專題企劃

淺談個人資料保護法民事賠償責任及數位鑑識相關問題

達文西個資暨高科技法律事務所主持律師 葉奇鑫
內政部警政署資訊室主任 李相臣

目　次

壹、前言——甚麼樣的土司會讓人流淚

據報載，一名具國立大學博士學位的科學園區工程師，在購物網站看到一款號稱「好吃到會流眼淚」的法式香烤吐司，售價僅新臺幣（下同）99元，就以某銀行信用卡付款。未料，剛完成消費，即接到詐騙電話，前後7次提款及轉帳，被騙1,200萬元。想像一下，一個如各位一般，在日常生活中謹慎小心絕不輕易透漏個人資訊的人，有一天，卻發現應該只有銀行知道的個人金融資料外洩了，這些原本應該萬無一失的個人資訊，現在卻可能因為網路犯罪造成損害，產生無從預知的不安全感。

「網路犯罪」（Cybercrime）已經成為所有利用網際網路作為犯罪手段的代名詞，雖然目前學說和實務並沒有一致定義，但多數學者認為「網路犯罪」著重在利用「網際網路」作為犯罪手段的特殊性。無論由個人資料的外洩造成有心人士為犯罪行為（例如網路詐騙），或是藉由網路駭客取得企業內的客戶資料，都是網路犯罪的主要型態。近年國外著名的個資外洩案例，例如英國的跨國連鎖百貨公司TJX，於2006年12月間發現該企業分別在2003年及2006年時，遭遇網路駭客入侵該公司電腦主機，竊取了客戶的信用卡、Debit卡以及其他支票紀錄等交易資料。此外，即使為全球知名的金融集團，客戶資料也可能不再安全。以美國花旗銀行為例，在2011年銀行內部所做的例行監控檢查中，發現資料庫曾遭駭客入侵，粗估約有20萬人資料遭竊[1]。

依據內政部警政署刑事警察局統計數據，2009年1～8月網路犯罪的項目中，將近7成（66.28%）的網路犯罪涉及網路詐欺和妨害電腦使用[2]。依據2010年1～10月電腦犯罪案件統

1　參閱http://news.networkmagazine.com.tw/classification/security/2011/06/10/24915/，最後檢索日：2012年01月01日。
2　參閱http://www.cib.gov.tw/crime/crime_stat.aspx，最後檢索日：2012年01月01日。

計，1～6月電腦網路犯罪發生數主要為詐欺案5,215件（占55.23%）為最多，妨害電腦使用1,708件（占18.09%）次之，智慧財產權案件1,176件（占12.45%）。而知名防毒公司賽門鐵克（SYMC）於2011年公布的「網路安全調查報告」（2011 State of Security Survey）中指出，2010年10月至2011年8月，台灣大約有67%的公司遭受過網路攻擊，受訪者更將網路攻擊列為主要擔憂因素[3]。此外，根據資策會FIND / 經濟部技術處「創新資訊應用研究計畫」統計，2010年第1季臺灣經常上網人口為1,068萬人，網際網路連網應用普及率為46%，而藉由網路產生的新興犯罪也隨著網路使用的快速成長不斷增加。

《個人資料保護法》（以下簡稱新個資法）即將施行，新法適用行業別擴增至各行各業，甚至蒐集個人資料的自然人也成為受規範對象。新法不區分個資筆數多寡或企業資本額，一律受到規範。此外，保護客體擴展到電腦處理以外的所有紙本或以其他方式蒐集處理利用之個人資料。若保有個人資料的公務或非公務機關發生個資外洩，造成當事人財產或非財產上損害，如當事人無法證明實際損害額時，新個資法定有每人每一事件500元以上2萬元以下之賠償範圍，對於同一原因事件造成之損害，最高賠償額更可達2億元。高額賠償規定對於擁有個人資料的企業而言，勢必造成嚴重衝擊。尤其新法引進團體訴訟機制後，個人資料受違法侵害之當事人不再需要自行提起訴訟，可委由公益團體為當事人提起訴訟、聘請律師及繳納裁判費等，當事人只需賦予訴訟實施權於公益團體即可進行求償，訴訟成本將大幅降低，勢必增加民眾提起個資訴訟的意願。

至於新個資法施行後，高額賠償責任究竟會帶來多少衝擊？若以鄰近日本為例，日本於2010年上半年發生之個資外洩十大事件中（詳參圖1），雖未發生涉及百萬人之重大事件，但是有涉及20萬人以上的個資外洩事件，且單就該年度上半年實際發生之個資事件即高達1,679件、共計557萬9,316人受害，因個資外洩造成之損失約1,215億7,600萬日圓，無論民間與政府都付出重大代價。

由日本JNSA協會所製作的統計數字來看，2010年已經是外洩數量最低的年度，如以外洩高峰期2007年觀之，僅有864件外洩事件，但造成了3,053萬人個資外洩，其受害人數更為可觀。

從時間序列觀察，日本個資法施行於2005年，而損害賠償案件高峰在施行後2年發生，接下來損害賠償總額即逐年降低。據推測，剛施行幾年內賠償金額上升的趨勢，可解釋為民眾與律師學習以個資法求償之學習曲線，而保有個資單位在施行前幾年遭求償成功後，即學習導入資安系統、數位鑑識科技等等，以降低個資外洩事件或減輕賠償責任，是以賠償總額開始逐年下降，該階段可謂為公務機關或非公務機關學習防範個資外洩之下降曲線（詳參圖2）。

3 詳細調查報告請參閱http://www.symantec.com/content/en/us/about/media/pdfs/symc_state_of_security_2011.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Aug_worldwide_securitysurvey，最後檢索日：2012年01月01日。

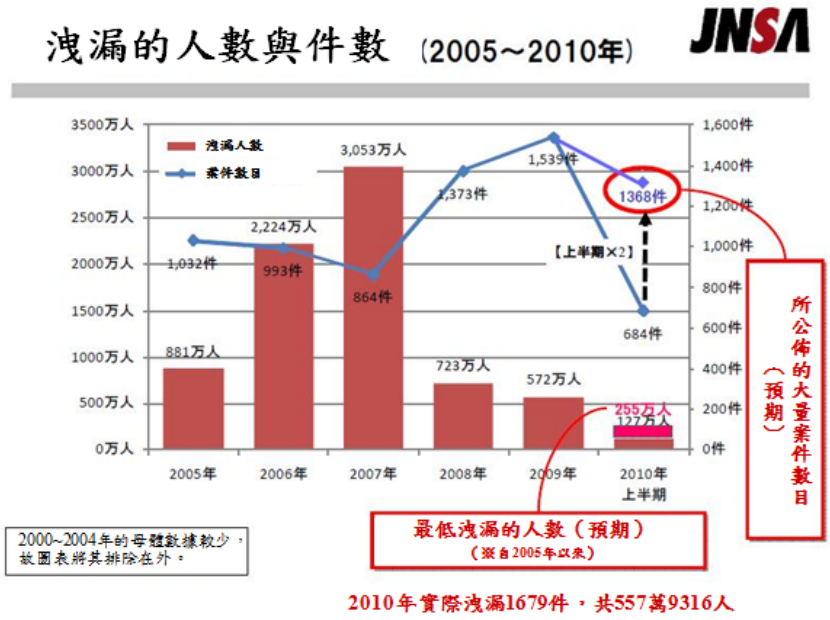

圖1　日本個資外洩事件洩漏人數與件數概況（2005~2010年）[4]

