الحماية الجنائية لقواعد البيانات في تشريعات الدول العربية

د. عبد الوهاب عبد الكريم المبارك

كليات الخليج – السعودية

ملخص البحث:

يتناول هذا البحث الحماية الجنائية لقواعد البيانات في تشريعات بعض الدول العربية، وبعد يتناول هذا البحث الحماية الجنائية لقواعد البيانات في تشريعات بعض الدول العربية، وبعد أن اتجهت أغلب دول العالم الى الحكومة الالكترونية وما يتبعها من نقل للمعلومات والبيانات عبر الشبكة المعلوماتية. قسمت هذا البحث الى ثلاث مباحث، تناولت في المبحث الأول مفهوم الحماية الجنائية ومفهوم قواعد البيانات فالحماية الجنائية تتمثل في سن التشريعات الجنائية التي تعاقب على الاعتداء على الحق العام والحق الخاص، وهي إضفاء الحماية التشريعية للمصالح التي يتوخاها الشارع ويعبر عن ذلك بالجزاء الجنائي على الجرح والقطع. وتختلف الحماية الجنائية في قانون الاجراءات عن الحماية الجنائية في قانون العقوبات حيث تستمد الحماية الجنائية في قانون الاجراءات عناصرها من قواعد قانون الاجراءات وهي القواعد التي تبحث في تنظيم جهات القضاء واختصاصاتها وكشف الجريمة وطرق إثباتها وضبط مرتكبيها والتحقيق معهم ومحاكمتهم وغيرها من القواعد الاجرائية وهي كذلك تقرر حق الدولة في العقاب ووجوب اعمال قواعد القانون الجنائي الاجرائية لاستيفاء هذا الحق. أما قواعد البيانات فهي عبارة عن مجموعة منظمة من المعلومات المهيكلة أو البيانات المخزنة عادةً بصيغة الكترونية أو في نظام حاسوب. أما المبحث الثاني تناولت فيه نطاق الحماية الجنائية لقواعد البيانات، ويشمل نطاق الحماية الجنائية قواعد البيانات الحكومية وقواعد البيانات الخاصة. وتعد قواعد البيانات الحكومية اللاعب الرئيس في ظل التحول الرقمي والانتقال من مفهوم الحكومة التقليدية الى مفهوم الحكومة الذكية.

وجاء المبحث الثالث مشتملاً على بعض الأفعال التي تشكل جرائم على قواعد البيانات، مثل جريمة الدخول غير المشروع وجريمة الاعتداء على قواعد البيانات وغيرها من الجرائم ومعاقبة التشريعات على ذلك. وقد ختمت البحث بأهم النتائج والتوصيات التي توصلت إليها.

الكلمات المفتاحية: الحماية الجنائية، قواعد البيانات، التشريعات، جريمة الكترونية.

Criminal Protection of Databases in Arab Legislation

Dr. Abdulwahab Abdulkarim Al-Mubarak

ABSTRACT:

This research examines the criminal protection of databases under the legislation of some Arab countries, especially because most countries around the world have moved toward e-government and the accompanying transfer of information and data through information networks. The research is divided into three sections. The first section addresses the concept of criminal protection and the concept of databases. Criminal protection is represented by the enactment of criminal legislation that punishes infringements on public and private rights. It involves granting legislative protection to the interests intended by the legislator, which is expressed through criminal sanctions imposed for violations and harm. Criminal protection in the Law of Criminal Procedure differs from criminal protection in the Penal Code. In the Law of Criminal Procedure, criminal protection derives its elements from procedural rules that regulate judicial authorities and their jurisdictions, the detection of crimes, methods of proof, the apprehension of offenders, investigation, and trial, as well as other procedural rules. These rules also establish the state's right to punishment and the obligation to apply criminal procedural law to realize this right. As for databases, they are defined as an organized collection of structured information or data, usually stored in electronic form or within a computer system. The second section addresses the scope of criminal protection for databases, which includes both governmental databases and private databases. Government databases are considered the main factor considering digital transformation and the transition from the concept of traditional government to that of smart government. The third section includes a discussion of some acts that constitute crimes against databases, such as the crime of unauthorized access, the crime of attacks on databases, and other related crimes, along with the penalties prescribed by legislation for such acts. The research concludes with the most important findings and recommendations reached by the study.

