒有任何對人之欺騙行為牽涉其中，但卻可藉由資料處理過程之影響，產生等同於欺騙的效果。從「財產權得喪變更紀錄」一詞可知，紀錄的變更會帶來財產權之變更。此乃依據電腦處理之特質而論。詳而言之，在自動化交易程序中，電腦系統自動進行金額的計算並紀錄交易狀況，此為該次資料處理過程之結果。因該次交易紀錄促使電磁紀錄的做成（更新），並立即做成財產上處分，因此直接產生財產權得喪、變更之效果。故刑法第三百三十九條之三在「製作財產權得喪變更紀錄」後直接跟著「獲得財產上不法利益或使他人獲得者」。換言之，這裡已經有一個電腦自動所產生的財產上處分行為。再以前述之擅自變更影印卡或電話磁卡，並使用之情形為例，使用過程是將卡片輸入電腦。由於影印卡或電話卡片上餘額額度之記載為不實，所以，構成「輸入虛偽資料」。之後，經過機器處理，機器在卡片上所從事的計費與餘額記載，便屬於「製作財產權得喪變更紀錄」，而當事人也藉以取得影印服務或通信服務之財產上不法利益。

再者，雖然我國立法例並沒有像日本立法例一樣，明確標出「不實」之字樣，但此電磁紀錄必定已是「不實」，才能具有詐欺等質性。林山田教授早期所提之電腦操縱罪之建議條文曾明定

163 黃榮堅，前揭文（註138），頁321。

「造成電腦資料處理之錯誤結果」[164]與最近之版本「造成電腦資料處理之錯誤結果」[165]均以「錯誤結果」為構成要件，此即表達等同於欺騙效果之陷於錯誤而為財產上處分。值得介紹者為日本立法例上所使用「不實電磁紀錄」之涵義。日本學者曾表示，日本刑法第二百四十六條之二第一項與第二項規定分別為：「在第二百四十六條之外，對他人用於處理事務之電子計算機輸入虛偽資料或不正指令而製作出有關財產權之得喪變更之不實電磁紀錄」，立法者在同一條內分別使用了「輸入虛偽資料」與「不實之電磁紀錄」等，其中「虛偽」與「不實」有區別的必要。如果資料或電磁紀錄出自行為人之虛構，此時適合用「虛偽」；但如果藉由機器或其他人之手而做出之紀錄，當與事實不相符合時，採用「不實」較為適當[166]，此與德國學者所強調之「不正確」之資料處理結果一樣，都是表達客觀意義上之與事實不符。

3.財產上得利

雖然我國刑法第三百三十九條詐欺罪之構成要件並沒有「財產上損害」，但依據我國刑法通說，第三百三十九條詐欺罪之構成要件要素間之關係為：「因」相對人財產上處分「而」造成相對人或第三人財產上損害。此項說明應是參照德國立法例之解釋，因為德國刑法詐欺罪所使用之構成要件是「致他人受損害」。與我國立法例相似，日本刑法第二百四十六條之二電腦詐欺罪與

---

164 林山田，〈電腦犯罪與刑法〉，收錄於法務部，電腦犯罪問題研討會實錄，1985年5月，頁47；同作者，〈評刑法修正草案〉，《台大法學論叢》第20卷第1期，頁202。

165 林山田，前揭書（註137），頁431。

166 參見，米澤慶治著，大塚 仁、河上和雄、佐藤文哉編，大コンメンタール刑法，第十卷，§ 246-2, Rdnr.22。

第二百四十六條詐欺罪之構成要件均缺少「致他人受損害」之構成要件。依據日本通說之見解，儘管條文並未明定構成詐欺罪必須有損害發生，但由於詐欺罪是財產犯，損害之發生乃理所當然，因此，參考德國學說而認為亦應以財產上損害為要件[167]。在我國，詐欺罪與不正利用電腦取財得利罪（即電腦詐欺罪）之構成要件均為「使人將本人或第三人之物交付」與「得財產上不法利益或使第三人得之」此類似於日本立法例。與日本立法例不同處在於，日本刑法中詐欺罪與電腦詐欺罪都僅係利得犯（獲利罪），但我國刑法中，不管是詐欺罪或電腦詐欺罪除利得犯，還包括財物犯。儘管有上述差別，但在解釋詐欺罪與電腦詐欺罪時，仍應以「財產上損害」為構成要件。

