

قضايا بحثية ٢

الباحث/عبدالسلام العتيبي

الأسبوع الثاني



قضايا بحثية ٢

Data Protection through Governance Framework

إعداد
الباحث/عبدالسلام العتيبي

في العصر الرقمي الحالي، أصبحت البيانات أحد الأصول الأكثر قيمة للمؤسسات والأفراد على حد سواء. من خلال الإنترنت والتكنولوجيا الحديثة، تتدفق كميات ضخمة من المعلومات عبر الشبكات المختلفة يومياً، مما يجعلها هدفاً مستمراً للهجمات والاختراقات. في هذا السياق، تزداد المخاوف المتعلقة بحماية البيانات الشخصية والمهنية، ويزداد الوعي حول ضرورة وضع سياسات وأطر حوكمة قوية لضمان سلامة البيانات وحمايتها من أي تهديدات قد تضر بالأفراد أو المؤسسات.

لكن مع تزايد حجم البيانات وتنوع مصادرها، تواجه العديد من المنظمات تحديات كبيرة في ضمان حماية هذه البيانات. المشكلة الأساسية تكمن في عدم وجود آليات حوكمة فعالة تضمن معالجة البيانات بشكل آمن وتنظيم الوصول إليها وفقاً للسياسات المعتمدة. كما أن معظم المنظمات تفتقر إلى البنية المناسبة لإدارة البيانات وحمايتها من المهاجمين أو حتى من الاستخدام الداخلي غير المشروع.

في كثير من الأحيان، تظهر الثغرات بسبب غياب التنسيق بين مختلف السياسات والإجراءات المتعلقة بحماية البيانات، مما يؤدي إلى تعرض البيانات للمخاطر. في بعض الحالات، قد تفتقر المؤسسات إلى توعية كافية لموظفيها حول أهمية الأمن السيبراني وأساليب حماية البيانات الشخصية، مما يؤدي إلى أخطاء بشرية قد تكون السبب في تسريب أو اختراق البيانات.

علاوة على ذلك، تأتي التحديات المتعلقة بالامتثال للقوانين واللوائح المحلية والدولية، مثل اللائحة العامة لحماية البيانات ((GDPR، التي تفرض على المنظمات الالتزام بشروط صارمة لحماية البيانات الشخصية. في هذا الصدد، تجد المؤسسات نفسها في حاجة ملحة إلى بناء إطار حوكمة يتماشى مع هذه التشريعات، ويضمن أمان المعلومات في جميع مراحلها.

إذاً، تكمن المشكلة الأساسية في الحاجة إلى تطوير أطر حوكمة شاملة وفعالة تتيح للمؤسسات حماية بياناتها، والتأكد من الامتثال للقوانين المتعلقة بحمايتها، وتدريب الموظفين على أساليب الوقاية من المخاطر الأمنية. هذا البحث يهدف إلى استكشاف كيفية تحسين تطبيق هذه الأطر، وكيف يمكن التغلب على التحديات التي تواجهها المنظمات لضمان حماية البيانات في عالم يتزايد فيه الاعتماد على التكنولوجيا بشكل مستمر.

تلخص الأدبيات السابقة مجموعة من الأبحاث والدراسات التي تناولت أطر الحوكمة من زوايا متعددة في حماية البيانات. يتمثل التحدي الرئيسي في تكامل الأطر التنظيمية مع الممارسات اليومية وتجاوز العقبات التي قد تظهر أثناء تطبيق سياسات الحوكمة في المنظمات. الأبحاث تشير إلى الحاجة الملحة لتطوير أدوات وتقنيات جديدة للتصدي للتحديات المستمرة في حماية البيانات، وكذلك التأكيد على أهمية التوعية والتدريب المستمر لجميع الأطراف المعنية.

-أطر الحوكمة وتطبيقاتها في حماية البيانات

تشير الأدبيات إلى أن أطر الحوكمة تمثل الإطار المنظم للمؤسسات لإدارة وحماية البيانات وفقاً للسياسات والقوانين المعتمدة. يُعتبر تقرير "Governance, Risk, and Compliance (GRC)" أحد أبرز الدراسات التي تطرقت إلى كيفية دمج الحوكمة والمخاطر والامتثال في هيكل واحد لحماية البيانات. وقد أظهرت الدراسات أهمية تبني نظام حوكمة شامل يتضمن وضع سياسات وقوانين واضحة تنظم جمع البيانات، تخزينها، معالجتها، ومشاركتها، وبالتالي تعزيز الأمان وتقليل فرص الاختراقات.

