淺談個人資料保障和網絡入侵法例

法人法語 香港律師會社區關係委員會

大型機構最近接連發生資料外泄事件，再次喚起公眾對資料外泄和網絡安全風險的關注。本文旨在為讀者簡單介紹相關法例和新加坡在有關方面的發展。

根據香港《個人資料（私隱）條例》（《個人資料條例》），資料使用者不得作出違反任何保障資料原則的作為或從事違反任何該等原則的行為。《個人資料條例》訂明六項保障資料原則，包括資料使用者須採取所有切實可行的步驟，以確保由資料使用者持有的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響。

香港法例目前並未強制資料使用者在資料外泄發生後須向個人資料私隱專員公署及受影響人士通報，亦未要求資料使用者收集個人資料時須就資料安全作出任何承諾或擔保。

然而，很多時候資料使用者在資料外泄後自願作出通報，公署收到通報後展開調查，如有需要，公署會發出執行通知要求資料使用者採取公署列明的措施以防資料外泄事件再發生。譬如說，公署過去曾對選舉管理委員會和警務處發出執行通知。

香港法例並未硬性規定資料使用者應如何防止其持有的個人資料外泄和應對網絡入侵。新加坡則於二〇一八年八月三十一日起實施《網絡安全條例》（Cyber Security Act）。《網絡安全條例》訂明，當某機構於新加坡持續提供重要服務，而其資訊系統如受到侵襲會對新加坡造成重大影響，當地的網絡安全專員有權指定該機構為持有重要資訊基礎設施（Critical Information Infrastructure）從而進行監管。這些機構每年須進行網絡安全風險評估，每兩年則要進行稽核。這些機構在發生網絡入侵後必須及時通報。對於網絡安全服務提供者，《網絡安全條例》亦有嚴謹的規範。

THE LAW SOCIETY OF HONG KONG 香港律師會

馮嘉麒
執業律師

香港律師會鄭重聲明，本文內容純屬個人意見，並不代表香港律師會立場。任何人士如因文章所載或漏載的資料而引致任何損失或損害，香港律師會及撰寫文章的律師絕不承擔任何責任。

本文於 2019 年 3 月 4 日(星期一) 於星島日報 (A7) 的「法人法語」專欄刊登