استخدام الوسائل التقنية والقانونية في حماية قواعد البيانات

أ.م.د. طالب محمد جواد عباس*

المُستلخص

إن انتشار انظمة الحاسوب الرخيصة والقادرة على الخزن، أدت إلى جمع كميات غير مسبوقة من البيانات من قبل المؤسسات من جميع جوانب الحياة اليومية. وأن هذا الجمع بطريقة ذكية في ملفٍ ورقي أو حاسوبي والوسيلة المُتقدمة لمعالجتها أيضاً، يسمى قاعدة البيانات بالمعنى الواسع. قواعد البيانات تلعب دورا مهماً في تطوير سوق المعلومات ومنتجاتها. وهناك عدد كبير من قواعد البيانات المتاحة على شبكة الإنترنت من شركات منتجه عديده و التي تجد سوقاً متزايداً في طلبها، وهي تسعى إلى الحصول على مكافأة جهودهم الفكرية والمهارية في بناء قواعد البيانات و بالتالي، فأن رغبتهم في تقييد النسخ من قواعد البيانات في حين أن المستخدمين حريصون على الاستفادة إما دون دفع ثمن ذلك أو الرغبة في الحصول على نسخ الحقوق بكلفة قليلة نسبياً هو المحور الرئيسي في حماية قواعد البيانات.

هذا البحث يقدم نموذجاً جديداً للتفكير في حقوق الملكية غير الملموسة من خلال التعامل مع التوجهات الحالية في ضرورة حماية منتجات المعلومات مثل قواعد البيانات وبدون التفريط في هذه الحقوق. هذا البحث سيتناول نوعين من الحماية وهي: الحماية التقنية والحماية القانونية.

الكلمات المفتاحية : قاعدة البيانات، حماية التقنية، حماية قانونية، حماية حقوق المؤلف

.

*جامعة النهرين/كلية هندسة المعلومات

المُقدمة

لم يعُد بإستطاعت مُتخذ القرار أن يتوصل إلى إتخاذ القرار المُناسب بدون أن تتوافر لديهِ جميع البيانات اللازمة لإتخاذ هذا القرار وتَحَمُّلْ المسؤولية الناشئة عنهُ، فإزدادت الملفات والوثائق وزادت مُشكلة حفظها وتبويبها هذا فضلاً عن إخفاق مُتخذ القرار في تحليل جميع البيانات التي ولو كان يعرفها، إلا إنهُ يتعذر عليهِ استخلاص النتائج منها بغية الحصول على المعلومات التنظيمية في مكانٍ واحد. ونتيجةً لإزدياد البيانات كمّاً ونوعاً لذا احتاجَ المُحلل إلى مُعالجتها حاسوبياً فأصبحت البيانات المُعالجة (معلومات) (Information) والمعلومات شيء والبيانات شيء آخر، كما استطاعت أجهزة الحاسوب أن تحّل مشاكل خزن البيانات وجمعها وتحليلها واسترجاعها بدقائق معدودة إن لم نقُلْ بمُدة أقصر منها.

ولما كانت عمليات خزن البيانات ومُعالجتها واسترجاعها تتم حاسوبياً، لذا اضطرَ الإنسان إلى تصميم قواعد بيانات لمُعالجة هذهِ العمليات الحسابية المُعقدة. وهذهِ القواعد لا تخلو أن تكون إما: ان تكون مُصممة من قِبَلْ شركات مُختصة للتعامل مع مُختلف أنواع البيانات ومُعالجتها مُعالجة حاسوبية أو أن تكون: مُصممة من قِبَلْ المُستفيد نفسه لأغراض معالجة بياناتهِ معالجة حاسوبية خاصة بهِ أو بشركتهِ.

وأيّاً كان المُصمم لهذهِ القواعد فإنَ الاعتداء عليها بدأ يزداد لأسبابٍ شتى منها على سبيل المثال تصفية الخصوم السياسيين أو مُنافسة التجار أو الصناعيين مُنافسة غير مشروعة أو سرقة مُحتوياتها آو معرفة أسرار الحسابات المصرفية والودائع المالية التي يقوم العُملاء بإيداعها في المصارف.

لقد قسم البحث إلى محورين تناول **الأول** حماية التقنية لقواعد البيانات، و**الثاني**، وسائل الحماية القانونية لقاعدة البيانات وموقف المُشرّع العراقيّ منها، ثم نعقبها بكلمة ختامية تجمع الافكار والعبر والاستنتاجات.

أولاً:- الحماية التقنية لقواعد البيانات

المعلومات مورد لا يقل ولا ينضب، تتزايد دوما ولا تتناقص بالاستخدام أو تستهلك، وترتبط بالزمان والمكان وتتفاعل مع التطور، وعلى متلقيها ومدى علاقتها بحاجته تتوقف، إلى حد كبير قيمتها. وهي في الحقبة المعاصرة مفتاح للموارد الأخرى، و خدمة تباع وتشترى، ومصدر قوة اقتصادية وسياسية لمن يحسن جمعها وتنسيقها واستخدامها. المعلومات مصطلح واسع يستخدم لعدة معانٍ حسب سياق الحديث، وهو بشكل عام يرتبط بمصطلحات مثل: المعنى والمعرفة والتعليمات والتواصل[1]. وليس من شكّ في أن المعلومات (البيانات) هي بضاعة العصر الرّائجة ومادتها الخام، ولكن كيف يمكن معالجة الكثير من هذه البيانات؟ كيف يمكن تخزين كل ذلك، وبعد ذلك يسترجعُ بسَـــــــــرّعة فقط الحقائق التي يريدون صناع القرار أن يعرفوا وفي الوقت الذي يريدون أن يعرفوا ذلك؟ الجواب هو إنهم يستخدمون **قواعد البيانات**[2]. ومن أجل هذا أصبحت قاعدة البيانات تمثل قطاعاً مهماً من قطاعات صناعة المعلومات وبالتالي ذات أهمية كبرى في الاقتصاديات الوطنية الأمر الذي يؤهلها لأن تصبح موضوع مهماً من مواضيع الحماية المدنية والتقنية. سنتناول في هذا الجزء تعريف قواعد البيانات (**المعلومات**) وأهميتها ونماذجها، مع عرض لمفهوم طرق الحماية التقنية.

1-1 تعريف قواعد المعلومات وبيان أهميتها ونماذجها

ازدادت معرفةأهمية تقنية قاعدة البيانات وتطبيقاتها يوماً بعد يوم.**وأصبحت القواعد تستخدم في كل مكان**: أنهاالعقل الأساسي للتجارة الإلكترونية وغيرها من التطبيقات **المستندة إلى** الويب.**وتكمن** في كونها **اداة من ادوات العمل التجاري واداء العمل في كل شركة وعلى نطاق واسع** وللتطبيقات التنفيذية **ودعم**

اتخاذ القرارات.قاعدة بيانات تستخدم أيضاً من قبل الآلاف من مجموعات العمل والملايين من الأفراد. وتقديرات لعدد قواعد البيانات النشطة في العالم اليوم يتجاوز 10مليون[3]. وتعرف قاعدة البيانات على إنها مجموعة من البيانات الدائمة أو المتواصلة(Persistent Data) التي تستخدم من قبل النظم التطبيقية لبعض المشاريع (مثل:المشاريع التجارية، العلمية، الفنية، أو أخرى)، وهنا يجب أن لا يفهم حقيقة أنها دائمة لمدة طويلة جداً، بل القصد دائمة مقارنة بالبيانات الأخرى الزائلة مثل، البيانات الداخلة، الخارجة، جمل السيطرة في برنامج، والنتائج العرضية من تنفيذ البرنامج. هذه الفكرة من الديمومة لهذا الحد تسمح لإعطاء تعريف دقيق لقاعدة البيانات[4].

ويمكن النظر إلى قاعدة البيانات من الجانب التقني كمجموعة تحتية منظمة لملفات و برامج تديرها تقنيات حاسوبية؛ ولذلك فمصطلح قاعدة البيانات لم يعد يدل على ملفات المعلومات اليدوية فقط بل أصبح معناه مرتبطاً باستعمالات الحاسوب ويشمل ذلك الدعامات المادية الحديثة لتخزين البيانات وكذلك استعمال الوسائط المتعددة كالأقراص المدمجة. ومن الممكن لصورة فوتوغرافية أن تشكل قاعدة بيانات بذاتها إذا كانت مخزنة بطريقة مرتبة ومنظمة ويمكن استرجاعها بواسطة جهاز حاسوب[5]. ويمكن النظر إلى قاعدة البيانات أيضاً من الجانبين التقني والقانوني على انها تشكل مصنفاً معلوماتياً مركباً . اذ تمتزج البيانات المستخدمة في قاعدة البيانات بالجانب القانوني بما تتضمنه من قوة أضفاء حكم المصنف التقني والحماية المقررة له على مجموع محتويات القاعدة (أي بياناتها) . أما البعد التقني فيتضمن برمجيات تسهل عملية الإخراج النهائي لمحتويات القاعدة[6].

وقد قام (ديت C. J. Date)، بعرض تصور مبسط لنظام قاعدة البيانات (System Database)، والذي يحتوي العناصر الثلاث التالية: (1) قاعدة البيانات المتكاملة (2) برامج التطبيقات (3) المستفيدون النهائيون الذين يتعاملون مع قاعدة البيانات من خلال الوحدات الطرفية البعيدة لتنفيذ العمليات التالية: (1) الاسترجاع (2) التحديث (3) الأدراج أو الإدخال (4) الحذف، وتعتبر عملية الاسترجاع هي أكثر العمليات شيوعا[7]. قواعد البيانات تستخدم من قبل تطبيقات مختلفة ولإغراض متعددة، وهناك تقسيم رباعي لنظام قاعدة البيانات، والذي يتضمن المكونات التالية[8]: المستفيدون، تطبيقات قاعدة البيانات، نظام إدارة قاعدة البيانات، وقاعدة البيانات. إن الفارق بين التقسيم الأول والثاني هو أن (ديت C. J. Date) دمج قاعدة البيانات وإدارتها في مكون واحد سماه قاعدة البيانات المتكاملة.