關於電腦詐欺領域內，財產上損害概念，有必要進一步說明。在資訊時代，人類所有活動幾乎離不開資訊，各種東西盡可能以數位或符號表示。財務支付工具（如現金）、商品等都盡量以數位形式之電腦資料來表示。所謂的「電子資金系統」其實也只是資料交換系統，利用網路來進行資金移轉，如果沒有伴隨金錢提領行為，其實也只是系統內資料之重新安排。所以，電腦詐欺罪之財產上損害必須與詐欺罪一樣，採取具體危險犯下的財產損害觀點。亦即，即使財產損害尚未發生，但很可能隨時出現。再者，由於具體危險犯也是一種結果犯，因此，不會影響詐欺罪結果犯之本質[168]。

在電腦詐欺罪的情形中，當涉及財產權得喪變更之電磁紀錄記載完成，由於已生財產上具體危險，此時即已既遂。舉例而言，對銀行電腦系統內資料之操縱，如輸入虛偽資料或程式操縱，由

---

[167] 參見，前田雅英著，董幡興譯，劉俊麟校訂，前揭書（註145），頁250。
[168] 參見，林東茂，前揭文（註90），頁207。

於已修改銀行的電磁紀錄，而讓機器做出財產權移轉的自動清算處理，並使銀行電腦系統進行金額的計算並紀錄交易狀況，因該次交易紀錄（記載於電腦記憶體與交易明細表）已是銀行與客戶關係的基礎，而客戶隨時可就帳戶內之金額處分。此時可認為已達事實上可處分狀態。如果已經構成事實上處於可以處分之狀態，儘管尚未提款，也不影響既遂之認定。又如行為人在提領金錢前，就遭逮捕，以致於不能取得金錢，但只這只能說是「不法所有意圖」或「不法利益意圖」的未實現，依據通說之見解[169]，即使不法所有或不法利益意圖未實現，仍可被認為已構成第三百三十九條之三之不正利用電腦取財得利罪之既遂犯。沒有疑問的是，如果在行為人操縱電腦系統之後，機器已經將現金送到現金出口供取走，此時若被逮捕，同樣也已構成電腦詐欺罪之既遂。

此外，如德國學者所指出，電腦詐欺罪與詐欺罪一樣，必須具備「直接性」。詐欺罪之「直接性」在於財產上損害與得利行為是直接來自處分行為。行為人（或第三人）「取得之利益」與被害人（不一定要是受騙者）「財產上損害」間具有「內容相等」（Stoffgleichheit）之關係[170]。易言之，財產上處分行為同時會在相對人方面產生「受損」，另一方面，產生「得利」兩種效果，就受損與受害內容是相等[171]。對此，本文稱為「同源對稱」關係。至於電腦詐欺罪之「直接性」是指，財產上損害與得利行為是直接來自於電腦製作涉及財產權得喪變更紀錄行為。對此，可舉下

---

169 在意圖犯中，行為若已生構成要件該當結果，即屬既遂，至於行為人主觀上之不法意圖是否實現，則與既遂之成立與否無關。參見，林山田，《刑法通論（上冊）》，2002年11月增訂八版一刷，第236頁。

170 參見，林東茂，前揭文（註90），頁200。

171 Cramer, in: Schönke-Schröder, StGB, 25. Aufl. 1997, § 263 Rdnr. 53. Tröndle-Fischer, StGB, 49. Aufl. 1999. § 263 Rdnr. 39.

例說明：某公司員工將公司電腦系統內之庫存的貨品資料改成報廢資料，之後將這些物品從倉庫取出並賣給他人，以獲得不法利益。此例中之行為構成「輸入虛偽資料」，同時電腦也製成財產權得喪變更紀錄，而且也有獲得不法利益。只是，該不法利益不是來自電腦所製成財產權得喪變更紀錄，而是行為人之將公司貨品取出與後來之處分行為，因此，其行為不構成刑法第三百三十九條之三不正利用電腦取財得利罪，而是刑法第三三五條第一項侵占罪。

㈢主觀不法構成要件

本罪之主觀構成要件除了包括一般主觀要件，如電腦詐欺取財故意（第一項）或電腦詐欺得利故意（第二項）之外，還包括特別主觀不法要件，如不法所有意圖（第一項）或不法利益意圖（第二項）。

三、刑法第三百三十九條之二、三與其他罪名間之關係

關於本罪與其他既有財產犯罪之關係，可說明如下：甘添貴教授認為，「電腦詐欺罪與普通詐欺罪間，不具備特別關係，也不具補充關係，但電腦詐欺罪之罪質，當然含有詐欺之成分，因此，二者具有吸收關係，即電腦詐欺罪為吸收規定，普通詐欺罪為被吸收規定。」[172]對此一問題，本文看法是擇一之排他關係，如果有人介入就是普通詐欺罪，如果是沒有人介入之自動化過