Keyword: Criminal, Databases, Legislation, Cybercrime

المقدمة:

شهد القرن العشرين تطوراً علمياً متسارعاً أدى هذا التطور الى تعقد الحياة البشرية وذلك بتزايد الابتكارات والاختراعات العلمية والتي يأتي على رأسها جهاز الحاسوب الذي شمل استخدامه مجالات التعليم والبحث العلمي وغيرها من المجالات الأخرى.

وقد أصبح استخدام الحاسوب مقياساً لتقدم الأمم ومواكبتها للتطور، بل ومؤشراً لثورة صناعية جديدة أساسها التكنلوجيا، وأمام هذه الجوانب والمجالات المختلفة لاستخدام الحاسوب وتقنية المعلومات كان من الطبيعي ظهور جوانب سلبية، وأبرز هذه الجوانب كان ظهور نوع جديد من الجرائم، سواءً كانت ترتكب باستخدام هذه التكنلوجيا أم جرائم تقع على هذه التكنلوجيا.

كما أن الأنظمة الحديثة تحتاج لتسيير أعمالها في مختلف المجالات الى تخزين كم هائل من البيانات الكترونياً وخاصة ما يتعلق بالعملاء والموظفين والفواتير وغيرها ولا تقتصر هذه الأنظمة على الأنشطة التجارية، بل حتى الحياة الشخصية لأنه يمكن تخزين أكبر قدر من البيانات على جهاز الحاسوب.

لذا، كان لابد من طريقة لتخزين وتنظيم هذه البيانات وإدارتها بشكل فعال، ومن هنا ظهر مفهوم قاعدة البيانات وتم إيجاد أنواع مختلفة من قواعد البيانات لكل منها منهجية مختلفة في تصميمها وطريقة تعاملها مع البيانات.

ولما كان من المسلَّم به أن الأنظمة المعلوماتية مهما تطورت فإنها تبقى عرضة لأصعب الاعتداءات وأكثرها دقةً.

كما أن موضوع جرائم الاعتداء على قواعد البيانات لمؤسسات القطاع العام أو القطاع الخاص في أية دولة يعتبر مثالاً حياً لجسامة ضرر الجريمة الالكترونية وتنوع أساليبها.

وقد أصبحت المواقع الالكترونية مستودعاً لأسرار الدول والجماعات والأفراد والمؤسسات العامة والخاصة، كما أن كثير من دول العالم اتجهت الى سياسة الحكومة الالكترونية وما يتبعها من نقل للمعلومات والبيانات عبر الشبكة المعلوماتية، وقد تطور الاعتداء ليصل الى قواعد

البيانات التي تسعى الدول في الحفاظ على سريتها لأنه يكلف الجهة المستهدفة خسائر كبيرة في كشف أسرارها والاعتداء على هيبتها وكيانها.

لذلك جاء هذا البحث متناولاً الحماية الجنائية من جرائم الاعتداء على قواعد البيانات.

أسباب اختيار الموضوع:

من أهم الأسباب التي دعتني لاختيار هذا الموضوع ما يأتي:

1- تسارع وتيرة التطور العلمي في مجال الحاسوب الذي شمل استخدامه في كافة مجالات الحياة.

2- اتساع نشاط المستخدمين للإنترنت أدى الى ظهور نوع جديد من الجرائم ترتكب باستخدام التكنلوجيا.

3- الحاجة الى المراجعة الدورية للتشريعات والقوانين التي تعمل على مكافحة جرائم الاعتداء على قواعد البيانات لتكون أكثر توافقاً مع التطورات التكنلوجية.

أهداف البحث:

1- توفير الحماية الجنائية من خطر الوقوع في هذه الجرائم

2- بيان مدى توافق التشريعات الجنائية العربية واتساقها في مجال الحماية الجنائية لقواعد البيانات مع الاتجاهات الدولية والإقليمية في هذا الشأن.

3- بيان مدى خطورة جريمة الاعتداء على قواعد البيانات في انتهاك سيادة الدول.