أما نظم إدارة قواعد البيانات ((Database Management Systems(DBMS)، فهي تلك البرامج التي تجعل من الممكن للمستفيدين لإدارة البيانات وتحقيق زيادة معدل الإنتاجية والوصول والإدامة والمعالجة تتم من خلالها.

هناك أربع طرق مختلفة لتمثيل وخزن المعلومات منطقياً على شكل قاعدة بيانات. ويشار لهذه الطرق المختلفة كنماذج (Models)، وهذه النماذج هي: (1) الهرمية (2) الشبكية (3) العلائقية (4) الكيانية أو الشيئية. النماذج الهرمية والشبكية كانت الاولى تستعمل لتطوير قاعدة البيانات. اليوم، على اية حال، أكثر المؤسسات تستعمل النماذج العلائقية لتصميم قاعدة البيانات.

يستخدم النموذج الهرمي العلاقات واحد-إلى-العديد (One-to-Many) ويعرض البيانات إلى المستفيدين بتركيب يشبة الشجرة. وقد تم تطويرهذا النموذج الهرمي في ستينات القرن الماضي لإدارة كميات كبيرة من البيانات لمشاريع التصنيع المعقدة.

تم إنشاءالنموذج الشبكيلتمثيل علاقات البيانات المعقدة بصورة أكثر فعالية من النموذج الهرمي، ومن أجل تحسين أداء قاعدة البيانات، وفرض معيارقاعدة البيانات. ولهذا فأن البيانات منطقياً تكون على

نحو مختلف بعلاقات العديد-إلى-العديد (Many-to-Many)، وكمثال على هذا النوع من العلاقات هي علاقة الطالب مع الدروس (Student-Course).

عرض E. F.Codd النموذج العلائقي في احدى بحوثه عام 1970. حيث يتم تمثيل البيانات في قاعدة البيانات في النموذج كجداول بسيطة ذات بعدين تدعى علاقة (Relation). ونتيجة عدم تناسب نظم ادارة قواعد البيانات التقليدية السابقة الذكر للتعامل مع التطبيقات المستنده على الرسوم والوسائط المتعددة (الصوت والصورة)، اخذت التوجهات الحالية والمستقبلية إلى نظم ادارة قواعد البيانات الكيانية التي تتمحور حول الكيان (Object) المتضمن خزنه للبيانات والاجراءات الذي يمكن المشاركة واسترجاع البيانات طوعياً أو آلياً من هذا الكيان، أي أن الكيان يحتوي البيانات والدوال أو الطرق (Functions or Methods) التي تعمل عليها[9]. كما انه أمن من الاستعمال غير المخول للبيانات من خلال ما يوفره لثلاثة انواع من الوصول هي: خاص، وعام، ومحمي.

Object-Oriented Databases Management Systems(OODBMs)))

2-1 وسائل الحماية التقنية لقواعد المعلومات

كلما كبر حجم البيانات وازداد عدد المستفيدين وازدادت البيانات المشتركة بينهم كلما استدعى الآمر إلى زيادة إجراءات الحماية القانونية (المدنية والجنائية) والتقنية على قاعدة البيانات وتكون درجتها بقدر قيمتها، وإن حماية البيانات أكثر أهمية من حماية الحاسوب لانها متاحة للقراءة من قبل الانسان. فقد كان من الضروري وضع نظام تقني يمنع المزورين و خاصة منهم المحترفين أمثال الهاكرز من خرق أنظمة الدخول للقواعد و استشارتها بطرق غير مشروعة، هذاالنظام المقرر لحماية قواعد البيانات لا يعطل التشغيل العادي للمعدات الإلكترونية و تطورهاالتقني، لذا يمكن تعريف حماية التقنية لقواعد البيانات: بأنها حماية البيانات ضد التدمير المتعمد أو غير المتعمد أو التعديل غير المخول باستخدام وسائل تقنية موجهة في الإطار العادي لعملها إلى منع أو تحديد التصرفات غير المرخص بها التي تقع على قاعدة البيانات.

وتعرف الحماية بأنها الحفاظ على حق مشغل القاعدة (أو مديرها) في مواجهةِ الاعتداء على بيانات القاعدة وتجريم فاعلها. وقد تتمثل هذه الحماية القانونية في الحماية الجنائية عندما ترى الهيئة الاجتماعية ضرورة تجريم وعقوبة المعتدي على بيانات القاعدة. كما يمكن تصور حماية بيانات القاعدة حماية تقنية باتباع وسيلة تكنولوجية مثل كلمة المرور. وهناك مجموعة من النقاط التي تؤخذ بنظر الاعتبار في مجال الحماية أياً كان نوعها ، ومنها وبشكل عام:(1) اعتبارات قانونية: فمثلاً، هل للمستفيد الحق القانوني بأستخدام عملية معينة على بيانات القاعدة. (2) السيطرة المادية، مثل حماية المكان الموجود فيها الحاسوب باستخدام الأقفال أو أي نوع آخر من الحماية التقنية. (3) سياسة الاستفسارات، مثلاً من تخول له الشركة الصلاحية بأستخدام أي عنصر من البيانات المخزونة أو المعالجة ضمن قاعدة البيانات. (4) مشاكل تشغيلية، مثل حالة استخدام كلمات المرور أو كيفية الحفاظ على سَـــــــرّية هذه الكلمات. (5) السيطرة بأستخدام المكونات المادية، مثل هل يمكن لوحدة المعالجة المركزية CPU أن تقدم أي نوع من الحماية لمواقع الخزن؟ (6) إجراءات الحماية من قبل نظام التشغيل، هل يقدم نظام التشغيل أي نوع آخر من الحماية للبيانات مثلاً هل تخول المستخدم أن يمحي محتويات الذاكرة أو مواقع الخزن أو ملفات البيانات حال الانتهاء منها. (7) إعمال تتعلق بنظام إدارة قواعد البيانات.

وهناك ستراتيجيات ووسائل وأساليب حماية عديدة ومتنوعة تستخدم لحماية البيانات المخزنة في قواعد البيانات وتتمثل هذه الوسائل في مجموعة من الرموز السَـــــــرّية أو أرقام سَـــــــرّية أو مكونات مادية أو برمجيات وتستخدم بشكل منفرداً أو مجتمعة اعتماداً على درجة أهمية البيانات المخزونة في قاعدة البيانات. وسيتم الحديث اولاً عن ثلاث استراتيجيات لحماية قواعد البيانات، ثم لاحقاً في الجزء الثاني سيتم التطرق عن الحماية المستندة على البرمجيات، بعد ذلك في الجزء الثالث سنتحدث عن الحماية

المستندة على المكونات المادية، ونختم مبحثنا بالجزء **الرابع** إذ يعرض لضرورة حمايةالوسائل التقنيةفي حمايةقواعدالبيانات.

1-2-1 ستراتيجيات حماية قواعد البيانات

أنَّ مستوى الحماية لقاعدة البيانات قد تأخذ اشكالاً متعددة، تبدأ من مجموعة الملفات الكاملة إلى ادنى مستوى مع قيمة بيانية محددة ضمن جدول معين في سطر (row) معين ضمن عمود (column) معين. ولكلّ مستفيد صلاحيات وصول (access rights) أو تخويلات (authorities) مختلفة لعناصر البيانات (data objects) المختلفة مثل لمستفيد معين صلاحية استعراض لملف معين وله صلاحية استعراض وتحديث لملف آخر، وبنفس الوقت لمجموعة من المستفيدين صلاحيات مختلفة لنفس عنصر البيانات. وأن ادارة وتنظيم وتنفيذ هذه الصلاحيات والتخويلات هي من صميم واجبات نظام ادارة قواعد البيانات (DBMS)، حيث يقوم بخزن هذه الصلاحيات ضمن الدليل (catalog) في صيغة تحديد الصلاحيات، بعد أن يتم القرار عليها من قبل المشرف العام على قاعدة البيانات ضمن المؤسسة وليس لها علاقة بالجوانب العلمية أو الفنية، وليست من واجبات نظام ادارة قاعدة البيانات. **وتتم إجراءات الحماية من خلال ثلاث استراتيجيات[10][11]، هي :**

الأولى : العزل (Isolation): ويقصد بذلك تخزين البيانات في موقع محمي بحيث لا يمكن، للأشخاص الذين لا يملكون صلاحية للدخول إليه، والوصول إلى هذه البيانات. وتتطلب استراتيجية العزل تحديد الأشخاص الذين يحق لهم الوصول إلى البيانات المعزولة.