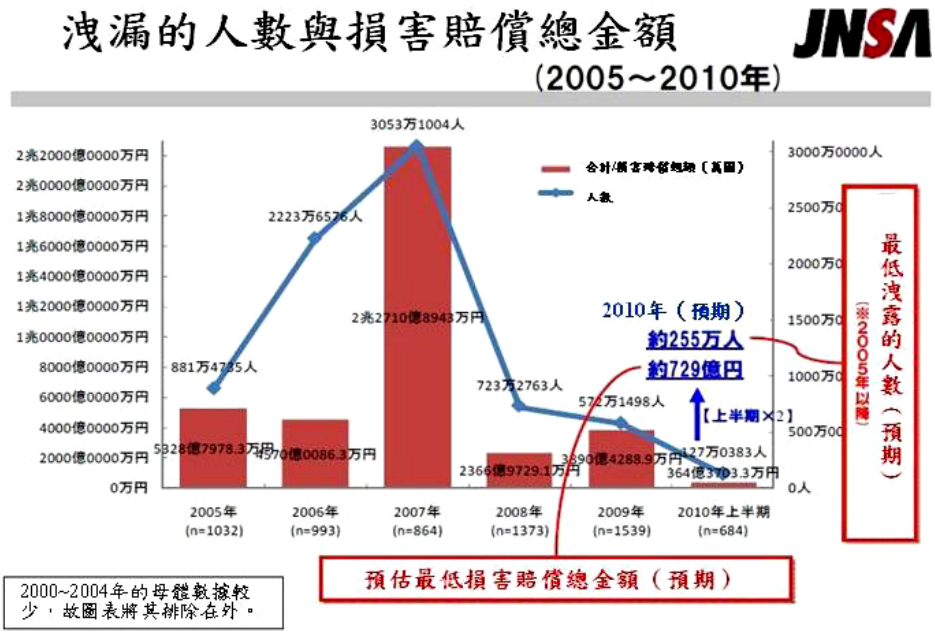

圖2　日本個資法公布後損害賠償總額曲線圖（2005~2010年）[5]

我國於新個資法上路後，未來5年個資求償趨勢為何，應可由國情及法規制度接近之日本參酌得知。基於日本人口為臺灣人口的5.4倍，我國新個資法正式施行日期約在2012年中旬，則以日本求償時間序列推估，我國個資民事損害賠償事件之求償高峰，約在2014年至2015年

4　本表為台灣經濟研究院彙整日本網路安全協會2011資訊保安報告書之資料後繪製，前開報告書詳見http://www.jnsa.org/result/incident/2010.html，最後檢索日：2012年1月1日。

5　本表為台灣經濟研究院彙整日本網路安全協會2011資訊保安報告書之資料後繪製，前開報告書詳見http://www.jnsa.org/result/incident/2010.html，最後檢索日：2012年1月1日。

間出現。如以人口數、民事賠償是否訂有上限、是否有個資保險制度、資安保護水準等種種因素納入考慮，則我國2013年之個資求償訴訟標的預估將達到100億元水準，而高峰期則可能達到300到500億元。因此對於因應新個資法施行後所需的各種法規制度，包含數位證據保存與數位鑑識法規，都有加以重新檢視之必要。

隨著網際網路使用率大幅提升，應運而生的網路犯罪亦日益猖獗，即使小心謹慎不輕易留下個人資料，也可能因為其他管道的外洩或藉由網路犯罪手法取得個人重要資訊，進而造成財產損失。在網路時代，任何人皆有可能成為前述案例中的網路犯罪被害者。此外，由於網路活動具有數位化與高度匿名性，活動紀錄不易儲存、容易竄改等特徵，因此於犯罪偵查與訴訟活動中，數位證據與鑑識便扮演了極為重要的關鍵角色。因此，若欲健全個資保護制度，勢必一併檢視以下將探討的數位鑑識相關問題。

貳、數位鑑識法制因應個人資料保護法可能產生之變革

一、數位證據

所謂數位證據，是指在電腦或網路設備中以電磁紀錄方式儲存而可供佐證犯罪之資料。有學者認為於電腦或網際網路中，資訊以數字零及一排列方式儲存，且系爭零與一數列可為犯罪事實認定者，即為數位證據[6]。亦有學者參照《電子簽章法》之規定，該法第2條第1項規定「電子文件：指文字、聲音、圖片、影像、符號或其他資料，以電子或其他以人之知覺無法直接認識之方式，所製成足以表示其用意之紀錄，而供電子處理之用者」。而認為將以人的知覺可以直接辨識之文字、聲音、圖片、影像、符號等以電子等無法以人之知覺直接辨識之方式儲存記錄，而該紀錄又作為特定事實證據時，該記錄即得稱為數位證據[7]。亦有學者認為以電腦或電子設備儲存或傳送特定具有表示意義之文字、聲音、圖片、影像、符號或其他資料，而該資料又可作為特定事實之證據時可稱為數位證據[8]。而數位證據不僅指儲存於電腦之證據，儲存於電子產品中之數位紀錄，亦可能成為數位證據[9]。

數位證據多由於電腦犯罪或網路犯罪而產生[10]，而電腦犯罪的定義，學說上有狹義說及廣義說，主張狹義說之學者認為電腦犯罪係指與電子資料有關之故意而違法之財產破壞行為，即使用電腦程式或相關設備破壞財產法益之財產罪[11]。主張廣義說之學者則稱，電腦犯罪即任何與電腦及其相關設備有關之犯罪，以電腦為犯罪工具或以電腦為犯罪之標的者皆可稱之[12]。亦有學者認為僅有以電腦為犯罪工具而使自己獲益或他人遭損失可稱之為電腦犯罪[13]。另有學者稱利用電腦之特性，以電腦為犯罪場所或電腦作為行為客體，可稱為電腦犯罪[14]。而電腦證據係指電腦犯罪之證據，即以

6 蘇清偉，電腦犯罪之數位證據鑑識，刑事科學第51期，2001年3月，頁81。
7 陳家瑤、吳佳育，數位證據於現行法律之相關問題，2002年「網際空間：資訊、法律與社會學術研究暨實務研討會論文」，2002年，頁94。
8 蔡震榮、黃玥婷，數位證據之證據力，刑事法雜誌第49卷第2期，2005年4月，頁3。
9 王以國，數位證據之刑事證據能力相關議題研究，科技法律透析，2008年11月，頁13。
10 劉秋伶，數位證據之刑事調查程序，國立政治大學法律學研究所碩士論文，2010年1月，頁11。
11 林山田，電腦犯罪之研究，刑事法論叢㈠，台大法律系，1987年5月，頁137-138。
12 *Id.*
13 劉江彬，資訊法論——電腦法律問題之探討，1999年1月，頁187。
14 蔡美智，虛擬世界的脫軌棋子——國內電腦犯罪與脫序事件簡介，律師雜誌第228期，1998年9月，頁52-53。

電磁紀錄之方式儲存之電子證據[15]。而數位證據的蒐集，便需要藉由數位鑑識程序，加以取得及保存。

二、數位鑑識於我國現行法制上之應用

數位鑑識程序涉及數位證據的保全及蒐集，而有關證據保全、蒐集等程序在訴訟法上，主要規範於《民事訴訟法》及《刑事訴訟法》，若以刑事訴訟程序而言，其所涉及的法規範尚包含《通訊保障及監察法》、《警察偵查犯罪手冊》及《刑事鑑識規範》等。分析如下：