[172] 甘添貴，前揭書（註136），頁339。

程，則屬於電腦詐欺罪，在網路上所發生之網路拍賣詐欺即屬於此種情形。舉例而言，行為人在網站上刊登不實廣告之行為，並從事從事虛偽競標，以向被害人詐財[173]。事實上，不管是登廣告或者輸入虛偽資料從事競標，都可以說行為人影響拍賣網站關於交易資料處理過程，不過，此類行為與電腦詐欺罪所要規範之行為之最大不同之處在於，行為人僅是以電腦資料處理作為犯罪工具，向被害人傳送不實資訊，因此其行為應僅構成傳統之詐欺罪，而非電腦詐欺罪。

至於電腦詐欺罪與偽造準私文書罪，由於甘教授認為詐欺罪所保護之法益包括個人之財產法益與社會之公共信用法益，因此，認為兩罪所侵害之法益具有同一性，應成立法條競合，優先適用吸收規定之電腦詐欺取財罪，排斥適用被吸收之偽造準文書罪[174]。

在濫用提款卡冒領現金之案例中，行為人可能同時構成刑法第三百三十九條之二與第三百三十九條之三，依據我國學者之見解，刑法第三百三十九條之二與第三百三十九條之三為事實上法條競合之關係，屬於特別構成要件之第三百三十九條之二排斥屬於普通構成要件之第三百三十九條之三[175]。針對此一問題，本文補充如下，如果在使用不法取得之真卡或偽造之卡片行為之評

---

173 日前刑事局破獲國內一樁利用雅虎奇摩拍賣網站詐財的詐欺案。該案事實如下：行為人進入拍賣網站後，先以假資料同時申請二十幾組會員帳號，再就高價位電子商品，刊登圖文並茂的廣告，以假競標、假交易的方式自行評估通過會員評價制度，誘騙被害人上當，並暗示是偽卡盜刷商品，底價很低，讓被害人瘋狂競標，再要求先行匯款並以流行的「宅急便」送貨到家。但等到買方將錢轉帳匯入指定帳戶，卻收不到貨品。

174 甘添貴，前揭書（註136），頁338。

175 參見，林山田，前揭文（註143），頁86；同作者，前揭書（註137），頁428；黃榮堅，前揭文（註138），頁323-24。

價，不採取本文所提議之糾正性解釋，則使用不法取得之真卡或偽卡並不會構成刑法第三百三十九條之三構成要件之「」，因此，即使藉由前述卡片濫用行為而從自動付款機器取得財物或財產上利益之行為也不會構成刑法第三百三十九條之二，當然就不會有兩構成要件競合之問題。又如前文討論所提及，如果將「輸入」解釋成「儲存」，則此等無權使用他人卡片資料之行為也不構成第三百三十九條之三所規定之兩種構成要件行為「輸入虛偽資料」或「輸入不正指令」中之任何一種，因為行為人都只是依據機器所提示之訊息，依序對電腦下達指令，並無任何有關資料或程式之「輸入」行為。即使銀行自動清算系統內之資料有所變更，都屬於機器自動所為，而非來自於行為人之行為。因此，藉由使用不法取得之真卡行為或偽卡而取得財物或財產上利益之行為只可能構成第三百三十九條之二。另一方面，如果採取本文主張之解釋方法，則可能構成第三百三十九條之二與第三百三十九條之三之法條競合關係，僅適用第三百三十九條之二即為已足。

肆、結　論

一、第三百三十九條之二不正利用自動付款設備取財得利罪之檢討

關於本條，首先要指出之立法缺陷是沒有未遂犯處罰之規定，此乃處罰上漏洞[176]。再者，上文曾介紹過，有些學說主張解

[176] 參見，林山田，前揭文（註143），頁89；同作者，前揭書（註137），頁

釋本罪應以詐欺相似性為解釋方向，本文也採相同立場。但此將產生如下問題：在解釋上，如果行為方式不具備詐欺相似性，例如，使用複製鑰匙開啟自動櫃員機機器而取走現金，則僅構成刑法第三百二十條第一項之竊盜罪。因此這樣的適用結果可能產生以下結果：實際上，利用卡片操作與複製鑰匙開啟機器應屬等值行為，但法定刑卻有第三百三十九條之二的三年以下與三百二十條第一項的五年以下有期徒刑之差別。