الثانية : التنظيم (Regulation): تتضمن هذه الاستراتيجية مراحل ثلاث، هي :

- التعريف (Identification): تحديد الأشخاص الذين يمكن أن يصلوا إلى قاعدة البيانات من خلال كلمات السَـــــــرّ أو استخدام رموز أو بطاقات ممغنطة أو مفاتيح أو غير ذلك. وتعتمد هذه الطريقة على المقارنة بين كلمة المرور المدخلة مع كلمة المرور الاصلية المخزونة بالحاسوب والتي يجب أن تبقى سَـــــــرّية ومحفوظة بالذاكرة (لاهمية كلمات المرور سيتم لاحقاً شرح طبيعة وضوابط استخدامها). ونحن نشير بملاحظة عابرة إلى أن غيرها من تقنيات التحقق (Authentication) متوفرة الآن والتي هي أكثر تعقيداً من مجرد فحص كلمة السَـــــــرّ وهي تتضمن مجموعة متنوعة من الوسائل البيومترية: قراءة بصمة الإصبع وماسحات شبكية العين، مصورات هندسة اليد، المدقق الصوتي، مميزات التوقيع وهكذا. مثل هذه الوسائل يمكن أن تستعمل بفعالية في جميع هذه الأجهزة وأن تستعمل للتحقق من الصفات الشخصية التي لا أحد يستطيع أن يسَـــــــرّقها.
- إعطاء الصلاحيات (Authorization): للاستزادة على ما ورد ذكرهُ أنفاً، يتم خلال هذه المرحلة تحديد صلاحية كل مستخدم للوصول إلى ملف أو مجموعة ملفات وتحديد طبيعة استخدامه لهذه البيانات: قراءة فقط، قراءة وتعديل، حذف وغيرها، وبذلك يتم تقييد صلاحيات المستخدمين وتمكينهم فقط من الوصول إلى مجموعات محددة من البيانات. كما يتم تحديد نوع العمليات التي يمكن أن يقوموا بها باستخدام هذه البيانات: قراءتها فقط أو تعديلها، أو حذفها، أو غير ذلك.
- الرقابة (Monitoring): وتتضمن هذه المرحلة تسجيل جميع عمليات الدخول إلى قاعدة البيانات واستخدام بياناتها، ويجب فحص هذه السجلات بصورة دورية لضبط عمليات الوصول ومنع محاولات الدخول غير المشروع أو الاستخدام غير المصرح به للبيانات.

الثالثة : التشفير (Encryption): وهي أفضل طرق الحماية، وتتم من خلال هذه الاستراتيجية إعادة ترميز البيانات وفق تشفير معين (عملية تحويل النص الواضح إلى مشفر)، بحيث لا يمكن فهمها الا اذا أعيدت صياغتها وفق هذه التشفيرة التي تكون عادة في منتهى السَـــــــــرّية.والنهج الأفضل لتشفير البيانات قاعدة البيانات هو أن نستخدم المكونات أو التطبيقات لتشفير البيانات قبل إرسالها إلىبيئة قاعدة البيانات للتخزين ومن ثم استخدام مكونات مماثلة أو التطبيقات على فك تشفير البيانات بعداسترجاعها من بيئة قاعدة البيانات. ونظرًا لأن عملية التشفير مكلفة و تتطلب وقتاً وجهداً، فإنها تستخدم عادة في الحالات التي تكون فيها البيانات حساسة جداً, وتمثل موضوعات في غاية الأهمية.

وسنحاول في السطور التالية بيان رأينا في الاستراتيجيات الثلاث التي تم شرحها. فنحن نعتقد أن الاستراتيجية الأولى وهي العزل، يتطلب نجاحها بشكل فاعل بوضع آلية أو إجراءات تحدد حماية وضمان أمن وسلامة قاعدة البيانات. وهذه الإجراءات قد تتضمن على سبيل المثال: إدارة وصول المستخدم، تعريفه إلى قاعدة البيانات، وتعيين كلمة مرور له والامتيازات التي يستطيع أن يحصل عليها من قاعدة البيانات (حدود وطبيعة البيانات). كما نلاحظ أن الاستراتيجية الثانية هي أوسع من الأولى بمراحلها الثلاث والتي نعتقد أنها قادره أن تحد من التجاوزات وتوفر الحماية المناسبة وذلك بالتنوع التقني المستخدم والتي تظهره المرحلة الأولى، كما لتمييز المرحلة الثانية بالإجراءات الإدارية في منح الصلاحيات للمستخدمين للوصول إلى قاعدة البيانات بضوابط محكمة ومقيدة، واعتقد ستكون أفضل لو أضيف لها وقت بداية ونهاية (فترة زمنية) لكل صلاحية إي إلا تكون دائمية، وأن لا تكون الصلاحية قابلة للتوارث (إي أنَ المخول غير قادر على منحها لغيره). كما نود أن نضيف أنَّ تنفيذ المرحلة الثالثة من الاستراتيجية الثانية، يتم بمساعدة عدة حزم لنظم إدارة قواعد البيانات تحتوي على ميزاتتسمحمن **احتواء سجل التدقيق**، الذي يسجل تلقائيا وصفا موجزا لعمليات قاعدة البيانات التي يقوم بهاجميع المستخدمين. هذه المراجعة تمكن مدير قاعدة البيانات من تحديد مسارات انتهاكات الوصول. إما الاستراتيجية الثالثة، فهي صراحة أفضل طرق الحماية ويجب أن يفهم المستفيد أن التشفير هو ليس حل لجميع مشاكل الحماية، حيث إذا لم يستخدم بشكل مناسب قد يؤثر على الأداء.

مع تعدد استراتيجيات الحماية وتنوعها مابين الشاملة والمحددة، نود أن نُبيّنَ بعض معايير الحماية والملاحظات المفيدة عليها:

1. اختيار لإستراتيجية معينة يعتمد على نوع التطبيق وتحقيقها لأهداف مالك قاعدة البيانات وعلى **النحو التالي**: (أ) السماح للأشخاص المرخص لهم باستخدام قاعدة البيانات كاملة (ب) **لمنع** الأشخاص غير المخولين من استخدامها (ج) **لمنع المنافس**ين من نسخها من أجل خلق منتج **تنافسي**.
2. يمكن دمج أو استخدام أكثر من إستراتيجية واحدة.
3. لا يجب أن تكون الإستراتيجية المختارة طارده لمستخدمي قاعدة البيانات من خلال إجراءات الحماية المبالغ فيها.
4. في حالة استخدام الإستراتيجية الثالثة (التشفير) يتعين فهم ثلاثة أمور: كيف يعمل التشفير، وكيفية تدفق البيانات في التطبيق، وكيفية حماية انسجام قاعدة البيانات مع السياسة الأمنية الشاملة في **المؤسسة. كما من الضروري ملاحظة قواعد وأس استخدام كلمات السَـــــــرّ أو المرور والتي** سيتم الحديث عنها لاحقاً.
5. **عندما تكون قاعدة ال**بيانات موزعة وليست مركزية، فمن الضروري أن نضمن ليس فقط أن البيانات في قاعدة البيانات محمية، بل رابط الاتصال بين المستخدمين وبياناتهم وبين مكونات الاتصال هي الأخرى آمنة لبيئة قاعدة البيانات الموزعة.

6. اعتماد أكثر من مستوى لتقنيات التحقق والتي تم الإشارة إليها أنفاً.
7. معالجة انقطاع الطاقة وتعطل الحاسوب من خلال استخدام منظم ومجهز الطاقة (UPS).
8. إنشاء وتحديث واختبار النسخ الاحتياطية للبيانات بشكل دوري ووفق طبيعتها وخطط لاستردادها.
9. تركيب أو تثبيت برامج مكافحة الفيروسات والتجسس.
10. توعيةالمستخدمين بالنتائج الضارة لهجمات الهندسة الاجتماعية والتي تُعَّرف على إنها: (عبارة عن مجموعة من التقنيات المستخدمة لجعل الناس يقومون بعمل ما أو يفضون بمعلومات سَـــــــرّية).

2-2-1 حماية قواعد البيانات المستندة على البرمجيات

تعتبرُ **كلمات السَـــــــرْ أو المرور** هي الأكثر شيوعاً في حماية التطبيقات العملية لقواعد البيانات. وقواعد البيانات المختلفة التي تتعامل بكلمات سَـــــــرْ مختلفة ومع مستويات مختلفة من السلامة. في السطور الآتية سيتم وصف بعض كلمات المرور المتداولة التي يجـب أن ينظر فيها عند بناء حماية كفوءة لقاعدة البيانات[12].

1. قواعد بيانات ذات كلمة مرور مفردة أو أحادية (Single – Password Databases). توفر وصول كامل إلى قاعدة البيانات، وإذا علم شخص غير مخوّل أو سيء بكلمة السَـــــــرْ حينئذ يتمكن من خلال ذلك الدخول إلى قاعدة البيانات. وأيضا يعني أن الجميع سيشتركون في أفشاء كلمة السَـــرّ . وهذا يعني أن أي تغيير في البيانات من الصعوبة تحديد الشخص الذي قام به.
2. قواعد بيانات ذات كلمات سَـــــــرْ فردية أو مستقلة (Individual Passwords). قواعد البيانات الأكثر تطوراً تعطي لكل مستعمل كلمة مرور منفصلة، وهذه لها فوائد متميزة على الأسلوب السابق. فإذا كانت قاعدة البيانات تسجّل النشاطات، فمن الممكن ان تخبرنا من قام به ومتى حصل ذلك النشاط.
3. كلمات السَـــــــرْ لنظام التشغيل . بعض قواعد البيانات لا تدير كلمات السَـــــــرْ بطريقة حسنة جداً. فبعض نظم التشغيل لا تستعمل التشفير الا قليلا أو حتى أحياناً بدونه، ولا يفرضوا المعايير القياسية لها (يختارون كلمات سَـــــــرْ قريبة منهم أو ضعيفة مثل:"12345" أو " كلمة سَـــــــرّ")، وهذا ما يسهل للمخترق بأن يصل بثواني قليلة إليها. لذا فان الحاجة إلى تكامل أمن قاعدة البيانات مع نظام الحماية لنظام التشغيل الذي عادة ما يكون متاحاً، فمن الضروري الأخذ بهذا الاتجاه . وذلك لصعوبة قيام المخترق من الوصول إلى سجلات نظام التشغيل والاطلاع على كلمات السَـــــــرْ.