㈠刑事訴訟程序

在刑事程序上，對於存放於電腦網路設備內資料進行犯罪之偵查蒐證，便是以電磁紀錄為偵查之客體。然而，不論是在實體法或程序法上，我國現行法並無「數位證據」抑或「數位鑑識」一詞，其在概念上較接近「電磁紀錄」。而「電磁紀錄」一語納入我國法規範加以定義及使用，首見於1997年10月刑法第220條第2、3項之增修：「錄音、錄影或電磁紀錄，藉機器或電腦之處理所顯示之聲音、影像或符號，足以為表示其用意之證明者，亦同。稱電磁紀錄，指以電子、磁性或其他無法以人之知覺直接認識之方式所製成之紀錄，而供電腦處理之用者」。直至2005年2月刑法修正而增訂妨害電腦使用罪章時，因刑法中涉及電磁紀錄之犯罪，已不限偽造文書印文罪章方得適用，立法者乃將本條第3項規定刪除，移列於總則篇第10條第6項，並將相關文字修正為「稱電磁紀錄者，謂以電子、磁性、光學或其他相類之方式所製成，而供電腦處理之紀錄」。

犯罪偵查過程中，為保全犯罪證據及被告，以利日後之追訴，刑事程序上搜索扣押等強制處分自有其必要性。惟相較於傳統的物證或書證，數位證據具有如：資訊存量龐大、傳遞快速；原始資料須經機器設備顯示其內容，無法以人的知覺直接辨識理解；資料容易複製，不易辨別是否為原本；資料容易竄改，不易辨別其內容之真實性；資料製作者不易確認，多需依賴科技及其他相關事證輔助等特性[16]。因此，數位證據不像一般刑案之犯罪證據來得有形以及具體，而極易被湮滅或損毀，這也使得其在證據之保全及蒐集上較一般傳統案件困難許多。首先，就蒐證程序而言，執法人員發現犯罪嫌疑時，其欲取得嫌犯電子郵件之資料，以及實體IP位置和所在實體位置，以利鎖定犯嫌目標，進而鎖定搜索地點或監聽對象，目前的作法是直接與擁有該資料之網路業者及電信業者聯繫，請求提供所需之資訊。惟因業者保存資料之期限不一，回覆之效率亦有所不同，且近來人權意識高漲，若業者以法無明文為由不予配合，將導致執法機關蒐證之困擾[17]。就目前刑事訴訟實務而言，數位證據之分析多半由承辦該案件之司法警察負責，然而科技日新月異，數位證據的數量急速成長，尤其在如竊取個人資料為犯罪行為的網路犯罪型態中，對於數位證據的蒐證更形重要，司法警察機關對於數位鑑識的能力勢必加以強化，以避免日後檢辯雙方於法庭攻防時，衍生出數位證據之證明力、甚至證據能力等問題。

其次，由於數位證據的保全將因執法人員取得資料之時點及資料是否涉及通訊內容，可區分為：「即時取得的內容通訊資料」、「即時取得的非內容通訊資料」、「非即時取得的內容通訊資料」及「非即時取得的非內容通訊資料」等四類，依我國目前《通訊保障及監察法》（以下簡稱「通保法」）及電信相關法

15 蔡震榮、張維平，電腦犯罪證據之研究，刑事法雜誌第44卷第2期，頁52。

16 王以國，數位證據之刑事證據能力相關議題研究，科技法律透析2008年11月，頁12-18。

17 潘維大、成永裕、葉奇鑫、法思齊、徐育安，「網路犯罪數位證據蒐集保全程序與相關證據法則之探討」，行政院法務部委託研究案（計畫編號：HU961002），2008年9月22日，頁63-81。

令，僅有涉及關於內容之蒐集，方適用通保法規範。在「即時取得的內容通訊資料」之情形，應可適用通訊監察之程序，惟就「非即時取得的內容通訊資料」，如儲存於被告或第三人電腦硬碟中之電子郵件內容或即時通訊交談紀錄等，應遵循通訊監察或搜索扣押之方式辦理，或由偵查機關逕為合目的性之判斷，在適用法律上尚存有諸多爭議[18]。最後，就審判階段而言，由於數位證據具有技術性，易變造、偽造、毀壞，又不易鑑定，因此易遭被告針對數位證據提出如：搜索不合法、傳聞證據、真實性「可能被竄改」之抗辯、真實性「程式可靠度」（Reliability of Computer Programs）抗辯或溢波抗辯等，而造成法官與檢察官在使用數位證據時極大困擾[19]。司法警察在犯罪偵查過程中，雖有《警察偵查犯罪手冊》第4章第17節「電腦犯罪案件之處理」之注意事項可供參考，惟從上述討論之爭議可知，數位證據的蒐證保全因涉及複雜及專業採證過程，日後自需研擬更為周詳之數位證據保全或採證程序規定供遵循，以確保數位證據在審判程序之證據能力與證明力。

㈡民事訴訟程序

相較於刑事訴訟程序的強制處分係由公權力介入的方式進行證據保全，民事案件採行當事人平等原則，且訴訟程序中的證據提出，皆須依照民事訴訟法第277條有關舉證責任之分配規定，應由主張有利於己事實之當事人，就其事實負擔舉證責任。因此，若當事人無法就有利於己之事實舉證時，該當事人可能遭受敗訴判決。換言之，當事人提供數位證據於法庭時，更需透過專家協助，經由一定的程序將數位證據呈現於法庭，以獲得有利於己之判決。然而，現行民事訴訟相關法規對於數位證據之提出或鑑識，僅得利用民事訴訟法第324條以下有關「鑑定」、第363條以下「書證」中有關「準文書」或第364條以下有關「勘驗」等程序就個案加以適用，並未因應數位證據之特殊性而有所特別規範。再者，就我國目前關於數位鑑識的討論，多從網路犯罪出發，再論及刑事訴訟相關規範。然而，在新個資法即將施行之際，未來如何在個資保護案件上發揮「發現事實」之功能，仍有賴數位鑑識在民事訴訟相關法制的發展。

㈢為因應網路犯罪數位鑑識制度應有的發展方向

為有利於網路犯罪的蒐證與證據保存，現行的數位鑑識制度應從證據資料保存、證據保全以及審判程序各階段分別予以討論，思考更健全的制度設計，以因應多元化的網路犯罪型態。

1. 證據資料保存階段

網路犯罪發生後，必須先完整保存數位資料，才能就該資料篩選出得以進行數位鑑識的證據。然而，就現行法規而言，《第二類電信事業管理規則》第27條之規定，規範電信業者針對不同紀錄之資料進行不同之保存期限，其最長之保存時限僅有六個月，但從數位證據蒐證來說，六個月的保存時間似乎不足。

關於資料保存期限，由於現行《商業會計法》等有關資料保存年限規定，以及新個資法中請求權時效分別為二年、五年的規定[20]。本文建議，《第二類電信事業管理規則》第27條[21]可參考上述法規將資料保存期限依據重要程度

18 吳兆琰，論網路環境下的通訊監察法制，科技法律透析，2005年2月，頁54-56；蔡美智，「通訊保障及監察法」關於網路監聽的相關爭議，資訊法律透析，1999年12月，頁39-40。

19 潘維大、成永裕、葉奇鑫、法思齊、徐育安，「網路犯罪數位證據蒐集保全程序與相關證據法則之探討」，行政院法務部委託研究案（計畫編號：HU961002），2008年9月22日，頁101-104。

20 個人資料保護法第30條：「損害賠償請求權，自請求權人知有損害及賠償義務人時起，因二年間不行使而消滅；自損害發生時起，逾五年者，亦同。」

21 第二類電信事業管理規則第27條：

加以適度延長。避免屆時因保存期限不足，造成證據滅失或毀損，而無法成為訴訟上證據之缺憾。

再者，由於現行規定除了電信業者以外，不論是網路服務業者（ISP）或是網路內容業者（ICP），尚無資料保存之相關規範。但消費者的資料在訴訟上對於其主張是否成立都有重要關聯，若未針對上述業者規範消費資料的保存義務，可能對消費者未來在訴訟上提出證據時產生不利影響。因此，建議對於上述ISP與ICP業者，可參考《第二類電信事業管理規則》對於數位資料保存期限之規定，適度延長保存期限至服務契約終止後若干年，以利證據保存。