أهمية البحث:

تعد قاعدة البيانات مخزن للأسرار للمؤسسة سواء أكانت عامة أم خاصة وهي بمثابة مستودع أو حاوية للبيانات مثلاً تحتاج الجامعات إلى قواعد البيانات لتخزن كافة بيانات الطلاب وتخصصاتهم وتخزن ما درسوه من مواد وما حصلوا عليه من درجات في كل مادة ومعدلاتهم

تتعرض البيانات دائما إلى أنواع كثيره من الاعتداء كالإتلاف والاستيلاء **وتتمثل** أهمية هذا الموضوع في أن الاعتداء على قواعد البيانات من الجرائم تمس كيان الدولة، وهذا البحث يكشف المهددات الأمنية الخطيرة المتعلقة بأمن الدولة ومؤسساتها بسبب هذه الجريمة

مشكلة البحث:

تكمن مشكلة هذا البحث في الإجابة على التساؤلات الآتية:

1- ما الحماية الجنائية

2- ما نطاق الحماية الجنائية لقواعد البيانات

3- ما الأفعال التي تشكل اعتداء على قواعد البيانات

4- ما عقوبة الاعتداء على قواعد البيانات

منهج البحث:

سوف يتبع الباحث في دراسة هذا الموضوع المزج بين المنهج الوصفي والمنهج الاستقرائي التاريخي حيث أقوم ببيان مفهوم الحماية الجنائية لقواعد البيانات، والتحديات التي تقف أمام القضاء عليها، مع تحليل المادة العلمية والتعقيب عليها، مع تتبع المراحل التاريخية لمواجهتها من خلال القوانين الداخلية والاتفاقيات الدولية، كما، أنني أورد المعلومة من مصدرها الأصلي وأعزو كل قول الى قائله ما استطعت الى ذلك سبيلا.

خطة البحث:

المبحث الأول: مفهوم مصطلحات البحث

المطلب الأول: مفهوم الحماية الجنائية

الفرع الأول: تعريف الحماية الجنائية في اللغة والشرع والقانون

الفرع الثاني: أنواع الحماية الجنائية لقواعد البيانات

المطلب الثاني: مفهوم قواعد البيانات

الفرع الأول: تعريف قواعد البيانات في التشريعات الداخلية

الفرع الثاني: تعريف قواعد البيانات القوانين الأوروبية

المبحث الثاني: نطاق الحماية الجنائية لقواعد البيانات

المطلب الأول: المطلب الأول: قواعد البيانات الحكومية

المطلب الثاني: المطلب الثاني: قواعد البيانات الخاصة

المبحث الثالث: الأفعال التي تشكل جرائم على قواعد البيانات

المطلب الأول: جريمة الاعتداء على قواعد البيانات الخاصة بالدولة وعقوبتها

المطلب الثاني: جريمة الدخول غير المشروع على قواعد البيانات وعقوبتها

المبحث الأول

مفهوم مصطلحات البحث

من الصعوبة بمكان تحديد البيانات التي يجب حمايتها تحت مظلة التشريعات الجنائية على سبيل الحصر، لأنه يعتبر ضرب من الخيال، وتلك البيانات لا نستطيع حصرها، فتشعب وتعدد أنواع البيانات يجعل من الصعب تحديدها وتكمن الصعوبة الأكبر في تحديد ما هو مباح نشره وتداوله وما هو عكس ذلك حيث يحظر نشره أو تداوله، بل يعد من قام بهذا السلوك مرتكباً لجريمة فعدم تحديد معيار واضح يفرق بين المعلومات المباحة السلوك مرتكبا والمعلومات المشمولة بالحماية يجعل الصورة ضبابية وغير واضحة بالنسبة لعموم المواطنين، وعليه سوف أتناول هذا المبحث في مطلبين كالآتي:

المطلب الأول: تعريف الحماية الجنائية في اللغة والشرع والقانون:

الفرع الأول: تعريف الحماية الجنائية في اللغة:

أولاً: الحماية الجنائية في اللغة:

يقال: (حمى الشيء من الناس حمياً من باب رمى، وحمية بالكسر، منعته عنهم والحماية اسم منه) (الفيومي،1999م)

(وتتكون الجملة من مركب إضافي بيانه كالآتي:

أولاً: يقال حمى الشيء من الناس حمياً من باب رمى وحميه بالكسرة منعه عنهم والحماية اسم منه، وحماه يحميه حمية وحماية بالكسر، وحموه دفع عنه، وهذا شيء حمي أي محظور لا يقرب، وحمى المريض ما يغيره منعه إياه وتحمى امتنع والحمى كغني المريض الممنوع ما يغيره، والحمية بالكسر ما حمى من شيء والحامية الرجل يحمي أصحابه والجماعة أيضاً حامية، وهو على حامية القوم، أي آخر من يحميهم في مغيبهم، وأحميته بالألف جعلته حتى لا يقرب ولا يتجرأ عليه.