ويعتبر التقاط كلمات سَـــــــرْ جيده شيْ من الفنَ. لذا تَمَيُّز كلمات السَـــــــرْ بالغموض ستكون مانعاً حصيناً لقدرة التخمين لدى اللصوص (الهاكرز)، والعديد من المؤسسات تلزم العاملين فيها ببعض الضوابط في خلق كلمات السَـــــــرْ، ويسبقها قليل من التدريب المناسب لفهم كيفية اختيار كلمة السَـــــــرْ الجيدة.

إن قواعد البيانات قد تكون **مركزية أو موزعة**، وتوجد القواعد المركزية في مكان واحد، بينما تتوزع البيانات المكونة للقواعد الموزعة على أجهزة حواسيب مختلفة تكون متصلة بشبكة حاسوبية. ولكل موقع على الشبكة إمكانية المعالجة المستقلة، وإمكانية تشغيل التطبيقات المحلية، ويشارك كل موقع في تنفيذ تطبيق مشترك واحد على الأقل. إن الحماية في قواعد البيانات الموزعة تكون أقل تحققاً، حيث أن شبكات

الاتصال بصفة عامة تمثل نقطة ضعف واختراق، مما يتطلب الحاجة إلى إجراءات حماية اضافية، اما قواعد البيانات المركزية فبدون إجراءات سيطرة تكون أكثر خرقاً للامنية والخصوصية.

وهناك مجموعة من المنتجات التي تعمل على حماية قواعد البيانات مثبته في الجدول وسيتم في السطور الآتية عرض ثلاثة من المنتجات على سبيل المثال.

جدول (1): لبعض منتجات الحماية المستندة على البرمجيات

الشركة المنتجة	المنتج	الموقع(الرابط)
Imperva	SecureSphere	http://ww.imperva.com/index.html
Application Security, Inc	DbProtect	http://www.appsecinc.com/products/dbprotect
Fortinet's FortiDB	FortiDB	http://www.fortinet.com/products/fortidb
SafeNet	ProtectDB	http://www.safenet-inc.com/products/data-protection/database-protection/
Oracle	Database Firewall	http:/www.oracle.com/technetwork/database/database-firewall/overview/index.html

1. **FortiDB:** إن برمجيات FortiDB هي الضمان الشامل لحماية قاعدة البيانات الحماية التقنية. والركيزة الاساسية التي تساعد الشركات ومقدمي الخدمات لحماية قواعد بياناتهم والعمليات الواردة عليها من التهديدات الداخلية والخارجية. **كما** يسمح البرنامج المذكور بسهولة وسَـــــــــرّعة التنفيذ، والتحكم بأطر العمل الداخلية لتقنية المعلومات، ومراقبة نشاطات قاعدة البيانات، والالتزام بالمراجعة والتدقيق وبشكل المنتظم لتقنية المعلومات. كما يتوفر لشركة Fortinet **المنتجة ثلاث أنواع من** المنتجات وهي على التوالي:(1) FortiDB2000B وهو مصمم للمؤسسات الكبيرة (2) FortiDB1000C وهو مصمم للمؤسسات المتوسطة ويتصف بالمراقبة المركزية، وبالتدقيق والمسح المتعدد التوزيع (3) FortiDB400B وهو مصمم للمؤسسات المتوسطة والصغيرة ويتصف بسَـــــــــرّع التنفيذ وسهولة الادارة.
2. **ProtectDB:** قواعد البيانات هي **عنصر أساسي في** أي مركز من مراكزالبيانات ومؤسسة SafeNet**تعتمد** أعلى معايير الحماية **في مجال** تشفيرقواعد البيانات و**حلول التحكم عند طرح** منتجاتها التجارية.**برامج** ProtectDB **لمؤسسة** SafeNet متكاملة مع تطبيق DataSecure

وجاهزة أن تسلم للشركات لتوفير حماية قوية للمعلومات الحساسة للزبائن والمخزنة في قواعد البيانات.إن العمل مع ProtectDB سيوفر المرونة في تشفير البيانات على مستوى العمود (column) داخل قواعد البيانات، وعند طبقة (layer) التطبيق، وخلال تحويل بيانات بطريقة الدفعات المساقة (batch-driven)، ومعالجة الحركات أو المعاملات.والسياسة الادارية المركزية المقدمة مع DataSecure تبسط تطبيق تشفير البيانات عملياً في أي عدد من البيئات غير المتجانسة لقواعد البيانات.

3. **SecureSphere:** برمجيات SecureSphereلمؤسسةImpervaهي من افضل الحلول العملية الوافية لحماية قاعدة البيانات وتأمين البيانات الحساسة المخزنة في قواعد البيانات. ، كما أن هذه البرمجيات توفر رؤية كاملة في استخدام البيانات ونقاط الضعف وحقوق الوصول.كما أنها تتيح الأمان وتدقيق ومخاطرالمهنيين من اجل تحسين أمن البيانات،والمقاومة بعدم الاستسلام لرغبات سلطة الآمر أو العليا.أن SecureSphereتمكن الزبائن منالاستفادة المثلى من نشرحلول أمن قاعدة البيانات عن طريق الجمع بين تقييم المسح البعيد، ومراقبة نشاط الشبكة.كما يمكن استخدام وكلاء لمراقبة نشاط محدد لبعض المواقع المحلية حصراً، أو لرصد كل نشاط لقاعدة البيانات،أو يقدم وكلاء لغرض رصد قواعد بيانات لأجهزة الحاسوب المركزية[13].

وعموماً نستطيع أنَّ نستخلص مما ورد أنفاً أن جميع البرمجيات التي تم الإشارة إليها أو لم يتم تشترك بخواص أساسية كي تكون مقبولة كمنتجات لحماية قواعد البيانات القائمة على البرمجيات، وهذه الخواص هي توفير القدرة على اكتشاف وتصنيف المعلومات الحساسة في قواعد البيانات، وتدقيق برمجيات قواعد البيانات ونقاط ضعف المنظومة أو التكوين (configuration)، مثل:(1) برامج التصحيح software patches (ربما يخلق المبرمجين ما يسمى برامج التصحيح التي تهدف إلى إصلاح الأخطاء الصغيرة أو الخلل، ومواطن الخلل أو إصدار نسخ توافقية مع نظام التشغيل[14]) والتحكم في الوصول (2) رصد وتدقيق التغييرات في الشكل أو التكوين (3) تشفير البيانات الحساسة (تشفيرالبيانات الحساسةليست سوىالخطوة الأولى. فبدون تطبيق تقنيات المصادقة القويةعلى مستوى التطبيق، فمن السهل علىالمحتالين في الحصول علىمفاتيح فك تشفيرتلك المعلومات الحساسة) (4) معلومات عن نشاط قاعدة البيانات (5) مراقبة نشاط قاعدة البيانات على الشبكة بالوقت الحقيقي (6) التنبيه على سياسة الانتهاكات والقدرة على عرض تقارير مختلفة.

كما يجب أن نشير لضرورة وجود نوع من التكامل ما بين برامج إدارة قواعد البيانات (DBMS) والمميزات التي تتضمنها برمجيات الحماية. وهذا يعني أن نجد نوعاً من الاقتران والتعاون التام والمسؤولية التضامنية بينهم، لضمان من أن البيانات هي آمنة في جميع الاوقات.

3-2-1 حماية قواعد البيانات المستندة على المكونات المادية

في الصفحات السابقة تركز حديثنا حول وسائل الحماية المستندة على البرمجيات لقواعد البيانات، لأن العديد منمسؤولي النظم يقضون قدراكبيرا من الجهدعلى حمايةالبرمجية ولا تفعل شيئا حول الحماية المادية أو الفيزيائية. وهذا منطقياً لمنع الهجمات على شبكات الاتصال بالإنترنت بسبب كونها مفتوحة مما يجعلها عرضة للملايين المحتملة من المتسللين. في السطور التالية سيتم الحديث بشكل موجز عن الحماية المادية لانها لاتقل أهمية عن الحمايات الأخرى.

تأخذ الحماية المادية بنهجين الأول يتسم بالطابع الإجرائي المرتبط بالجانب البشري وهذا ما سوف نتحدث عنه في الجزء الأول والثاني والثالث، والنهج الثاني تقني يعتمد بشكل أساسي على الأجهزة في حماية قواعد البيانات وهذا ما سيتم الحديث به في الجزء الرابع.

الجزء الأول(العاملون على قواعد البيانات)وإن كان معظم العاملين في المؤسسات هم **صادقون وعاملون** بجد واخلاص، الا ان هناك حالات عديدة مثيرة تجاه **الادارة تتمثل** بسَـــــــرّقة بعض الموظفين البيانات المخزونة حاسوبياً.وكانت هناك أيضا حالات كثيرة حيث تزايدت حالات فقدان الموظفين والمتعاقدين بيانات مخزونة حاسوبياً بسببالإهمال. **والمبدأ العام** يفترض بأن **الناس** صادقين **في الأساس** ولكن هذا لايعني أنهم **من** الممكن أن لا يتخذوا قرارات سيئة وخاطئة. **لذلك لا نقترح أن** يتم تفتيش الموظفين **قبل** مغادرتهم **مراكز العمل** عائدين الى منازلهم، **ولكن** إذا كانت قاعدة البيانات تحتوي علىالبيانات المالية، **وأرقام بطاقات** الائتمان ،والأسَـــــــرّارالشخصيةالأخرى (مثلالخوارزميات **لاختيار**أرقام اليانصيب)، يجب **على الأقل توفر بعض وسائل الإشراف على** عدم تشجيع الموظفين على إخراج الاجزاء السرية من محتويات قاعدة البيانات على أقل تقدير.

الجزء الثاني(الأجهزة والمعدات الحاوية على قواعد البيانات) وسائط عالية الخزن وصغيرة الحجم قادرة أن تحمل العديد من الكيكابايت من البيانات. وهناك محركات اقراص USB المحمولة يمكن حملها بسهولة في حقيبة اليد تستوعب ما يصل إلى (2) تيرابايت، ومن المحتمل ظهور محركات أكبر من ذلك في المستقبل القريب.