而有關電子商務業者保存及提供電子資料之義務，目前並無法律規範其保存年限，僅有相關定型化契約範本中提及業者之保存時間。反觀線上遊戲產業，由於竊取線上遊戲寶物、帳號被盜及遊戲點數使用上的相關爭議時有所聞，而數位資料保存對於案件偵辦及處理上又有相當重要性，因此目前透過「線上遊戲定型化契約範本」第13條規定不得低於三十天保存期，以及「個人網路銀行業務服務定型化契約範本」第18條資料要求保存年限為五年，據此要求業者，就其登錄資料及交易資訊給予一定程度的保存。

由於《消費者保護法》（以下簡稱消保法）第17條規定，主管機關得於定型化契約中訂定應記載和不得記載事項。因此本文建議可參考「線上遊戲定型化契約範本」與「個人網路銀行業務服務定型化契約範本」有關資料保存年限之規定，於現行電子商務業者之定型化契約範本內，增訂業者的資料保存以及資料提供義務，而其保存期限亦建議適度延長至契約終止後若干年。此外，若證據資料保存涉及電子文件時，則可參考《電子簽章法》第6條[22]之規定辦理，如此將有助於網路犯罪發生後，有

經營者對於調查或蒐集證據，並依法律程序查詢電信之有無及其內容者，應提供之。
前項電信內容之監察事項，依通訊保障及監察法規定辦理之。
經營者對於第一項電信通信紀錄應至少保存期間如下：
一、語音單純轉售服務通信紀錄應保存六個月。
二、網路電話服務通信紀錄應保存六個月。
三、網際網路接取服務：
㈠ 撥接用戶識別帳號、通信日期及上、下網時間等紀錄應保存六個月。
㈡ 非固接式非對稱性數位用戶迴路（ADSL）用戶識別帳號、通信日期及上、下網時間等紀錄應保存三個月。
㈢ 纜線數據機用戶識別帳號、通信日期及上、下網時間等紀錄應保存三個月。
㈣ 張貼於留言版、貼圖區或新聞討論群之內容來源IP位址與當時系統時間應保存三個月。
㈤ 免費電子郵件信箱及網頁空間線上申請帳號時之來源IP位址及當時系統時間應保存六個月。
㈥ 電子郵件通信紀錄應保存一個月。
四、虛擬行動網路服務通信紀錄應保存六個月。
經營者應核對及登錄其用戶之資料並至少保存至服務契約終止後一年；有關機關依法查詢時，經營者應提供之。虛擬行動網路服務經營者或E.164用戶號碼網路電話服務經營者應將使用者資料載入其系統資料檔存查後始得開通；以預付卡或其他預付資費方式經營虛擬行動網路服務者或E.164用戶號碼網路電話服務者，亦同。
前項用戶之資料包括使用者姓名、身分證統一編號、第二證件號碼及住址等資料，且虛擬行動網路服務經營者或E.164用戶號碼網路電話服務經營者另應包括所指配號碼。
前項證件號碼，於法人申請時，指營利事業登記證號及代表人身分證號；於自然人申請時，指身分證號及足資辨識身分之證明文件證號。
主管機關得限制經營者受理民眾以同一身分證統一編號申請電信服務之用戶號碼數。經營者應依主管機關公告之限制條件及執行方式辦理。
第四項之虛擬行動網路服務經營者或E.164用戶號碼網路電話服務經營者應於受理申請二日內完成其使用者資料之載入。

22 電子簽章法第6條：
文書依法令之規定應以書面保存者，如其內容可完整呈現，並可於日後取出供查驗者，得以電子文件為之。
前項電子文件以其發文地、收文地、日期與驗證、鑑別電子文件內容真偽之資料訊息，得併同其主要內容保存者

關犯罪證據之保存。

最後，在證據資料保存階段，為提高業者保存意願以及分擔成本，建議可參考《電信事業處理有關機關查詢電信通信紀錄實施辦法》訂定《網路事業處理有關機關查詢紀錄實施辦法》，使業者提供數位資料時可要求機關或當事人於請求業者調閱資料時皆須負擔一定費用，確保業者和使用者皆有一定的收費標準可依循。

2. 證據保全程序

由於數位證據具有易於竄改及毀損的特性，因此需要特殊的保存方式。在偵查階段，目前並未針對數位證據有所規範，為健全數位證據保存程序，本文建議於現行《法務部贓證物庫處理數位證據注意事項》中，針對數位證據之保存加以規範，以利日後於訴訟中進行數位證據之鑑識與分析。於訴訟階段，本文亦建議增訂「司法院贓證物庫處理數位證據注意事項」，對於法院保存數位證據的程序與環境有所明確規定，以妥善保存數位證據。

此外，由於數位證據蒐證及分析的標準作業流程部分，為數位證據得否於法庭上作為釐清案件使用之關鍵，而成為數位鑑識專家最重視之核心議題。目前第一線蒐集數位證據之人員主要由警察和調查局調查官負責，因此各該單位的採證程序非常重要。在警察人員部分，目前警政署定有《警察偵查犯罪手冊》，該手冊對於各單位處理各類刑事案件應如何踐行採證程序有所規定，但該手冊卻未對數位證據採證之流程加以規範。為因應數位證據之特性，建議可於《警察偵查犯罪手冊》增訂數位證據部分。而調查局目前並未有公開的數位證據鑑識手冊，建議調查局得研擬「調查局偵查犯罪手冊」，制訂數位鑑識標準作業流程。美國聯邦調查局鑑識手冊（Forensic Handbook）中有關數位鑑識有完善之注意事項，或許有關單位可參考該手冊，做為我國第一線執法人員在程序上之參考依據。至於在偵查中及審判中，則建議法務部增訂「檢察官處理數位證據注意事項」以及司法院增訂「法官處理數位證據注意事項」，以確保偵查中以及審判中得以順利針對數位證據進行鑑識及調查，確保其高度之證明力。

3. 審判程序

數位鑑識制度於審判階段之重點在於要提出哪些資料，以及如何提供，即所謂證據開示問題。參考美國聯邦民事訴訟法第26條有關「電子儲存資料」（Electronically Stored Information，ESI）提出之規定，兩造當事人依法應提供之電子儲存資料的範圍主要包含以下資料[23]：

⑴ 應主動提供與訴狀之主張或爭執相關，而可能提供訊息之人名、地址及電話。

⑵ 與訴狀主張或爭執相關，在該當事人佔有、保管或控制之下的所有文件、電子儲存資料、有體物的複製品、分類或存放地點。

⑶ 對造所請求的各種損賠金計算所依據之文件或其他證據資料的調查和複製品。

⑷ 保險契約。

因此，在我國民事訴訟程序上，本文建議可參考美國民事訴訟法中有關電子資料開示規定，增訂現行我國民事訴訟相關條文，或於目前《辦理民事訴訟事件應行注意事項》中，就電子儲存資料制定相關章節，以更加完善證據保存之規範。

