

القوانين و المحاسبة لتطبيق أمن المعلومات

د. خالد بن سليمان الغنبر ❖

جامعة الملك سعود

ksaksu@gmail.com

تخيّل لو لم يكن هناك مراقبة للاختلاسات والتلاعب ولا يوجد قوانين تحد منها أو تعاقب من يخالفها، فهل يتردد المخالف في تنفيذ مخالفته وهو في مأمن من العقوبة. تخيل لو لم يكن هناك قوانين لمتابعة ولعاقبة المدراء على تقصيرهم في متابعة الأمور المالية في إدارتهم، فهل سيبالون بالقصور والتجاوزات المالية؟ مثلما هناك قوانين وأنظمة تجبر المدراء على الاهتمام بالأمور المالية، فإننا نحتاج إلى قوانين تجبر المدراء على الاهتمام بحماية المعلومات من التلّف أو السرقة أو الفقدان.

هناك دوافع عدة لتطبيق مفهوم أمن المعلومات، ولعل من أهمها الخوف من مخالفة القوانين. فبالاستناد لإحدى الدراسات حول هذا الدافع، أوضحت الدراسة أن ٧٦٪ من الشركات غيرت أو طورت من إجراءاتها فيما يختص بأمن المعلومات بسبب تلافي مخالفة أحد القوانين الجديدة في أمريكا.

وحسب علمي فإنه لا يوجد إلى الآن من القوانين هنا في السعودية ما يعاقب متخذي القرار على تجاهلهم تطبيق أمن المعلومات في منظماتهم. ولعلي أتساءل عن ما إذا كان هناك قوانين تحد من تسرب بيانات عملاء البنوك و تعاقب المتقصرين. هل هناك إجراءات موثقة لإتباعها عند حدوث سرقة أو تسرب معلومات؟ هل هناك سياسة محددة في المنظمات للتعامل بسرية مع معلومات الموظفين والعملاء؟ أسئلة كثيرة تحتاج إلى الوقوف عندها، ليس لتحسين أمن المعلومات في المنظمات -فأمن المعلومات وسيلة وليست غاية- ولكن للمحافظة على استمرارية نشاط المنظمة، سواء حكومية و ذلك بتقديم الخدمات للمواطنين، أو منظمات خاصة لتحافظ على الإيرادات والأرباح.

لننقف عند بعض الأمثلة على القوانين الأمريكية التي تحث على تطبيق مفهوم أمن المعلومات مع ذكر قيمة العقوبة:

أولاً: قانون المحاسبة للتأمين الصحي (HIPAA)، القانون يركز على التأمين الصحي والسجلات الصحية، ولكن ما يهمنا هنا أن القانون يجبر المراكز الصحية (كبيرة كانت أو صغيرة) على حماية المعلومات الصحية للمرضى من الفقدان أو التلّف أو اطلاع أشخاص غير مصرح لهم سواء كانت ورقية أو رقمية، وذلك بتحديد سياسات وإجراءات لأمن المعلومات. و عقوبة المخالف تبلغ كحد أعلى \$٢٥٠٠٠٠ وعشرة أعوام في السجن.

ثانياً: قانون (GLBA) مثل (HIPAA) و لكن لحماية معلومات عملاء البنوك والشركات المالية، و عقوبته \$٥٠٠٠٠٠.

ثالثاً: قانون ساربنس اوكسلي (Sarbox)، سُن هذا القانون بعد حوادث تلاعب الشركات مثل فضيحة شركة انرون، و القانون يضع ضوابط أكثر صرامة فيما يختص بالتقارير المالية من حفظ و اطلاع و إتلاف، و عقوبة مخالفته تصل إلى خمسة ملايين دولار و عشرين سنة سجنًا.

رابعاً: قانون ولاية كاليفورنيا لحالة اختراق قواعد البيانات، و لعل هذا القانون أكثرها غرابة، حيث يُلزم القانون أي هيئة حكومية أو شخص أو شركة تعمل في ولاية كاليفورنيا بإبلاغ سكان كاليفورنيا المسجلين فيها عن أي اختراق أو محاولة اختراق حدثت لمعلوماتهم الإلكترونية خلال ٤٨ ساعة. صحيح أن القانون لا يلزم بحماية كاملة لمعلومات العملاء لكن بالنسبة للشركات فإن هذا القانون يلزمهم بطريق غير مباشر بحماية المعلومات، وذلك لأن إهمالهم حماية المعلومات