如前所述，刑法第三百三十九條之二是為了彌補自動付款設備濫用行為無法以竊盜罪與詐欺罪處罰之法律上漏洞，但值得討論之問題的是法定刑是否適當。自從本法通過施行後，社會上有法定刑過輕之批評，故 2002 年 11 月行政院院會針對電腦犯罪所通過之刑法修正草案中曾提高本罪法定刑，將 1997 年該次所通過之「處三年以下有期徒刑、拘役或一萬元以下罰金」改為「處五年以下有期徒刑、拘役或十萬元以下罰金。」立法理由在於「以詐術使銀行行員陷於錯誤而交付財物，係犯刑法第三百三十九條之詐欺罪，最重可量處五年有期徒刑，然若以不正方法透過銀行付款設備取得財物，最重卻僅得處三年有期徒刑，刑度顯然失衡，故將本條之最高刑度亦提高為五年有期徒刑。」[177]本文認為，從德國立法例可知，刑法第三百三十九條之二雖本質上為電腦詐欺罪之一種型態，但由於觸犯本罪者均屬不具備電腦知識，無法操縱電腦資料處理過程之尋常百姓，而且所造成之損害更無法與影響銀行或其他金融機構之電腦詐欺行為所造成之損害相比，故

430-31。

[177] 在2003年6月3日立法院第五屆第三會期第十四次會議審議時，此刑法修正草案並未獲通過。所以，刑法第三百三十九條之二不正利用自動付款設備取財得利罪之法定刑仍是原來所規定之三年以下有期徒刑、拘役或一萬元以下罰金。

我國立法者在 1997 年該次立法設立減輕規定，顯然是值得讚許之立法設計。

二、第三百三十九條之三不正利用電腦取財得利罪之檢討

從前文所述可知，與日本電腦詐欺罪立法例不同之處在於我國刑法第三百三十九條之三構成要件多了「不正方法」。正如前文所討論者，可能為贅語。不過，本文仍嘗試去給予新的意義，將此概念理解成「不正輸入行為」，而在不正輸入行為之下再分成：輸入虛偽資料與輸入不正指令。在此要提出者為，2001 年網路公約（Convention on Cybercrime）第八條與電腦有關之詐欺罪之規定為「出於為自己或第三人取得不法利益之詐欺或其他不誠實之意圖，故意的與無權的從事以下行為：一、輸入、修改、刪除或隱匿電腦資料。二、其他影響電腦系統運作之行為，並藉以造成他人財產損失。」[178]該公約在規定主觀要件之意圖與客觀要件之行為時，均使用了「無權」（without right）一詞。在翻譯意圖要件時，本文將 "without right" 一詞翻譯成「不法」。至於跟在故意之後之 "without right"，本文將之翻譯成「無權」。「無權」

[178] 網路犯罪公約第8條所規定之與電腦有關詐欺（Computer-related fraud）原文如下：Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:
a. any input, alteration, deletion or suppression of computer data;
b. any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

一詞在本構成要件中之地位，似乎類似於我國刑法第三百三十九條之三之「不正方法」。只不過，從歐洲議會所提出之解釋備忘錄中關於第八條之說明，無法得知該條約特別使用「無權」或「不法」之用意[179]。但從該公約其他條文所使用「無權」一詞之用法可知，此概念是強調對資料並無存取或修改權限。所以，該條文之「無權」是要來限制公約第八條第一項之輸入、修改、刪除或隱匿電腦資料，以及公約第八條第二項之其他影響電腦系統運作之行為。相較之下，我國之立法例所使用「輸入虛偽資料」與「輸入不正指令」之立法例已經足以彰顯詐欺罪之內涵，似乎沒有必要將構成要件之「不正方法」解釋成描述資料操縱行為是在未獲授權下進行；亦即，行為人所從事之輸入虛偽資料與不正指令等行為是未獲得系統管理者同意之行為。本文認為，資料操縱行為是否是在授權下進行並不是詐欺罪所考慮之重點，是否製造了輸入虛偽資料與不正確程式等影響資料處理程序結果之行為才是關鍵。

再者，由前文有關德國電腦詐欺立法例之介紹可知，德國立法例是以電腦操縱理論為立法範本。如果用傳統以來學說上有關電腦犯罪討論時所使用之輸入操縱、程式操縱、輸出操縱可知，我國刑法第三百三十九條之三所規定兩種行為類型：輸入虛偽資料與不正指令以製作財產權得喪變更紀錄，就是有關輸入操縱與程式操縱之立法，顯然地，缺少輸出操縱與硬體操縱。