三、小結

由以上說明可知，為因應新形態的犯罪，數位鑑識扮演極重要角色，尤其對於利用網路

為限。

第一項規定得依法令或行政機關之公告，排除其適用或就其應用技術與程序另為規定。但就應用技術與程序所為之規定，應公平、合理，並不得為無正當理由之差別待遇。

23 Stephen C.Yeazel, Federal Rules of Civil Procedural 69（2005）

和電腦犯罪發生所產生的民、刑事訴訟，更有賴完善的數位鑑識制度加以配合。當數位證據經由妥善蒐集和保存之後，隨即衍生出如何追究民、刑事責任的議題。其中，由於絕大多數的網路和電腦犯罪，都以各種個人資料為犯罪標的，因此於民事訴訟中與個人資料保護相關的賠償規定顯得更形重要。以下將藉由《個人資料保護法》之重要內容進行說明，並對法規適用可能產生的問題加以討論。

參、個人資料保護法相關規定簡介

我國對於個人資料之保護規範，始於1995年頒布之《電腦處理個人資料保護法》，後於2010年4月27日經立法院三讀修正通過，並於同年5月26日經總統公布之新個資法，為該法第一次且大幅度修法，影響層面之廣，不論公務或非公務機關均受規範，任何有關個人資料之蒐集、處理、利用及相關之檔案安全維護措施，皆須符合新法之規定，新法亦提高民事、刑事及行政責任。

新個資法中要求公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏[24]。非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏[25]。如違反新法之規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，須負損害賠償責任，其民事賠償金額更高達2億元[26]。

2011年10月27日《電腦處理個人資料保護法施行細則草案》（簡稱施行細則草案）預告公布，搭配新個資法，其中對於就網路犯罪可能涉及的相關問題有所特殊規範。

一、個人資料定義

新個資法第2條對於個人資料之定義如下：

「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。」

於施行細則草案第4條中對於上述病歷資料、健康檢查資料以及前科資料加以說明：

「（第1項）本法第2條第1款所稱病歷之個人資料，指下列各款資料：一、醫師依醫師法執行業務所製作之病歷。二、各項檢查、檢驗報告資料。三、其他各類醫事人員執行業務所製作之紀錄。（第2項）本法第2條第1款所稱醫療之個人資料，指除前項病歷以外，其他以治療、矯正或預防人體疾病、傷害、殘缺為目的，所為之診察、診斷及治療；或基於診察、診斷結果，以治療為目的，所為之處方、用藥、施術、或處置等行為全部或一部所產生之個人資料。（第3項）本法第2條第1款所稱基因之個人資料，指由一段去氧核醣核酸構成，為生物體控制特定功能之遺傳單位訊息。（第4項）本法第2條第1款所稱性生活之個人資料，指性取向或性慣行之個人資料。（第5項）本法第2條第1款所稱健康檢查之個人資料，指對於無明顯疾病症狀，非出於對特定疾病診斷或治療之目的，以醫療行為所為診察行為之全部或一部之總稱。（第6項）本法第2條第1款所稱犯罪前科之個人資料，指經緩起訴、職權不起訴或法院判決有罪確定之紀錄。」

施行細則草案將新個資法中較易混淆之病歷與醫療資訊概念作一釐清，惟語意上，病歷仍為醫療資訊概念所得涵括，似乎仍有必要加以說明。

24 個人資料保護法第18條。
25 個人資料保護法第27條第1項。
26 個人資料保護法第28條第4項。

二、安全維護義務

新個資法第18條：「公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏」，第27條第1項：「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏」。

因此公務機關和非公務機關對於所保有之個人資料皆有一定程度的保護義務，至於所謂適當安全維護措施的意義為何？在施行細則草案第9條中有如下規定：

「（第1項）本法所稱適當安全維護措施、安全維護事項或適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之必要措施。（第2項）前項必要措施，應包括下列事項：一、成立管理組織，配置相當資源。二、界定個人資料之範圍。三、個人資料之風險評估及管理機制。四、事故之預防、通報及應變機制。五、個人資料蒐集、處理及利用之內部管理程序。六、資料安全管理及人員管理。七、認知宣導及教育訓練。八、設備安全管理。九、資料安全稽核機制。十、必要之使用紀錄、軌跡資料及證據之保存。十一、個人資料安全維護之整體持續改善。（第3項）第一項必要措施，以所須支出之費用與所欲達成之個人資料保護目的符合適當比例者為限」。

三、告知義務

新個資法第12條規定：「公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人」。

按當事人之個人資料遭受違法侵害，往往無法得知，致不能提起救濟或請求損害賠償，因此新法規定公務機關或非公務機關所蒐集之個人資料被竊取、洩漏、竄改或遭其他方式之侵害時，應立即查明事實，以適當方式（例如：人數不多者，得以電話、信函方式通知；人數眾多者，得以公告請當事人上網或電話查詢等），迅速通知當事人，讓其知曉。

而施行細則草案則於第18條規定：「（第1項）本法第12條所稱適當方式通知，係指即時以書面、電話、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。但耗費過鉅者，得斟酌技術可行性及當事人隱私之保護，以網際網路、新聞媒體或其他足以使公眾得知之方式為之。（第2項）依本法第12條通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施」。

此外，公務機關違反本條規定而隱匿不為通知者，其上級機關應查明後令其改正，如有失職人員，得依法懲處；非公務機關違反本條規定而隱匿不為通知者，其主管機關得依新個資法第47條第2款規定限期改正，屆期仍不改正者，得按次處以行政罰鍰[27]。

肆、個人資料保護法可能產生之民事損害賠償問題

新個資法中要求各機關對於個人資料之維護須採行安全維護事項或適當安全措施，使我國個資保護水準與國際接軌，立意甚佳。惟國內中小企業甚多，如一律要求有蒐集個資之各種行業[28]，均需遵循本條規定建置符合國際水準之個資保護標準，恐將造成新進市場之任何企業，因考量個資法遵循成本過高之情形，而選擇放棄創業，實可能扼殺中小企業蓬勃發展之契機。以日本為例，其《個人情報保護法》中對於企業若於半年內未有一日處理超過

27 個人資料保護法第12條立法理由。

28 幾乎所有行業均必然蒐集員工之人事資料，因此所有行業均無法自外於本條規定之要求。

5,000筆個人資料之事業，不適用之；而澳洲對於年營業額不超過300萬元澳幣的企業亦毋須適用個資法，上述規定皆將規模較小的企業排除於個資法保護的範圍，以避免造成因法規遵循成本過高，而產生不必要的市場進入門檻，反而扼殺正常商業發展。上述規定，值得我國參考。

此外，我國新個資法第12條所規定之通知方式，除列明得以「書面」、「電話」、「傳真」、「電子文件」或「其他足以使當事人知悉或可得知悉之方式」為之，並考量耗費過鉅之情形，放寬得以網際網路、新聞媒體或其他足以公眾得知之方式為之，平衡機關通知成本與當事人權益保護。但新個資法第12條規定中所謂的「查明後」始有通知義務，是否可能使該條通知義務成為具文？且查明至何種程度始為「查明後」？未來勢必發生爭議。

而新個資法中，有關民事損害的規定，係採定額、限額的賠償制度。雖然如此規範乃為避免被害人舉證不易的窘境，惟此類案件之損害多具有抽象、主觀、難以計算之特性，再者新法雖規定公務或非公務機關皆應採行適當之安全維護事項或措施，惟應如何遵循及採取哪些必要措施法皆無相關之規範，未來實務上於審判案件時，將可能因審酌是否有達安全維護之標準不一，導致相同類型之案件損害賠償數額有所差異。

而由於現行《電腦處理個人資料保護法》僅限於電腦處理之個人資料遭到外洩或其他侵害時，方有請求損害賠償的可能性，因此大大降低了當事人引用現行個資法作為請求權基礎求償的機率。再者，現行法未設計團體訴訟機制，造成個資外洩的受害人若欲個別提起訴訟時，所需支出的訴訟成本（包含勞力、時間、費用等）負擔過鉅，因此現行《電腦處理個人資料保護法》自1995年施行至今鮮有對個資外洩之侵權單位提起訴訟者，自然缺乏有關個人資料外洩時，民事損害賠償的基準。法院欠缺賠償基準的情況下，自然難以應付未來可能發生的民事損賠訴訟。以下將就現行法院判決加以分析。