أن العديد من الحواسيب القويةهي أيضاً صغيرة نسبياً، بحيث يستطيع الشخص التقاط الخادم والهروب به. اما إذا كان جهاز الحاسوب كبير جداً يصعب نقله بعيداً، فأنه بدقائق قليلة يتمكن من إزالة محرك **القرص الثابت. لذا نرى حفظ خادم** قاعدة البيانات في **مكتب مفصل و** يتم الوصول إليه عن طريق **للشبكة** الداخلية، **مماسيوفرقدر** من الحماية **الإضافية. كما** أن مسألة حماية الحاسوب المحمول خصوصاً في هذه الأيام يصعب تحقيقه. لأن الغرض من تصميم الإجهزة المحمولة هو لحملها. **فاذا كانت الحاجة لا تتطلب** النقل بعيداً عن الموقع، فربما يكون من الأفضل شراء جهاز حاسوب منضدي (Desktop) **والذي** سيكون من المؤكد أقل كلفة.

أنَّ سَـــــــرّقة أجهزة الحواسيب المحمولة (Laptop)أصبحت مشكلة كبيرة ومتنامية، لذا يجب أن نفترض أن أي بيانات يحملها الحاسوب المحمول هي عرضة للسَـــــــرّقة. فاذا كانت هناك ضرورات ملزمة لتخزين بيانات حساسة على الحاسوب المحمول فأختيار وسيلة التشفير هي ضمان لحماية البيانات **المخزنة**. قد يعتقد البعض أن نظم تشغيل الحواسيب المحمولة ستعمل على إيقاف السارق من قراءة القرص الثابت، ولكن هذا غير متاح.

الجزء الثالث(الوضع المتعمد للأخطاء أو نواقص لحماية قواعد البيانات وبرمجياتها) إن وضع أو سن تسلسلات إضافية غير ضرورية من ايعازات البرمجيات في تعليمات البرنامج الكامل في عدة أماكن [15] **أو وضع متعمد للأخطاء أو النواقص في** قاعدة البيانات قد تساعد على اكتشاف المعتدي على هذا البرنامج. شريطة الا تكون لهذه التسلسلات الإضافية أي عوامل أساسية لأداء البرنامج او تشغيله. فإذا كان هناك سبب للشك في أن منافس قد نسخ شفرة البرمجيات، فيمكن رفع دعوى قمع التقليد ضد المنافس منافسة غير **مشروعة**. فإذا كان رمز البرمجيات المستخدمة من قبل المنافس يتضمن نفس التسلسلات غير الضرورية من رمز البرنامج، فأن هذا الإجراء دليلاً على تقليد البرنامج من قبل المنافس. وهذا الآمر ينطبق على البيانات في قاعدة البيانات، فإذا قاعدة بيانات **المنافس تحتوي على أخطاء أو إغفالات** ذاتها، **فأن ذلك** دليل جيد وكبير أن قاعدة البيانات تم نسخها، كما ينبغي **أن تكون** هذه الأخطاء قد تم توثقيها بعناية. **ومع ذلك**، هناك **عنصر إضافي** الذي يمكن استخدامه **لإثبات النسخ، والذي** أود أن أشير إليه هو"التوقيع" **الحاسوبي**، هذاالتوقيع يتعلق بالتعليمات البرمجية **للحاسوب أو البرمجة** نفسها **المستخدمة** لتسجيل **المعلومات والبرامج**

التي تعالج المعلومات.فالمبرمج وبشكل طبيعي يضع توقيعه معينة أوأسلوب لطريقته في البرمجة، لذا فالمبرمج لديه الفرصة لغرس عمدا توقيعات مخفية يمكن تمييزها في عمله.

الجزء الرابع(الأجهزة والمعدات الحامية لقواعد البيانات) من المميزات التي تتمتع بها الحماية القائمة على الأجهزة لقواعد البيانات، بأنها لا تتطلب عمليات تنصيب للبرامج مما يجعل من السهل نقل جهاز الحماية من حاسوب إلى آخر. وفي حالة فقدان أو سَـــــــرّقة المحرك، فهناك حماية شبه مضمونه للبيانات الهامة، وذلك من خلال التمتع الكثير من هذه المحركات بمقاومة العبث بها بجعل البيانات الموجودة عليها عديمة الفائدة تماماً عندما يقوم شخص ما بمحاولة الكشف عنها. ونعتقد أن هذه الخواص ستشجع العديد من المستخدمين لقواعد البيانات إلى التحول واعتماد هذا النهج الذي يتسم بالدفاع الإيجابي مقارنة بالنهج الأول بمحوريه الذي يمكن أن يطلق عليه بالدفاع السلبي(ويقصد بالدفاع السلبي هي الإجراءات والتدابير المتخذة من أجل التقليل من تأثير الاختراقات والقرصنة وتضليل المنافسين وتقليل الكلف ودعم الدفاع الإيجابي عند اعتماده)، واستكمالاً للفائدة نعرض في الجدول (2) لبعض الشركات المنتجة لهذه الأجهزة.

جدول (2): لبعض منتجات الحماية المستندة على الأجهزة

الشركة المنتجة	المنتج	الموقع(الرابط)
Imperva	SecureSphere	http://www.imperva.com/products/ssp_hardware-appliances.html
SafeNet	HSMs	http://www.safenet-inc.com/hardware-security-modules...
Oracle	Oracle Database 11*g*	http:/www.oracle.com/database//**security**/hsms-for-**oracle**-tde-40...

ورأينا إن مستوى تدابير الحماية المناسبة لاتخاذها، يعتمد على تقديرنا للمخاطر الممكن حدوثها وتكلفة الخسائر الناجمة عنها. وهذا يقصد به أنه من الخطأ تجاهل الحماية المادية، ومن الخطأ أيضاً التفكير المهووس لدرجة الذعر. آخيراً، اتخاذ تدابير معقولة و لا نذهب بعيداً لدرجة المغالات في تلك الإجراءات.

بعد أن عرضنا في السطور أعلاه بشيء من الايجاز لكل من نهجي حماية التقنية (المستندة على البرمجيات و المستندة على الاجهزة) واستكمالاً للفائدة نقدم جدول مقارنة بين النهجين أدناه:

جدول(3): مقارنة بين **الحماية القائمة على الأجهزة و الحماية القائمة على البرمجيات**	
الحماية القائمة على الأجهزة	**الحماية القائمة على البرمجيات**
يوفر تدابير وقائيةأساساً.	يوفر تدابير كاشفة ووقائية.
تتسم بالطابع الإجرائي المرتبط بالجانب البشري وبالأجهزة والمعدات.	**تتسم بالطابع الموضوعي المرتبط بالجانب البرمجي.**
تركز توعية العاملين لأهمية حماية قواعد البيانات، لأنهم يشكلون التهديد الرئيسي وبنفس الوقت خط **الدفاع الأول.**	تركز على مواكبة وتحديث برامج الحماية وتدريب العاملين عليها.
تؤكد على تطبيق إجراءات عند استخدام أو عند ترك أي من العاملين على قواعد البيانات.	**تؤكد على سلامة** وصحة برمجيات الحماية المستخدمة ورصانة الجهات المجهزة.
يتم بناؤها خصيصاً ضمن البنية التحتية للمعدات أو الأجهزة التي تحتوي قاعدة البيانات.	ببساطة برمجيات تنصب على أجهزة الحاسوب لتصفية حركة الدخول والخروج للحاسوب الذي يحوي قاعدة البيانات.
يمكن لها أن تكون **فعالة جداً مع الحد الأدنى من** التكوين (التكوين configuration هو ترتيب في الوحدات الوظيفية طبقاً لطبيعة، وعدد، والخصائص الرئيسية لنظام الحاسوب)، كما يمكن حماية الحواسيب التي تحتوي قواعد البيانات وترتبط **بالشبكة.**	تحمي الحواسيب الفردية **(المستقلة)** التي يتم التنصيب عليها.

4-2-1 حماية وسائل التقنية المستخدمة لحماية قواعد البيانات

وقبل أن نختم هذا الجزء من البحث نود أن نشير إلى الحاجة لتوفير حماية لوسائل التقنية المستخدمة لحماية قواعد البيانات والتي تتصف بالطابع القانوني المانع بالإضرار وبأيقاف عمل وسائل الحماية.

إن الوسائل الموجهة لحماية قواعد البيانات على أساس تقني لا يمكن أن تكون فعالة إلا إذا كانت محمية هي الأخرى من أي تحويل أو تغيير لمسارها أو هدفها. لهذا أوجدت المجموعة الأوربية قرار توجيهها أدرجت فيه طرق لحماية الوسائل التقنية المقررة لحماية قواعد البيانات. وعلى هذه الأساس فإن على الدول التي تنتمي إلى المجموعة أن تفرض حماية قانونية ضد تصنيع،تصدير وتوزيع، بيع،إيجار،إشهاربهدف البيع أوالإيجار،حيازة منتجات أومصنفات مثل قواعد البيانات لأهداف تجارية،أوحيازة مواقع خدمات التي تكون موضوعا للتجارة بهدف تحويل الحماية،أو حيازة وسائل ومنتجات منشأة بهدف السماح أوتسهيل تحويل الحمايةالتي توفرها كل وسيلة تقنية فعالة،وهذاماجاء في **المادة السادسة فقرة 4 من القرارالمذكورأعلاه** [16].

ومن خلال ما استعرضناه من أهمية توفير وسائل التقنية لحماية قواعد البيانات وطرق حماية لوسائل التقنية لحماية قواعد البيانات في أولاً أنفاً، يكون من الضروري توفير حماية من نوع آخر ارتأت العديد من الدول ومنها العراق أن تكون هذه الحماية على أساس قانوني(مدني وجنائي) وهذا ما سيتم البحث في ثانياً.