在輸出操縱之情形，如果是針對電腦輸出物，由於本身已經是文書，自得視具體情況而依據偽造文書與行使偽造文書罪，以

---

[179] Explanatory Report to the Convention on Cybercrime, No. 90. 〈http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.〉(visited June 11, 2003)

及傳統詐欺罪論處。值得注意者，由德國學說之討論可知，有些輸出操縱是用電腦詐欺罪來規範。相對照之下，我國之立法似有不完善之處；再者，電腦資料處理程序有賴資料與軟、硬體配合。對此資料處理程序的操縱可由此三個部分來著手：資料操縱、程式操縱與硬體操縱。因此，在將來修法上，有必要增設類似於德國第二百六十三條 a「其他無權影響資料處理過程」之網羅性構成要件規定來涵蓋諸如硬體操縱或其他新的操縱技術。

本文在有關刑法第三百三十九條之三客觀構成要件分析時已經指出，在自動櫃員機濫用案例中可能無法適用「輸入虛偽資料」或「輸入不正指令」之構成要件。現今立法上的迫切問題在於如何規範以無權使用他人資料方式影響資料處理程序之結果，因而取得財產上不法利益之行為。從前文關於德國立法例之介紹可知，德國刑法第二百六十三條 a 之「無權使用資料」可用來規範自動櫃員機濫用或其他新技術之案例，如賭博性電玩機器、電話銀行之濫用與資訊系統濫用等。但由於我國刑法第三百三十九條之三並無與德國立法例之「無權使用資料」相類似條文，且目前條文所規定之「輸入不正指令」行為顯無法適用，形成處罰上漏洞。

在此必須強調者，前述自動櫃員機（ATM）與零售點終端機系統（POS）雖屬於電子支付方式，但還是屬於以消費者本人出示卡片傳統支付方式。將來所要發展的網際網路環境下的電子支付都不必送卡到機器前去刷卡，而是透過鍵盤，利用網路將資料送出去。以網路銀行為例，藉由個人電腦及其他終端機，透過網際網路與金融機構連線，利用存款帳號進行轉帳、繳稅、繳費、餘額查詢及信用卡購物等各項業務[180]。在此環境下所衍生之大多

[180] 楊正宏，《電子商務致勝教本》，金禾資訊股份有限公司，2002年4月初版

數濫用問題之特徵為冒用他人身份資料。目前網路信用卡冒用便為最明顯之案例。使用信用卡在網路進行支付，只要鍵入卡號、身分證明字號、有效日期便可刷卡，無須出示信用卡與當事人簽名，網路上之商店再以電腦連線連至信用卡中心，即可請款。在所取得為財物以外之利益情形，由於此一過程完全沒有人介入，無法適用傳統詐欺罪。但如本文多次提及之問題，在冒用他人信用卡之情形也可能無法依據我國刑法第三百三十九條之三論罪。

另外是關於主觀不法要件與未遂犯之立法建議。林山田教授曾指出，本罪由於在詐欺罪章，就其罪質而論，屬於獲利罪，而非如竊盜罪屬於取得罪，其在不法意圖上，與竊盜罪者有所不同，而本罪卻因循已經錯誤的第三百三十九條詐欺罪所規定之「意圖為自己或第三人不法之所有」；再者，本罪未設未遂犯之處罰規定，因此，林山田教授建議修正此不當立法[181]。針對前述未遂犯問題，本文認為在正式立法補救缺漏前應可採取補救辦法。2003 年 6 月 3 日立法院針對電腦犯罪所三讀通過之刑法修正條文中第三百五十八條之入侵系統罪[182]可以用來處罰意圖為自己或第三人不法利益入侵銀行系統而修改資料等未遂行為。

展望未來，以網際網路為基礎之各式電子支付會逐漸取代傳統支付工具，原本要用來規範利用自動化電腦資料處理程序以取得不法利益之行為之刑法第三百三十九條之三，由於構成要件之侷限性而影響適用範圍。在尚未修法前，補救之道應在於採取無

一刷，頁8-49。

181 林山田，前揭書（註137），頁430。

182 2003年6月3日立法院三讀通過之刑法第三百五十八條規定「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而使用他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」