一、我國現行「電腦處理個人資料保護法」有關民事損害賠償判決之分析

在現行法時代發生之個資外洩事件，以現行法作為請求權基礎之訴訟案，由前述分析可知數量必然十分稀少，自2004年至今約僅有兩百多件，而原告勝訴可據以參酌賠償金額之案件就更顯珍貴了，7年來約僅有9件（詳參表1）。

由此9件案例分析，被告之行業別因現行個資法之限制，不脫離現行法下規範之八大行業，分別為：銀行（2件，1件含員工）、證券商（2件、1件含離職員工）、電信業者（及其員工）、網路書店、徵信業及資訊業者、網購賣家及公務機關。大部分案例引用現行個資法第18條或第28條作為請求權基礎，此兩條文在新法依然存在，僅有賠償額度自每人每事件2萬元以上10萬元以下，修正為500元以上2萬元以下；而同一原因事實合計最高賠償額，則由2,000萬元提高至2億元，如該原因事實所涉利益超過2億元，以該所涉利益為限，是如當事人能證明超過外洩者獲有超過2億元之利益時，其賠償額將會更高。

實際判賠之金額部分，唯一一件公務機關為被告之案件（臺灣臺北地方法院99年度北國簡字第16號判決）遭判賠5,000元，與現行個資法規定下限2萬元不符。由該判決析之，似與原告並未主張法院應適用現行個資法第27條規定作為損害賠償額度審酌之標準有關，並非係參酌新個資法規定降低賠償額度，始作為賠償額度僅有5,000元之決定因素。其他8件賠償案例，賠償金額均自2萬元起跳，除有2萬元、3萬元及8萬元案件各一件以外，有三位被告被判應賠償10萬元，超過10萬元則有13萬7,900元、15萬元、21萬4,500元及25萬元者。

表1　原告勝訴可據以參酌賠償金額之案件

裁判案號	被告行業別	請求權基礎	事實摘要	賠償金額
臺灣高等法院98年度上易字第1229號民事判決	銀行	電腦處理個人資料保護法第18條、第28條、民法第184條第1項前段、第188條第1項、第195條。	原告未曾向被告申請信用卡，然被告於民國97年間誤向聯合徵信中心申報原告持用之信用卡遭強制停卡致原告之名譽、信用受有損害。	25萬元
臺灣板橋地方法院99年度重勞訴字第10號民事判決	證券商離職員工	民法第153條、第199條、第184條第1項前段、營業秘密第12條第1項前段。	被告藉職務上之機會，取得原告未授權被告查閱之客戶資料後離職。	21萬4,500元
臺灣臺南地方法院94年度訴字第121號民事判決	個人、電信業者及其員工	電腦處理個人資料保護法第28條、民法第184條第1項前段、第188條第1項、第195條。	被告甲為利用職務之便，受被告乙之請託擅自進入電腦系統查詢電話使用人即原告之姓名、住址相關資料，並告知被告乙藉以確定原告之身分。	個人：15萬元 電信業者及其員工：8萬元
臺灣臺北地方法院97年度訴字第1683號民事判決	網路書店	民法第184條第1項前段第195條、電腦處理個人資料保護法第28條適用第27條。	原告等於被告網站購買台北金馬影展套票，因被告處理疏失，竟夾帶其餘477位註冊成功之會員資料含會員帳號、姓名、地址、電話、手機、電子信箱資料，外流到其他數百人之信箱之中，無法追回。	13萬7,900元
臺灣臺中地方法院94年度重訴字第196號民事判決	銀行及其員工	電腦處理個人資料保護法第6條及第18條、第28條及民法第188條之規定。	被告甲利用任職被告公司業務之機會，取得原告申辦現金卡之個人資料，進而利用此一資料，冒用原告名義，辦理變更住址及掛失補發現金卡。	10萬元
臺灣臺北地方法院93年度訴字第2455號民事判決	徵信業者、資訊業者	電腦處理個人資料保護法第27、28條規定。	被告乙違法蒐集原告之個人資料，又與被告甲共同意圖營利，提供被告甲之付費會員，得透過網路超連結方式，以每筆資料200元之價格付費查詢。	徵信業者：10萬元 資訊業者：10萬元
臺灣基隆地方法院93年庭訴字第82號民事判決	證券商	電腦處理個人資料保護法第27、28條規定。	未經原告同意蒐集其姓名、地址等資料並發送廣告信函。	3萬元
臺灣宜蘭地方法院羅東簡易庭99年度羅小字第56號民事小額判決	網購賣家	民法第184條第1項前段、第195條。	原告於網拍上購買被告商品，被告於評價留言公開原告家中之系爭家用電話號碼，使原告之家用電話號碼遭第三者知悉。	2萬元
臺灣臺北地方法院簡易庭99年度北國簡字第16號民事判決	公務機關	國家賠償法第5條、民法第195條。	被告將原告之個人資料公布於薪給發放標準之陳情函並予以張貼。	5,000元

資料來源：達文西個資暨高科技法律事務所彙整

對於個資外洩或其他侵害個資權利之人，究應負擔多高之賠償額？實無法從區區9件案例中，獲得清楚的判斷基準。對於侵害個資權利之公務或非公務機關而言，由於賠償金額與外洩事件間之關連性尚難估計，自然會對斥資投入資安產品之意願大為下降，如此又可能導致個資外洩的發生機率，無法達成欲防護個資外洩之立法目的。

二、自由心證主義於個資外洩損害之認定問題

新個資法有關民事損害賠償規定之構成要件，規定於第28條（針對公務機關）：及第29條（針對非公務機關）：「違反本法規定致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利」者。條文規定較現行法更為詳盡，可知個資當事人得據此加以求償之範圍，不僅僅止於個資外洩情形，舉凡違法蒐集、應告知當事人而未告知、應通知而未通知、逾期保存或利用個資、當事人請求更正或刪除卻未為之……等等，均可能符合求償之構成要件。而其他各種違反個資法要件的情狀，如個資外洩、應通知未通知、逾期保存資料等侵害權利之行為，當事人勢將難以證明其實際損害額之多寡，如此皆可適用新個資法第28條第3項規定，由法院以自由心證方式，酌定賠償金額。此時審判者究應如何衡量其損賠金額之高低？判斷標準為何？勢必將成為攻防焦點與審判爭議。

此外，新個資法明定公務機關對於違反個資法的侵害行為採無過失責任；非公務機關違反規定時之責任認定則採舉證責任倒置之設計，只需當事人舉證證明個資係由該非公務機關所侵害，非公務機關即必須舉證證明自己之無過失，否則將被認定為有過失。而非公務機關要如何證明已達「無過失」之情狀，實為極度不確定的法律概念，多數審判者可能皆傾向於有外洩即有過失。法諺有云：「舉證之所在，敗訴之所在」，則當有違反新個資法的情事發生，個資當事人如可證明違反新個資法之行為，係其請求之公務機關或非公務機關所為，且當事人請求法院以自由心證酌定賠償額者，則法官即面臨審查損害賠償額度的過程，不得以當事人無法證明其所受損害額度而駁回原告之訴。

此外，未來若發生大量求償金額之個資訴訟案件，不論個別求償或以團體訴訟方式湧入法院，而當事人又無從證明所受損害，均取決於法官行使自由心證之情形下，如無損害賠償金額基準得以參考，勢將造成審判者承審此類案件時極大不確定性，判決結果及賠償責任也將欠缺可預測性。