ثانياً:- وسائل الحماية القانونية لقاعدة البيانات

مع قدرة التقنيات على تحقيق حماية فنية للمنتجين في حماية قواعد بياناتهم، فأنها مازالت في مرحلة مبكرة من تطورها وليس استخدامها واسع النطاق لحد الان. لذا فأن الحاجة إلى الحماية القانونية من

منظور قانوني مازالت مطلوبة. وبسبب عدم وجود قانون خاص لحماية قواعد البيانات، فأن الحماية القانونية لقواعد البيانات تعتمد حالياً على قانون حقوق المؤلف، وقانون العقد، وقانون العلامة التجارية، وقانون الاسرار التجارية. ومهما يكون، فأن قانون الاسرار التجارية المتاح يحمي فقط قواعد البيانات غير المنشورة. أما قانون العلامة التجارية فهو يحمي فقط العلامة التجارية لقواعد البيانات من الاستعمال غير المسموح بها. لذا فأن قانون العقد وقانون حق المؤلف هما أكثر الوسائل القانونية فعالية لتقديم الحماية لقاعدة البيانات. ولهذا السبب سنركز في هذا الجزء من البحث عليهما ونختمه بجزء ثالث يتضمن توجهات داعمه لكلا القانونين.

1-2 حماية قواعد البيانات بموجب نظام حق المؤلف

أنَّ قواعد البيانات تقع تحت وصف المصنف الأدبي حسب ما هو متفق عليه في جميع التشريعات، و هي بهذا تتمتع بالحماية الكاملة، لذلك وفقاً للقواعد القانونية في حق المؤلف [17]وإن حقوق الطبع والنشر تعطي المبدعين أنواعاً محددة من الحقوق المادية للسيطرة على طرق استخدام بيانات القاعدة، وهذه الحقوق تبدأ حالما يتم تسجيل المواد كتابةً أو بأي طريقة أخرى، ففي كثير من الحالات فإن المؤلف أيضاً لديه الحق في التحديد على بيانات معينة ضمن قاعدة البيانات (وقد وضحنا البعض من هذه المحددات في المبحث الأول)، والاعتراض إذا تم تشويهها أو تحريفها، وتتم حماية قواعد البيانات بموجب هذا القانون إذا كان أختيار البيانات أو ترتيب محتوياتها يستلزم جهداً [18]أي مادامَ أعدادها كان مُتميزاً بطابع الأصالة أو الترتيب أو الاختيار أو أيّ مجهود شخصيّ آخر يستحق الحماية (قانون حماية حق المؤلف رقم (3) لسنة 1971 المُعدل المادة السادسة من القانون العراقي).

إن طابع الأصالة يظهر في تصميم هيكل (بنية) قاعدة البيانات، أي المعمارية لهذه القاعدة وليس البيانات أو المواد بحد ذاتها[19]فإذا بذلَ المُعّد جهداً في ترتيبِ القوانين أو في مُتابعة تعديلاتها مع التعليق عليها والاشارة المُستفيضة الى موضع الالغاء أو التعديل ،فإنَ جهده يصلح لأن يكون جهداً مُبتكراً ينشأ عنهُ وبسببهِ حقٌ يعترف بهِ القانون، يُدعى بحق المؤلف. فحقوق الطبع والنشر تحمي المصنفات الأصلية الأدبية والدرامية والموسيقية والفنية، والإصدارات التي نشرت من أعمال، والتسجيلات الصوتية (بما في ذلك الأقراص المدمجة)، والأفلام (بما في ذلك أشرطة الفيديو وأقراص الفيديو الرقمية) والبث.

لذا نرى أن الشرط الضروري لتمتع قاعدة البيانات بصفة خاصة بالحماية المقررة وفق حق المؤلف هو الأصالة والابتكار. وأيَّاً كان نوع هذهِ القاعدة –ورقياً أم حاسوبياً- فإنَ حُكم المؤلف ينطبق على مُصممِها غالباً. وحكم الابتكار يتلاءم مع مضمونها و مُعالجتها ولاسيما إذا كانت هذهِ المُعالجة تتم عبرَ أجهزة الحاسوب. وإذا تصورنا ان مُصممَ هذهِ القاعدة قامَ بتصميم البرمجيات العاملة فيهِ، فإنَ حكم المؤلف يُضفى عليهِ أيضاً لفرضين، يكفي أحدهما للحكم عليه بأنهُ مؤلف. الفرض الأول، هو لو اقتصرَ دوره على مجرد تصميم البرَنامج فهو مؤلف للبرَنامج لا للقاعدة ومن ثمَّ أذا أستخدمَ مبتكر قاعدة البيانات هذا البرَنامج في تشغيل قاعدتهِ فلا يمنع ذلك من القول ان مُصممَ هذهِ القاعدة هو مؤلفٌ لها على الرغم من استفادتِهِ من برَنامج قامَ غيره بتصميمهِ. والفرض الثاني، هو لو قامَ مُصمم القاعدة بتصميم البرمجيات العاملة فيهِ ايضاً، فإنهُ ومن باب أولى يُعتبر مؤلفاً لها إذ أنَّهُ يُصبح مؤلفاً للقاعدةِ بتصميمهِ إياها، وهذهِ مسألة مفروغٌ منها. كما يصبح أيضاً مُصمماً للقاعدة وبضمنها البرمجيات العاملة فيها كلها، وهذهِ مسالة بديهية تُعبرُ عن نفسها بنفسها.

ولو تتبعنا اتجاه المُشرِّع العِراقيَّ في قانون حماية حق المؤلف رقم (3) لسنة 1971 المُعدل لوجدناهُ قد خَففَ من شرطِ (الابتكار). فلمْ يستلزم لإضفاء صفة المؤلف على مُصمم قاعدة البيانات أو مُعدها أن يكون ابتكاره متميزاً أو أن يكون قد بذلَ فيهِ جهداً واسعاً في سبيل إعدادهِ أو أضاعَ وقتاً كبيراً

في تصميمهِ [20]وإنما إكتفى بضرورة بذل جهد شخصيّ معقول –أيّاً كان نوعه- لإضفاء الحماية على قاعدة البيانات، ولو كان موضوع مَحَلَّ بياناته يتعلق بمختارات الشعر أو النثر أو مجموعات الاغاني الرومانسية أو غيرها من الاغاني لابل حتى لو كان مضمونها إعادة نشر المُصَنَّفات التي آلت الى المُلك العام [21]وهذا مانصت عليهِ المادة (السادسة) من قانون حماية حق المؤلف رقم (3) لسنة 1971 المُعدل، بقولها: ((يتمتع مايلي بالحماية طالما كان متميزاً بطابع الاصالة أو الترتيب أو الاختيار أو أيّ مجهود شخصيّ أخر يستحق الحماية:

1. المجموعات التي تنتظم مصنفات عدة لمختارات الشعر والنثر والموسيقى وغيرها من المجموعات دونَ المساس بحقوق مؤلف كل مصنف.
2. مجموعات المُصنَّفات التي آلت الى المُلك العام.
3. مجموعات الوثائق الرسمية كنصوص القوانين والانظمة والاتفاقيات الدولية والأحكام القضائية وسائر الوثائق الرسمية.)) [22].

2-1-1 حماية مؤلف المُصَنَّف المُشتق في قاعدةِ البيانات

ولمَّا كانت إدارة قاعدة البيانات ببياناتها ومُعالجاتها غير مُقتصرة أو مُحددة ببرنامج أو مُصنف أو مؤلف ما من البرمجيات أو المُصَنَّفات أو المؤلفين، فإنَ بإمكان مُصمم هذهِ القاعدة (أو مُعّدها) ولاسيما إذا تولى إدارة القاعدة بنفسهِ من الاستفادةِ من المُصَنَّفاتِ المحمية السابقة أو المُعاصرة أو حتى اللاحقة على تصميم قاعدة البيانات وذلكَ لإمكانية إدخالها وإدراجها فيها كبيانات، ومن ثم يستفيد مُصمم هذهِ القاعدة من جهد غيرهِ[23]. إذ لاشكَ في تمتع قاعدة البيانات بالحمأيّة القانونية للملكية الفكرية سواء أكانت مطروحة على المُستفيدين خاليةً من البيانات أو مُزودة بنوع منها. فإذا كانت القاعدة من النوع الثاني، أيّ من النوع المُزودة بالبيانات (كالمُصنَّفات مثلاً)، فإنَ ممّا لايقبل الشك أن يتم إدخال هذهِ البيانات (أو المُصنَّفات) بشكل يتناسب مع نوع القاعدة. فإذا كانت القاعدة التي قامَ بتصميمها المؤلف ورقية اضاف المُصمم المُصَنَّف الورقي المطلوب الى قاعدتهِ؛ وذلك بإستنساخهِ وإدراجهِ في هذهِ القاعدة كما هو أو بإعادة طباعتهِ. وأمَّا لو كانت قاعدة البيانات حاسوبية فمِّن الممكن إدراج هذا المُصَنَّف بتغير قاعدتهِ الورقية (أو المادية) الى قاعدة رقمية. ويواجه المنافس المهتم في نسخ فقط الاجزاء غير المحمية بحقوق المؤلف سيواجه عقبتين :(1) عملية فصل الحقائق من النص قد تتطلب عمل كبير(على الرغم وربما اقل من ذلك بتحسن التقنيات) (2) قد تكون المواد المحمية بحقوق النشر متكاملة بما يكفي لإعطاء المنتج الأول ميزة تنافسية في السوق. وأخيراً، قواعد البيانات التي تحتوي نص محمي بحقوق النشرلديها احتمال أقوى لحماية حق المؤلف من تلك التي هي حقيقية بحتة[24].

