

## 第六章 結論與建議

### 第一節 結論

近年來雇主對於電子郵件與電腦網路資源監看之重視，而造成員工因不當使用電子郵件與電腦網路資源而被解僱之比例也往上增加。根據本研究初步探索，原因有三：一、是履行法律的責任，避免成為員工在網路上從事不法活動的共犯或是幫助犯。根據 2007 年美國管理協會與 e 化政策學會之調查發現，由於員工的不當電子郵件內容，造成近 24% 的公司被法庭傳喚，甚至 15% 的公司需要為此面對法律訴訟<sup>1</sup>。二、提高員工的生產力，使員工上班時間不從事與公務無關的事務，一方面保護員工避免觸法，另一方面也可使員工更專注於所應完成之工作，進而提高工作效率。三、是維護企業之電腦系統安全，減少員工不當使用電腦資源與電子郵件而致使企業資訊系統遭到惡意駭客、電腦病毒與木馬入侵之機率。

任何環境只要有兩個以上的人存在，都可能發生法律與管理上的問題。網際網路環境使得企業的法律訴訟與管理問題也開始不斷在網路環境之中發生。雇主監看權與員工隱私權問題也隨之出現。企業經營的立場，是無法承受員工長期的網際網路上遊蕩，無所事事，影響工作效率，或在網路上作出與企業形像不符的事情，例如瀏覽不正的網站內容，或從事不法，使得企業必需負擔法律上的責任。更有甚者，藉由企業的電子郵件傳遞企業內部機密資料，從而造成重大損失，因此在網路監看上與管制電子郵件的內容，有其必要性。對於避免員工在電腦上從事違法行為使企業受到牽連，或避免企業機密遭到竊取而

---

<sup>1</sup> 同註 2。

外洩，企業的監看亦有正當性。

由本研究整體之探討與個案訪談分析後之初步結論，雇主監看員工使用電腦之界限，首先應遵循法律之規範，如本研究於第三章第三節所述之民法、刑法、通訊保障及監察法、電腦處理個人資料保護法等等相關法律對於監看權之限制。否則，縱然員工已簽下「雇主監看同意書」，若違反法律，仍應為無效，而有侵害員工職場隱私之虞。此外人才是雇主的重要資源<sup>2</sup>，雇主應維護員工之人格權，本研究認為雇主或可參考學者Hanau 提出雇主監督員工之人格權是否有不當侵害之界限提出以下之三項觀察標準，而定出適當之工作規則。

1. 員工收發電子郵件係基於職務原因或私人原因所為？
2. 員工電子郵件之收發係受雇主之許可或受雇主之禁止？
3. 員工之收電子郵件係在工作時間之內或工作時間之外？

近年來，隨著社會對於隱私權的重視，也出現對保障職場隱私權之有利的判決，例如 2008 年 6 月在美國舊金山區第九巡迴庭的訴訟案 *Quon v. Arch Wireless Operating Co. Inc.*<sup>3</sup> 之中，法院判定：縱使員工是在上班時間使用雇主之電腦資源，雇主仍不能在不知會員工或不徵得員工同意之情況下，直接監看員工之電子郵件。未來職場雇主的過度監看與職場隱私權維護之訴訟可能仍會繼續出現。從德國的法制規定，對於隱私權法有明確的規定，例如企業應設立類似隱私長的職務，已確保單位中相關的成員，包括顧客、員工、高階管理人之隱私權，值得我國有關企業參考。

本研究在針對管理學之雇主監看權與員工職場隱私權的調和之

---

<sup>2</sup> Burke, Ronald and Cooper, Cary, *The Human Resources Revolution-Why putting people first matters*. Elsevier Press, 2006, pp. 13-14.

<sup>3</sup> *Quon v. Arch Wireless*, 529 F.3d 892 (9th Cir. 2008).

最佳實務分析中，本研究認為企業應充份尊重員工，謹慎地訂定明確之「可接受的使用政策」與「職場員工監看政策」。並盡充份告知員工之義務，避免日後發生糾紛。可以妥當地運用正式與定期的員工教育訓練，給予員工充分之時間發問以促使員工能真正理解。重視與員工的互動，傾聽工的心聲，適時調整「職場員工監看政策」，使之合乎人性化。員工在充滿人性化的職場工作，才會發揮潛能，提高工作效率。



## 第二節 本研究之建議

### 一、對於員工的建議

企業聘僱員工之目的在於借重其能力，時間與團隊合作，以使得企業之任務得以完成。企業支付薪資是期待員工進入企業之後，員工要能為部門與企業作出貢獻，解決問題。員工在上班時間內，理應作好自己的份內之事，解決企業的問題，而非為企業製造問題。特別是職場上競爭激烈，員工應有所體認，應努力發揮所長，不應將寶貴時光浪費在無益甚至是有害的網站上。此外，本研究對於員工還有以下三項建議：