因此，為使得未來個資外洩案件發生時，就有關民事損害賠償計算有一相對客觀的標準，藉此於個案中供法院參考，有其迫切的重要性。

三、新個資法民事損害賠償因子之建立

數位時代之下，個資外洩鮮少能夠追回，其外洩之損害亦無從事先預測，如新個資法上路後能促使保有個資單位重視個資保護議題，確實投入心力保障個人資料，才能確實發揮個資法保障與平衡個人資料利用的立法目的。本文建議可考慮制定法院審理得參酌之「個資法民事損害賠償金額酌定參考要點」或類似「辦案手冊」之方式，提供法院審理時得參考之依據。

以下參考現行智慧財產法院所適用之《量刑參考要點》及司法院「性侵案件量刑基準表」為依據，搭配新個人資料保護法條文內容，草擬之「個資事件民事損害賠償基準表」，法院可依據具體個案情形，參考基準表之審理因子，判斷被告之過失責任與損賠額度。期待藉由提供法院參考因子的方式，方便審判時依據個案情狀，行使更細緻的自由心證，不但可改善目前審判者於個資損害事件中欠缺參考基準的缺失，亦有助審理細緻化，對於個資當事人及擁有個資的單位，皆可增加對

判決之可預測性。

表2　個資事件民事損害賠償基準表

違反法條	賠償額度因子	審酌標準	備註
1. 新個資法第3條 （預先約定拋棄或限制以下權利：⑴查詢或請求閱覽⑵請求製給複製本⑶請求補充或更正⑷請求蒐集、處理或利用⑸請求刪除。）	1. 約定拋棄或限制權利行使之期間 2. 侵害權利種類數 3. 個資保有之型態及規模 4. 獲利情況 5. 和解及履行狀況 6. 再次侵害	• 侵害行為時間長短 • 查詢閱覽權、製給複本權、補充更正權、停止處理利用權、刪除權是否均受侵害 • 是否據以營利及其規模 • 獲利高低之具體情形 • 是否和解及其履行情形 • 有無前次個資侵權行為	
2. 新個資法第5條 （個人資料之蒐集、處理、利用⑴未尊重當事人權益及未依誠信原則為之⑵逾越特定目的之必要範圍茲與蒐集之目的無正當合理關連）	1. 未依誠信原則 2. 與蒐集目的關連性 3. 侵害權利狀況 4. 個資蒐集處理利用之型態及規模 5. 獲利情況 6. 和解及履行狀況 7. 再次侵害	• 情節輕重 • 強弱 • 是否違反誠信、逾越範圍及無關連性均構成 • 是否據以營利及其規模 • 獲利高低之具體情形 • 是否和解及其履行情形 • 有無前次個資侵權行為	
3. 新個資法第6條 （無但書情形而蒐集處理利用醫療、基因、性生活、健康檢查及犯罪前科個資）	1. 侵害權利種類數 2. 個資蒐集之型態及規模 3. 獲利情況 4. 和解及履行狀況 5. 再次侵害	• 是否就五項敏感個資均有蒐集 • 是否據以營利及其規模 • 獲利高低之具體情形 • 是否和解及其履行情形 • 有無前次個資侵權行為	
4. 新個資法第8條 （無第2項情形未告知第1項之應告知事項）	1. 侵害權利狀況 2. 個資蒐集之型態及規模 3. 獲利情況 4. 和解及履行狀況 5. 再次侵害	• 是否六項應告知事項均未告知 • 是否據以營利及其規模 • 獲利高低之具體情形 • 是否和解及其履行情形 • 有無前次個資侵權行為	
5. 新個資法第9條 （無第2項情形未告知第1項之應告知事項）	1. 侵害權利狀況 2. 個資蒐集之型態及規模 3. 獲利情況 4. 和解及履行狀況 5. 再次侵害	• 是否六項應告知事項均未告知 • 是否據以營利及其規模 • 獲利高低之具體情形 • 是否和解及其履行情形 • 有無前次個資侵權行為	
6. 新個資法第10條 （無但書情形時未依當事人請求答覆查詢、提供閱覽及製給複製本）	1. 侵害權利狀況 2. 個資保有之型態及規模 3. 獲利情況 4. 和解及履行狀況 5. 再次侵害	• 未依請求答覆查詢提供閱覽及製給複製本之情節輕重 • 是否據以營利及其規模 • 獲利高低之具體情形 • 是否和解及其履行情形 • 有無前次個資侵權行為	
7. 新個資法第11條 （第1項：未維護個人資料之正確，未依當事人請求更正或補充）	1. 侵害權利狀況 2. 個資保有之型態及規模 3. 獲利情況 4. 和解及履行狀況 5. 再次侵害	• 未維護個人資料之正確，未依當事人請求更正或補充之情節輕重 • 是否據以營利及其規模 • 獲利高低之具體情形 • 是否和解及其履行情形 • 有無前次個資侵權行為	

違反法條	賠償額度因子	審酌標準	備註
（第2項：於正確性有爭議時未停止處理或利用；亦未註明爭議或經書面同意）	1. 侵害權利狀況 2. 個資保有之型態及規模 3. 獲利情況 4. 和解及履行狀況 5. 再次侵害	• 未維護個人資料之正確，未依當事人請求更正或補充之情節輕重 • 是否據以營利及其規模 • 獲利高低之具體情形 • 是否和解及其履行情形 • 有無前次個資侵權行為	
（第3項：於特定目的消失或期限屆滿時，於非執行職務必須或經書面同意時，未刪除、停止處理或利用個資）	1. 侵害權利狀況 2. 個資保有之型態及規模 3. 獲利情況 4. 和解及履行狀況 5. 再次侵害	• 保留個資之期間 • 是否據以營利及其規模 • 獲利高低之具體情形 • 是否和解及其履行情形 • 有無前次個資侵權行為	
（第4項：違法蒐集處理利用個資未刪除或停止）	1. 侵害權利狀況 2. 個資保有之型態及規模 3. 獲利情況 4. 和解及履行狀況 5. 再次侵害	• 保留個資之期間、違法蒐集之手段 • 是否據以營利及其規模 • 獲利高低之具體情形 • 是否和解及其履行情形 • 有無前次個資侵權行為	
（第5項：可歸責機關事由而未更正補充個人資料，而未於更正補充後通知曾提供利用之對象	1. 侵害權利狀況 2. 個資保有之型態及規模 3. 獲利情況 4. 和解及履行狀況 5. 再次侵害	• 可歸責之事由重大性、未更正補充資料之期間長短、未通知曾提供利用之對象之期間 • 是否據以營利及其規模 • 獲利高低之具體情形 • 是否和解及其履行情形 • 有無前次個資侵權行為	
8. 新個資法第12條 （違反本法致個人資料被竊取、洩漏、竄改或其他侵害，未於查明後通知當事人）	1. 侵害權利狀況 2. 個資保有之型態及規模 3. 獲利情況 4. 和解及履行狀況 5. 再次侵害	• 未查明違法侵權狀況、未於查明後通知當事人 • 是否據以營利及其規模 • 獲利高低之具體情形 • 是否和解及其履行情形 • 有無前次個資侵權行為	
9. 新個資法第13條 （第1項：就當事人查詢、提供閱覽、製給複製本之請求，未於15日內為准駁之決定又未延長，或延長後仍未於15日內准駁）	1. 侵害權利狀況 2. 個資保有之型態及規模 3. 獲利情況 4. 和解及履行狀況 5. 再次侵害	• 未為准駁之期間長短 • 是否據以營利及其規模 • 獲利高低之具體情形 • 是否和解及其履行情形 • 有無前次個資侵權行為	
（第2項：機關未於30日內就第11條請求為准駁又未延長，或延長後仍未於30日內准駁）	1. 侵害權利狀況 2. 個資保有之型態及規模 3. 獲利情況 4. 和解及履行狀況 5. 再次侵害	• 未為准駁之期間長短 • 是否據以營利及其規模 • 獲利高低之具體情形 • 是否和解及其履行情形 • 有無前次個資侵權行為	
10. 新個資法第15條 （公務機關蒐集處理敏感資料外之個資未具特定目的或不符合第15條第1-3款情形而蒐集處理）	1. 侵害權利狀況 2. 個資蒐集處理之規模 3. 和解及履行狀況 4. 再次侵害	• 未具特定目的蒐集處理、不符合第15條第1-3款情形或兩者兼具 • 個資數量多寡 • 是否和解及其履行情形 • 有無前次個資侵權行為	