2-1-2محددات لحماية حقوق المؤلف

يجب على مشرعي حماية حقوق الملكية الفكرية بوجه عام ومشرعي حماية حقوق النشر بوجه خاص أن يأخذوا بعين الاعتبار مصالح المؤلفين والمبدعين واحتياجات المجتمع من أجل الوصول إلى المعلومات و المعرفة. لذا يتطلب تحقيق توازن بين الاثنين، من خلال خضوع حقوق النشر لنوعين من القيود[25].

1. قيود على مدة حماية حق المؤلف: تحمى الاعمال لفترة زمنية، وعند انقضاء الأجل، فأنها تدخل في نطاق الملك العام ومن ثم يمكن استخدامها بحرية من قبل أي شخص.
2. قيود على المنافع الاقتصادية: تفرض القوانين الوطنية قيود واستثناءات على الاستغلال الاقتصادي لحقوق النشر خلال فترة الحماية.

يهدف من حقوق التأليف والنشر هو لتأمين للمؤلفين خلال حياتهم، وإلى ورثتهم التمتع الحصري من ثمرة عملهم الابداعي، فترة من الزمن بعد وفاة المؤلف. ومع ذلك، فأن الوصول إلى الاعمال الفكرية

بالنهاية سوف يسود، وبالتالي فأن حقوق المؤلفين، أو الأقل حقوقهم الاقتصادية تنتهي صلاحيتها. وبهذا الحال يصبح العمل غير محمي بموجب حق المؤلف ويكون في نطاق الملكية العامة.

2-2 حماية قواعد البيانات بالتعاقد

تتم حماية حقوق اصحاب قواعد البيانات من خلال العقود، وهي ممارسة قانونية اخرى يتم استخدامها بشكل فعَّال من قبل مزودي قواعد البيانات. والعقد هو اتفاق وقد يتضمن اتفاقاً جامعاً لعدة عقود منضوية تحته ويصف مجموعة مقبولة من التفاهمات المتضمنة للالتزامات بين الطرفين والتي يتم صياغتها غالباً بعد المناقشات والمفاوضات. وقد يضمن العقد حقوق المؤلف قبَلَ صاحب قاعدة البيانات، اما حق المؤلف نفسه فهو محمي قانوناً بموجب قانون حماية قاعدة البيانات أو بموجب قوانين حقوق النشر. ويضمن العقد حماية المؤلف وصاحب قاعدة البيانات من خطر أو اي اعتداء يقوم به ايٍّ اجنبي. إن مالك قاعدة البيانات هو الشخص المسؤول عن محتوياتها، لذايتطلب أن تكون خالية من كل الاعباء القانونية. وينبغي أن يحترم اتفاق الاستثناءات ليحقق الاستخدام العادل للباحثين والتربويين[26]. ويمكن ضمان المساءلة عن دقة البيانات في قواعد البيانات بواسطة شرط في اتفاق تعاقدي(الترخيص) بين المبتكر أو المستحدث لقاعدة البيانات ومستخدميها[27].ويشترط لصحة هذا الاتفاق أنْ يكون تحريرياً لا شفهياً، والكتابة كشرط وضعت لمصلحة المؤلف وحده. وهذا ما نصت عليه المادة (الثامنة والثلاثون) من قانون حماية حق المؤلف العراقي رقم (3) لسنة 1971 المعدل، بقولها: ((للمؤلف أنْ ينقل إلى الغير حقوق الانتفاع المنصوص عليها في هذا القانون إلاَّ أنْ نقل احد الحقوق لا يترتب عليه أعطاء الحق في مباشرة حقٍ آخر ويشترط لصحة التصرف أن يكون مكتوباً أنْ يحدد فيه صراحةً بالتفصيل كل حق يكون محلاً للتصرف مع بيان مداه والغرض منه ومدة الاستغلال ومكانه. وعلى المؤلف أنْ يمتنع عن أيّ عمل من شَأنِهِ تعطيل استعمال الحق المتصرف به)).

أنَّ مزج تدابير الحماية التقنية (شرحت في المبحث الأول) مع الاحكام العقدية المحمية تحت طائلة المسؤولية العقدية يمكن أن تمنع اعمال القرصنة أو أنْ تحد كذلك من الاستثناءات المسموحه للدخول إلى القاعدة مثل التعامل المشروع (fair dealing) للباحثين والتربويين، والحظر القانوني على التحايل على تدابير الحماية التقنية التي تتحكم في الوصول إلى قواعد البيانات ذات الملكية العامة، وهذا يتوقف على كيفية صياغته، فلمزيد منه يمنع الجمهور من ممارسة الحقوق الحالية[28] .

3-2 ستراتيجيات سائدة لتعريف الابتكار في قواعد البيانات

العديد من القضايا قد نوقشت حول كيفية حماية قواعد البيانات، من الاستخدام غير المصرح به، وكيف يتم الترخيص لها. لذا فأن إلقاء نظرة عامة لممارسات صناعية، سوف يكون مفيداً في دراسة مدى كفاية الحماية القائمة ومدى تأثير أي تغييرات في القانون[29]. واحدة من التوجهات التي درست من قبل منتجي صناعة قاعدة البيانات، هو تبني وسائل داعمة أو ستراتيجيات ثلاث لتغطية القصور في تحديد معنى الابتكار في قانون حق المؤلف؛ وذلك لان الابتكار هو شرط استمرار تقديم الحماية للمؤلف فبدونه لاحماية لحق المؤلف وبتحققه تقدم الحماية اللازمة له.

1. **تعزيزحماية حق المؤلف عن طريق تغييربنيةأومحتوىقواعد البيانات لدمج المزيد من الإبداع.أن** تعزيزحماية حق المؤلف قد يترتب عليها<u>إضافة</u> نص محمي بحقوق النشرأو<u>تغيير</u>اختيار وترتيب قاعدة البيانات لجعلها أكثر إبداعا. وأنْ كلا النهجين يزيد من احتمال أن قاعدة البيانات ككل سوف تكون مناسبة لحقوق الطبع والنشر لكنها محدودة في فائدتها كوسيلة لمنع النسخ من المكونات (الحقيقية) لقاعدة بيانات.بالإضافة إلى ذلك، وهذا يتوقف على نوعقاعدة

البيانات، وأن هذه المناهج قد جعلت قاعدة البيانات أكثر تكلفة لإنتاج وأقل قيمة لمستخدم يسعى الى مجموعة شاملة وسهلة الوصول إليها من البيانات.

2. **زيادة الاعتماد على العقود.** العقود هي مصدر رئيسي للحماية للمنتجين قاعدة البيانات، سواء من العقود والاتفاقات المتفاوض عليها والتي وردت في مجموعة متنوعة من الأشكال المطبوعة والإلكترونية .نموذجياً، حيثُ يتم استخدام عقود لتقييد الوصول، تحديد شروط المسموح بها للاستخدام، ووضع شروط لإنفاذ والتعويضات شركات مختلفة توفر هياكل مقاوتة من الأسعار.وأنه المعيار العادل للمنتجين للانخراط في الأسعار التفاضلية،وفرض الرسوم المخفضة للمؤسسات غير الربحية و التعليمية.
3. **توظيف الضمانات التقنية لمنع الوصول غير المصرح به والاستخدام.** الضمانات التكنولوجية لا تزال في مراحل التطوير، فهناك مجموعة من التقنيات المتطورة المستخدمة في الشركات المنتجة لنظم أدارة قواعد البيانات (DBMS) مثل (SAP، Peoplesoft، Oracle7) على أساس كلمة المرور والرقم السري(PIN).وبقدر مايتم إستخدامها يفضل أن تكون في تركيبة مع التراخيص وتنفيذالحقوق القانونية.وهذه التقنيات من المؤكد أن يتوسع اعتمادها في المستقبل القريب مع تقنيات أكثر تقدماً، وهي نظم التحقق من الهوية المستندة على الترميزوالتي تم الاشارة لبعضها في المبحث الأول.

أنَّ هذه الستراتيجيات الساندة لمفهوم الابتكار أو تعريفه تجعل من مصمم القاعدة مؤُلفاً تقنياً للخطوة الابداعية فيها، بكلّ ما تحمل هذه الكلمة من معنى، وذلك مهما كان نوع القاعدة المصممة أو الغرض الذي صممت من اجله. بينما لاتعتبر البيانات الداخلة من قبل الشخص أو المستفيد إلى قاعدة البيانات مؤُلفاً إلاّ اذا توفرت شروط الحماية القانونية لمؤلفي المصنفات بوجه عام أو توافرت فيه على الاقل احدى الستراتيجيات الحديثة التي تناولناها في هذا المطلب وخاصة ستراتيجية تغيير بنية أو محتوى قواعد البيانات لدمج المزيد من المصنفات الابداعية فيها.

وهذا يعني أنَّ الابتكار أو الابداع هو عملٌ مفترض وجوده في تصميم قاعدة البيانات، مادام المصمم قد بذل جهوداً كبيرة في ابتكارها أياً كان نوع ذلك الابتكار أو طبيعته أو حجمه ولم يقم بالاعتداء على أيّ حق محمي لغيره من مصممي قواعد البيانات أو لم يدرج فيها مصنفاً بغير أذن من مؤلفه كتابةً. ومن ثمَّ يفترض حماية حقوق مصمم القاعدة باعتباره مبتكراً للخطوة الابداعية غير القابلة للتبرئة (أو لحمايتها بمقتضى نظام براءات الاختراع) لعدم استكمالها لشروط البراءة من تطبيقٍ صناعي مباشر.