權他人使用資料行為構成刑法第三百三十九條之一之「輸入虛偽資料」之解釋。

至於將來修法建議為將刑法第三百三十九條之三第一項與第二項分別規定為「意圖為自己或第三人不法之利益，以輸入虛偽資料或不正指令或以其他不正方法影響資料處理程序，而製作財產權之得喪、變更紀錄，而使他人財產受有損害者，處七年以下有期徒刑。」「前項之未遂犯罰之」。為了與刑法第三百三十九條之二相配合，本文認為應在條文中保留「不正方法」，藉以描述行為方式，以呈現不法內涵標示之功能。但由於樣態多樣化，故立法者僅以概括性條款之立法方式立法。因此，輸入虛偽資料、不正指令等均屬於「不正方法」之例示。並且將「不正方法」當成控制性解釋方法，藉以讓第三百三十九條之二與之三等能藉此與傳統詐欺罪在犯罪結構上與不法內涵上達到等值性之要求。

參考資料

一、中文期刊論文

1. 林山田，〈評刑法修正草案〉，《台大法學論叢》，第 20 卷第 1 期。
2. 林山田，〈評詐欺罪章中之新增三罪〉，《月旦法學》第 49 期。
3. 林東茂，〈詐欺罪的財產損害〉，《警大法學論集》，第 3 期。
4. 林東茂，〈詐欺或竊盜-一個案例的檢討〉，《刑事法雜誌》第 43 卷第 2 期。

二、中文書目

1. 林山田，《刑法通論（下冊）》，2002 年 11 月增訂八版一刷。
2. 林山田，《刑法各罪論（上冊）》，2002 年 4 月修訂三版一刷。
3. 林山田，《刑法各罪論（下冊）》，2002 年 4 月修訂三版一刷。
4. 甘添貴，《體系刑法各論》，第二卷，2000 年 4 月初版。
5. 前田雅英著，董幡興譯，劉俊麟校訂，《日本刑法各論》，五南圖書出版公司，2000 年 5 月初版一刷。
6. 黃榮堅，《刑罰的極限》，2000 年 4 月，元照初版第二刷。
7. 黃榮堅，《刑法問題與利益思考》，1995 年 6 月，月旦初版。
8. 法務部保護司主編，《電腦犯罪問題研討論實錄》，法務通訊雜誌社，1987 年 8 月三版。

三、西文期刊論文

1. Tiedemann, Klaus: Die Bekämpfung der Wirtschaftskriminalität durch den Gesetzgeber, in: JZ 1986, 865ff.
2. Bühler, Christoph: Ein Versuch, Computerkriminellen das Handwerk zu legen: Das Zweite Gesetz zur 34.Bekämpfung der Wirtschaftskriminalität, in: MDR 1987, 448ff.
3. Ranft, Otfried, Zur "betrugsnahen" Auslegung des 263a StGB, in : NJW 1994, 2574ff.

4. ders., Der Bankomatenmißbrauch, in : wistra 1987, 79ff.
5. Mitsch, Wolfgang: Strafbare Überlistung eines Geldspielautomaten-OLG Celle, NJW 1997, 1518, in : JuS 1998, 307ff.
6. Haft, Fritjof: Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG), in: NStZ 1987, 6ff.
7. Bühler, Christoph: Geldspielautomatenmißbrauch und Computerstrafrecht, in: MDR 1991, 16ff.

四、西文書目

1. Lenckner, Theodor, Computerkriminalität und Vermögensdelikte, Heidelberg, Karlsruhe 1981.
2. Schultz, Hartmut: Computerkriminalität, München 1992.
3. Sieber, Ulrich: Computerkriminalität und Strafrecht, 2. Aufl. Köln, Berlin, Bonn, München 1980.
4. Dreher, Eduard/Tröndle, Herbert: Strafgesetzbuch und Nebengesetze, 47. Aufl. München 1995.
5. Lackner, Karl/Kühl, Kristian: Strafgesetzbuch mit Erläuterungen, 23. Aufl. München 1999.
6. Lackner, Karl: Strafgesetzbuch mit Erläuterungen, 21. Aufl. München 1995.
7. Tröndle, Herbert /Fischer, Thomas. Strafgesetzbuch und Nebengesetze, 49. Aufl., München 1999.
8. Schönke, Adorf/Schröder, Horst, Strafgesetzbuch, 25. Aufl. München 1997.
9. Wessel, Johannes/Hillenkamp, Thomas, BT/2 , 22. Aufl. 1999 Heidelberg.1999.
10. Maurach, Reinhart/ Schroder, Friedrich-Christian/Maiwald, Manfred BT/1 8. Aufl. Heidelberg 1995.