違反法條	賠償額度因子	審酌標準	備註
11. 新個資法第16條 類似第5條 （公務機關之個資利用未於執行法定職務必要範圍內為之，不符蒐集特定目的或未符合但書情形卻為特定目的外之利用）	1. 與蒐集目的關連性 2. 侵害權利狀況 3. 個資利用之型態及規模 4. 獲利情況 5. 和解及履行狀況 6. 再次侵害	• 強弱 • 是否未於執行法定職務之必要範圍內為之、逾越特定目的均構成 • 是否據以營利及其規模 • 獲利高低之具體情形 • 是否和解及其履行情形 • 有無前次個資侵權行為	
12. 新個資法第17條 （公務機關未將1-4款事項公開於電腦網站或以其他適當方式供公眾查閱）	1. 侵害權利狀況 2. 個資保有規模 3. 和解及履行狀況 4. 再次侵害	• 未將1-4款事項供公眾查閱之期間長短 • 個資數量多寡 • 是否和解及其履行情形 • 有無前次個資侵權行為	
13. 新個資法第18條 （公務機關未指定專人辦理個資安全維護事項）	1. 侵害權利狀況 2. 個資保有規模 3. 資安維護水準 4. 和解及履行狀況 5. 再次侵害	• 未指定專人辦理個資安全事項之期間長短 • 個資數量多寡 • 是否達到侵權行為時之資安技術一般水準、資安管理流程是否健全、是否符合政府或市場通用之資安保護標準 • 是否和解及其履行情形 • 有無前次個資侵權行為	
14. 新個資法第19條 類似第5條 （第1項：非公務機關蒐集處理敏感資料以外個資未符特定目的或第1-7款規定）	1. 侵害權利狀況 2. 個資蒐集處理之型態及規模 3. 獲利情況 4. 和解及履行狀況 5. 再次侵害	• 蒐集處理個資未符特定目的或1-7款或兩者均未符合 • 是否據以營利及其規模 • 獲利高低之具體情形 • 是否和解及其履行情形 • 有無前次個資侵權行為	
（第2項：當事人依第1項第7款但書規定要求刪除、停止處理利用而未為之）	1. 侵害權利狀況 2. 個資蒐集之型態及規模 3. 獲利情況 4. 和解及履行狀況 5. 再次侵害	• 未刪除、停止處理利用之期間長短 • 是否據以營利及其規模 • 獲利高低之具體情形 • 是否和解及其履行情形 • 有無前次個資侵權行為	
15. 新個資法第20條 類似第5條 （第1項：非公務機關未於特定目的必要範圍內又未符但書情形下，利用敏感資料以外之個資）	1. 個資利用之型態及規模 2. 獲利情況 3. 和解及履行狀況 4. 再次侵害	• 是否據以營利及其規模 • 獲利高低之具體情形 • 是否和解及其履行情形 • 有無前次個資侵權行為	
（第2項：非公務機關依前項規定利用個資行銷者，當事人拒絕接受行銷而未停止）	1. 行銷之型態及規模 2. 行銷之頻率 3. 和解及履行狀況 4. 再次侵害	• 是否據以營利及其規模 • 行銷頻率之高低及期間長短 • 是否和解及其履行情形 • 有無前次個資侵權行為	

違反法條	賠償額度因子	審酌標準	備註
（第3項：非公務機關首次行銷時未提供拒絕接受行銷方式或未支付所需費用）	1. 侵害權利狀況 2. 當事人拒絕行銷所付費用 3. 獲利情況 4. 和解及履行狀況 5. 再次侵害	• 未告知行銷之期間長短 • 實際支出費用高低 • 獲利高低之具體情形 • 是否和解及其履行情形 • 有無前次個資侵權行為	
16. 新個資法第21條 （非公務機關有本條情形受主管機關限制而仍國際傳輸個資者）	1. 國際傳輸之型態及規模 2. 國際傳輸之頻率 3. 獲利情況 4. 和解及履行狀況 5. 再次侵害	• 是否據以營利及其規模 • 傳輸頻率之高低及期間長短 • 獲利高低之具體情形 • 是否和解及其履行情形 • 有無前次個資侵權行為	
17. 新個資法第27條 （第1項：非公務機關未採行適當之安全措施防止個資被竊取、竄改、滅失或洩漏）	1. 個資被竊、竄改、滅失或洩漏之型態及規模 2. 個資外洩之頻率 3. 個資保有之型態及規模 4. 和解及履行狀況 5. 再次侵害	• 個資外洩數量情狀 • 外洩頻率高低及期間長短 • 是否據以營利及其規模 • 是否和解及其履行情形 • 有無前次個資侵權行為	
（第2項：非公務機關未依主管機關之指定訂定個資檔案安全維護計畫或業務終止後個資處理方法）	1. 未訂定計畫或方法之期間 2. 個資外洩之型態及規模 3. 個資外洩之頻率 4. 和解及履行狀況 5. 再次侵害	• 期間長短 • 個資外洩數量情狀 • 外洩頻率高低及期間長短 • 是否和解及其履行情形 • 有無前次個資侵權行為	

上述表格僅就新個資法規定內容，盧列相關的參考因子，提供法院審酌時參考。此外，由於新個資法第29條中對非公務機關之損害賠償責任採舉證責任倒置之設計，非公務機關於個資外洩事件發生時，必須舉證無故意過失始可免責[29]。因此，目前社會各界對於個資保護之遵循規範有迫切需要。

但由於損害賠償與過失責任的認定，涉及法院審判核心，因此上述因子可說是提供一個討論的開端，供各界參考，希望得以藉由民事損賠因子的討論，逐步建立起過失責任與賠償基準。

伍、結論

在即將施行之新個資法中，對於個人資料的保護義務與民事損害賠償責任，相較於現行法皆大幅提高。尤其團體訴訟與高額民事賠償的規定，皆對於公務與非公務機關帶來嚴重衝擊。而在網路時代犯罪日新月異的同時，不論新型態APT（Advanced Persistent Threat）攻擊，亦或是「社交工程」（Social Engineering）犯罪，皆使得公務與非公務機關無法完全防範日新月異的侵害模式。誇張的形容，稍一不慎，任何機關都可能面臨「賠償到流眼淚」的高額損害賠償風險。而在現今欠缺法院審理標準的情況下，建立個資事件民事損害賠償基準，供法院與各界遵循有其迫切需要。

本文希望藉由對新個資法適用個資外洩事件時可能產生之爭議，以及有關民事損害賠償基準的建立，提供各界參考與討論。更期待藉由未來司法實務的經驗累積，能逐步建立起個資保護損害賠償與過失責任之認定標準，共同促進個人資料之合理利用與隱私保障的平衡。

29 個人資料保護法第29條第1項：「非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限」。