الخاتمة

لقد حاولنا في هذا البحث تحديد ما إذا كانت الانواع المختلفة من الحماية سواء كانت مفردة أم مجتمعة- ستوفر الحماية الكافية لقواعد البيانات. وعندما يتعلق الآمر بحماية بيانات حساسة في قاعدة بيانات، ليست هناك حلول مثالية، أياً من التقنيات الحالية لا يمكن أن تضمن الحماية المطلقة. لذا فأن بحثنا هدفه هو أختيار أفضل الخيارات التي سوف تعمل على الامتثال لمتطلبات حماية قاعدة بياناتك. أن فهم كيف توفر الانواع المختلفة من أساليب الحماية القانونية والتقنية سوف تساعدك على تقييم نقاط الضعف وتمنعك من الاستسلام للشعور بالأطمئنان الزائف. اما إذا كنت ترغب في بناء أو شراء حلاً تقنياً لحماية قاعدة البيانات، فمن الضروري التأكد من أنه يستخدم التشفير القوي، ويوفر حماية معقولة لمفاتيح التشفير، وتقييد الوصول إلى البيانات المشفرة. بينما لاتوجد برمجيات حماية تجعل بياناتك آمنة تماماً، فأنه يمكن المدخل الصحيح يساعدك على تجنب الانواع الاكثر شيوعاً في تعرضها للخروقات.

إن قواعد البيانات، سواء المنشورة أوغير المنشورة ذات قيمة كبيرة إلىمجموعة متنوعة من الشركات. لهذا فهي تحتاج إلى الحماية الكافية من منظور قانوني بسبب أن الضمانات التكنولوجية لازالت في مرحلة مبكرة من تطورها وليست واسعة الاستعمال. و على الرغم من أن الجميع متفقون على أن قواعد البيانات تحتاج إلى حماية قانونية كافية فإن مستوى الحماية والشكل الذي ينبغي عليه اتخاذها لتوفير الحماية الكافية كانت موضع تباين في وجهات النظر. مقابل ذلك فأن الاستثمار الخاص في إنشاء قاعدة البيانات زاد بشكل كبير في السنوات الأخيرة، خلاف ما يتصل بمستوى وشكل حمايتها.

توفر التشريعات الحالية على قدر معين من الحماية لقواعد البيانات مع تركيبة من حق المؤلف، التراخيص (العقد)، الاسرار التجارية، والعلامة التجارية وغيرها. وقد تركز بحثنا على قانون حق المؤلف لكونه هو الطريقة الاكثر فعالية لحماية قواعد البيانات من منظور حق من حقوق الملكية الفكرية، حين أن قانون العقد يوفر حماية فعالة عن طريق تقييد الوصول إلى قواعد البيانات. وعموماً فأن قانون الحقوق الملكية الفكرية هو الشكل الاكثر مرغوب فيه من وجهة انصار حماية قواعد البيانات.

اخيراً، ما لم يتم التعاون بين مؤسسات تقنيات الحماية (برمجيات ومعدات H/S) والشركات المنتجة لقواعد البيانات، فربما يرجح كفة تسيد الاتجاه القانوني بأن تقوم المحاكم بالعمل على خلق مثل هذه الحماية. لذا فأن الحل هو في أيديهم ولزاماً عليهم أن يأخذوا أمن وحماية قاعدة البيانات على محمل الجد.

المصادر

1. د.طالب محمدجوادعباس، عبدالجبارضاحي، جرائم تقنيه المعلومات وإثباتها مجله كليه الرافدين-الجامعة، العدد 28 لسنة 13، 2011.

2 .Carlos Coronel, Steven Morris, Peter Rob, "Database Principles of Design,Implementation, and Management", Printed in China by China Translation & PrintingServices Limited, 9th Edition, **2011**, p5.

3.David M. Kroenke , David J. Auer, "Database Concepts ", Pearson Prentice Hall, Upper Saddle River, New Jersey 07458, Third Edition, **2008**, P3.

4. C. J. DATE,, "An Introduction to DATABASE Systems", Seventh Edition, Addison-Wesley Publishing Company, pp (9-10), **2000**.

5. بوعمرة اسيا، " النظام القانوني لقواعد البيانات"، مذكرة لنيل شهادة الماجستير في القانون فرع الملكيه الفكريه، 2004/2005، ص12.

6. د.فاروق الاباصيري، "عقد الاشتراك في قواعد المعلومات الإلكترونية:دراسة تطبيقية لعقود الإنترنت"، الناشر:دار النهضة العربية، 2003، ص29.

7. د. علاء عبدالرزاق السالمي، د. محمد عبدالعال النعيمي، "اتمتة المكاتب"، دار المناهج، الطبعة الاولى، 1999، ص ص(69-70).

8.David M. Kroenke , David J. Auer, previous reference, P14.

9. Laudon C Kenneth, "Management Information Systems-Manage the Digital Firm", Prentice Hall, 9th edition, chapter7, **2006**.

10. د.إيهاب بني هاني و د.معن الصقر، "انظمة المعلومات التسويقية"، ط1، القاهرة، الشركة العربية المتحدة للتسويق والتوريدات 2010، ص ص(292-293).

11. د.هلال محمديوسف و سليمة باجي عبدالله، "تطبيق محوسب امني لحماية البيانات"، مجلة كلية الرافدين الجامعه للعلوم، العدد 4 السنه التالته 2000م، ص ص(21-22).

12.Rod Stephens, "Beginning Database Design Solutions", published by wiley publishing, Inc, **2009**, pp (390-391).

13. Imperva, Data Center Security Solutions, http://www.imperva.com/index.html

14.WiseGEEK, "what is software pitches",http://www.wisegeek.com/what-is-a-software-patch.htm, **2012**.

(15)د.طالب محمدجوادعباس، د.اكرم فاضل سعيد، "الحماية القانونية والتقنية لبرمجيات الحاسوب"، بحث منشور في مجله كليه التراث-الجامعه، العدد 12 لسنة 2012.

(16)بوعمرةاسيا، مصدر سابق، ص129.

(17)المصدر السابق، ص145.

18.Intellectual Property Office, "Copyright: Basic Facts", www.ipo.gov.uk/c-basicfacts.pdf.

19. Petya Totcharova, "The ABC of Copyright", UNESCO Culture Sectore, p 20, **2010**, www.unesco.org/culture/copyright.

20.ينظر ديالا عيسى ونسه، حمايه حقوق التاليف، المرجع السابق، ص43. و د.طوني ميشال عيسى، التنظيم القانوني لشبكة الانترنيت، المرجع السابق، ص113

21. انتقد د.جمال هارون في مؤلفهِ: الحمايه المدنيه للحق الادبي للمؤلف في التشريع الاردني (دراسة مقارنه)، ط1، عمان: دار الثقافة، 2006، ص150 منح الحماية مجموعات الشعر ومصنفات الملك العام والوثائق الرسمية وذلك لان الترتيب لايرتقي الى المستوى الابتكار، إذ كتب في ص150 من مصنفهِ المذكور، مايأتي: ((بمعنى ان الترتيب وحده دون الابتكار يكفي لمنح الحماية، في حين ان الابتكار دون الترتيب هو الشرط المعتبر لغايات الحماية)).

22. عدلت المادة (السادسه) من قانون حماية حق المؤلف رقم (3) لسنة 1971 المعدل بموجب امر سلطه الائتلاف المؤقته المنحله (CPA) رقم (83) في 2004/5/1.

23. ينظر: د.محمد خليل يوسف ابو بكر، حق المؤلف في القانون (دراسه مقارنه)، ط1، بيروت، لبنان: المؤسسة الجامعية للدراسات والنشر والتوزيع (مجد)، 1429هـ، 2008م، ص159، التي جاء فيها مايأتي: ((ويتطلب من المؤلف الذي يضع العمل المشتق الحصول على اذن او ترخيص من صاحب العمل الاصلي او خلفائه لإستعمال العمل الاصلي والمحافظة على حقوقهِ المادية والمعنوية)).

24.U.S. Copyright Office, "Report on Legal Protection for Database", August **1997**, P19, www.copright.gov/reports/db4.pdf.

25. Petya Totcharova, previous reference, p45.

26.Gupta V.K, "Legal Protection of Database", Malaysian Journal of Library&Information Science, Vol.5, No.2, December **2000**: 19, P 27, http://ejum.fsktm.um.edu.my/article/158.pdf

27. Susan Corbett, "Legal Protection for the Database: Is there a better way?", 30 November **2011**, P 26, www.iscr.co.nz/.../Databases_and_copyright_paper_Fin...

28. Ian R. Kerr, Alana Maurushat and Christian S. Tacit, "Technical Protection Measures: Tiling at Copyright's Windmill", OTTAWA LAW REVIEW VOL. 34, No. 1, **2003**, P 48, www.commonlaw.uottawa.ca/index.php?option...
29.U.S. Copyright Office, previous reference, p20.

Employing Technical and Legal Means to Protect Databases

Ph.D.(Assist. Prof) Talib M. Jawad Abbas*

Abstract

The prevalence of inexpensive and powerful computer systems and storage has led to the gathering of unprecedented amounts of data by organizations from all facets of daily life .This intelligent data gathering in a manual or a computer form as well as its advanced processing are, generally called database. Data bases play an important role in the development of information market and its products. A large number of databases are available online from foreign vendors which now find an increasing market in the country. Authors or developers are interested in receiving remuneration from databases which are based on intellectual and skillful inputs. Thus, they want to restrict copying from databases while the users are keen to make use of the information either without paying for it or through having copying rights at relatively lesser cost.

This study presents a new paradigm for thinking about intangible property rights in response to recent criticism that information products such as databases should not be over-propertied. This study shows two main types of available protection: technical protection and legal one.

Keywords: Database, technical protection, legal protection, copyright protection.

* Al-Nahrain University/ College of Information Engineering