-التحديات في تطبيق الحوكمة لحماية البيانات

دراسات مثل تلك التي قام بها **Saxena and Jain (2020)** تناولت التحديات التي تواجهها المؤسسات عند تطبيق أطر الحوكمة في سياق حماية البيانات. أبرز هذه التحديات تتعلق بنقص التنسيق بين الفرق داخل المؤسسات، مما يؤدي إلى عدم تحقيق التكامل بين الأنظمة المختلفة لحماية البيانات. كما يشير العديد من الباحثين إلى أن الغياب عن تدريب الموظفين على الإجراءات الأمنية ورفع الوعي بالمخاطر يمكن أن يؤدي إلى تهديدات تتعلق بالأمن السيبراني.

-الامتثال للقوانين والتشريعات

تعتبر **اللائحة العامة لحماية البيانات (GDPR)** في الاتحاد الأوروبي إحدى القوانين المحورية التي طرحت العديد من الدراسات حول كيفية تكامل هذه القوانين مع أطر الحوكمة المؤسسية. أظهرت الأدبيات المتعلقة بـ **GDPR** أهمية وضع أنظمة قوية لضمان الامتثال وتحديد المسؤوليات داخل المؤسسات بشكل دقيق، بالإضافة إلى التأكيد على ضرورة تبني ممارسات مثل تشفير البيانات وتحديد صلاحيات الوصول. مثلاً، دراسة **Kuner (2017)** حول "حماية البيانات في ظل لوائح **GDPR**" أشارت إلى دور الحوكمة في تحسين الامتثال للحقوق الرقمية للأفراد وحمايتهم.

- إدارة المخاطر وحماية البيانات

تعتبر إدارة المخاطر جزءاً لا يتجزأ من أطر الحوكمة التي تهدف إلى حماية البيانات. في العديد من الأدبيات، مثل **ISO/IEC 27001** التي تتعلق بإدارة أمن المعلومات، يُسلط الضوء على ضرورة وجود خطة متكاملة لإدارة المخاطر وحمايتها من التهديدات المحتملة. تشير دراسات مثل تلك التي قدمها **Stoneburner et al. (2002)** إلى كيفية تحليل المخاطر المرتبطة بالبيانات واستخدام نماذج الحوكمة لتقليل تلك المخاطر.

-التهديدات السيبرانية وتأثيرها على حماية البيانات

تتناول العديد من الدراسات تأثير التهديدات السيبرانية مثل الهجمات الإلكترونية، والبرمجيات الخبيثة، والتسريب الداخلي على أطر الحوكمة لحماية البيانات. تشير دراسة **Peltier (2016)** إلى أهمية تبني استراتيجيات أمنية شاملة للتصدي لهذه التهديدات، والتي تشمل التحقق من الهوية، إدارة صلاحيات الوصول، وأدوات التشفير.

- التقنيات الحديثة وتأثيرها على حماية البيانات

أظهرت الأدبيات الحديثة، مثل دراسات **Zhou et al. (2020)**، أن التقنيات الحديثة مثل الذكاء الاصطناعي والحوسبة السحابية قد تساهم في تعزيز آليات حماية البيانات، ولكنها أيضاً تثير قضايا جديدة تتعلق بالأمن السيبراني. كما أن تطبيق تقنيات مثل **Blockchain** قد يساهم في تحسين حماية البيانات وضمان شفافية التعاملات الإلكترونية.

-التوعية والتدريب في إطار الحوكمة

تشير العديد من الأدبيات إلى أن غياب التوعية الأمنية من أكبر العوامل التي تزيد من ضعف حماية البيانات. دراسات مثل تلك التي أجراها **Münch (2019)** أكدت أن التدريب المنتظم للموظفين على أهمية حماية البيانات وأساليب الوقاية من الهجمات يعد عاملاً حاسماً في نجاح تطبيق أطر الحوكمة بشكل فعال.



Thank You