- 1、遵循職場倫理規範：公務部門或是企業工作的員工，自應遵循職場上的倫理規範，不連上違反法律或違反公共秩序善良風俗的網站，與散發違反法律或違反公共秩序善良風俗的電子郵件，例如：暴力或色情的網站與郵件，賭博網站與電郵等等。這些內容不僅擔誤上班時間，破壞企業形像，還兼具敗壞個人的道德操守與社會風氣，實不足取。上班時間員工上網作私人用途，除了占用了上班時間，影響整體員工的上班士氣，更可能會將公司的商業機密傳至競爭者公司的人，傷害公司的利益甚大。員工欲使用網際網路作為私人的用途來運用，建議下班後回自己私人的電腦進行。
- 2、熟悉工作規則：員工除應了解自己與企業所簽定的僱傭契約中了解自己的權利義務，特別是公司對於員工隱私權的政策外，也應熟悉工作職掌與工作規則，了解在自己領域的職場上應遵守的原則，特別是工作規範中對於自己在電腦與電子郵件，應

理解這些都是企業資產，而非私人的資產，因此在使用上應依據工作規範或工作守則的規定，若是以上皆沒有看到有關員工隱私權明確的規範，則也應探詢主管或是人事部門的意見，了解到自己可期待的合理隱私權界限。原則上使用上述企業的資產，自應以企業的利益作為最主要的考量。

- 3、了解可申訴管道：若是發覺企業內有過度的侵害到員工的隱私權時，侵犯或洩露員工私領域的事務時依法可以申訴，討回公道，伸張正義。例如員工申訴委員會，工會組織等等。

## 二、對於雇主的建議

企業內部的人力資源，是企業內最重要的資產，所有的工作都需要員工去共同協力去推動完成。因此對於組織內的每個成員都應尊重，特別是員工的資訊隱私權，不得任意予以刺探，揭露與傳播。以下是對於業主或高階管理者的四項建議：

- 1、明訂隱私權政策：企業在電腦系統與電子郵件上，為防止日後與員工發生侵犯員工隱私權的爭議，應在僱傭契約、工作規範或是企業內部的管理政策中作出明確的規範與宣示，使得每個員工都能清楚了解到企業內部員工有哪些的監控方式，最好能明訂違反規定之懲處，使得員工發生警惕作用，不致於讓員工因有意或無意之中讓企業蒙受損失，並造成員工因為沒有認識而失去工作。
- 2、結合資訊安全之教育訓練：企業平時應將電腦上的隱私權與資訊安全的教育訓練結合一起。由於電腦的資訊安全與公司商業機密與員工隱私權皆很有關聯。若是企業內部的電腦系統遭到

電腦駭客的侵入，無論是企業內部的機密資料與是員工或是顧客的資訊隱私權，皆可能受到嚴重的侵犯，造成非常大的傷害。即使企業的監控權與員工隱私權之間有明確的規範，駭客的木馬與病毒，仍然會造成重大的損失。因此企業內部，應全面建立資訊安全機制，確保企業機密與員工以及顧客隱私權的安全。

- 3、加強隨身碟之控管：目前絕大多數的企業，包括公營或是民營機構，除了少數的例外，對於員工隨身碟或是可重覆讀寫光碟片等可攜性儲存設備的使用，皆缺少有效的控管。而此種可攜式的儲存設備，由於傳播檔案的同時，也容易感染電腦病毒與木馬。只要感染木馬，將造成駭客入侵企業的電腦系統，使得企業的資料或顧客的資料，甚至員工的隱私權，皆無法充分的保障。有必要訂定出可攜式性儲存設備的使用規範。機構可以規定只有使用機構中經過檢驗的加密隨身碟才可以連接在機構中的電腦，使用隨身碟的員工需依規定向單位申請並且登記列管，以減少機密或隱私資料外洩的機率與電腦遭受電腦病毒與木馬侵入的機率。
- 4、重視員工隱私權：企業在制定相關的監看政策時，應注意維持保護企業營業秘密與員工隱私權的平衡，以免造成員工不滿，不利公司長期發展。公司的監看政策必須經過授權的特定人員來監看，監看目的亦必須是為了公司的合法商業利益與公司財產之適當使用。企業若欲以工作規則就電子監看與隱私權保護作事前約定，則應尋求在約定時，就能夠尋求保護企業機密與員工隱私權的平衡，此種態度將可有效降低對員工隱私權的侵害。企業可加強對員工的正式教育訓練，使員工了解無形資

產，特別是營業秘密在現在知識經濟時代的重要性與價值為，以及這些資訊對企業的重要。若任意將企業的營業秘密傳送出去，將會損害企業與員工的整體權益。教育訓練的過程中，應給予員工充分的時間發問，藉由互動，可以調整公司職場隱私權政策，使之更為人性化，更重視人權。在制定相關監看政策時，鼓勵員工的參與，以取得員工對公司政策的認同。