وفي الحديث (لا حمى إلا رسول الله) وأحميته بالألف أيضاً وجدته حمى، وتثنية الحمى حميان بكسر الحاء على لفظ الواحد وبالياء وسمع بالواو فيقال حموان، قاله ابن السكين وحميت المريض، حمية القوم حماية، نصرتهم) (2) (الشيرازي، 1371هـ)

ثانياً: الحماية الجنائية شرعاً: (هي إضفاء الحماية التشريعية للمصالح التي يتوخاها الشارع ويعبر عن ذلك بالجزاء الجنائي على الجرح والقطع، والجمع جنايات وقد وردت بمعنى الذنب أو الجرم نفسه تسميةً بالمصدر) (الفيومي، 1928)

ثالثاً: الحماية الجنائية قانوناً:

(يقصد بمصطلح الحماية الجنائية بصفة عامة، أن يدفع قانون العقوبات عن الحقوق والمصالح المحمية جميع الأفعال غير المشروعة التي تؤدي الى النيل منها بما يقرره لها من عقوبات)

(عبد القادر، 2020م)

أما المقصود بالحماية الجنائية في نطاق قواعد البيانات هو أن يدفع قانون العقوبات عن قواعد البيانات سائر الأفعال غير المشروعة خاصة جرائم سرقة البيانات واتلافها أو الدخول غير المشروع عليها.

الفرع الثاني: أنواع الحماية الجنائية لقواعد البيانات:

ان الحماية الجنائية في قانون الاجراءات تختلف عن الحماية الجنائية في قانون العقوبات حيث تستمد الحماية الجنائية في قانون الاجراءات عناصرها من قواعد قانون الاجراءات وهي القواعد التي تبحث في تنظيم جهات القضاء واختصاصاتها وكشف الجريمة وطرق إثباتها وضبط مرتكبيها والتحقيق معهم ومحاكمتهم وغيرها من القواعد الاجرائية وهي كذلك تقرر حق الدولة في العقاب ووجوب اعمال قواعد القانون الجنائي الاجرائية لاستيفاء هذا الحق

(أبو عامر 1985م)

وبالتالي نستطيع أن نقول إن حماية قواعد البيانات في القانون الجنائي مشمولة بحمايتين

أولاً: حماية موضوعية:

وتتمثل في النصوص المتعلقة بتجريم الاعتداء على قواعد البيانات في التشريعات الجنائية المختلفة والعقوبة على هذا الاعتداء. مثل القانون رقم 75 لسنة 2018م في جمهورية مصر

العربية وهو قانون مكافحة الجرائم المعلوماتية المصري وقد عاقب هذا القانون على جرائم الاعتداء على قواعد البيانات وذلك في المواد 1، 11، 12، 21، 38
ونظام مكافحة جرائم المعلوماتية في المملكة العربية لسنة 1428هـ مثل المادة 2/ 4 أو المادة 5 فقرة (1) و(2)

ثانياً: حماية إجرائية:

وتتمثل في كيفية اتباع الإجراءات المتعلقة بقواعد البيانات وتحديد الجهات التي تتولى التحقيق والمحاكمة فيها وهناك إجماع حول المنظور العالمي للجريمة الإلكترونية من حيث طبيعتها ونطاقها وارتباطها بشبكات دولية مما أثر على الاقتصاد العالمي والتنمية وقابليتها للانتشار السريع (البشرى، 2011م)

مما جعل التحقيق في الجرائم الإلكترونية يتميز عن التحقيق الجنائي في الجرائم التقليدية ويمكن بيان أهمها في الآتي:

1- يعد التحقيق في الجرائم الإلكترونية له ذاتية خاصة ومستقله مستمدة من الطبيعة الخاصة والمميزة للجريمة الإلكترونية عن الجريمة التقليدية فالتحقيق بها ال يعد استثناء على التحقق في العالم المادي فأكثر المساحات الافتراضية التي تنمو فيها الجريمة الإلكترونية هي بيئة شبكات الأنترنت وقواعد البيانات والبريد الإلكتروني والنقود الإلكترونية والتجارة الإلكترونية والأسهم والسندات والأنظمة الأمنية الحساسة ونشر الفيروسات والإرهاب الإلكتروني.

(البشرى، 2011م)

2- التحقيق في الجرائم الإلكترونية يتميز بتطور المفاهيم المستخدمة فيه فأصبح هنالكً مصطلحات جديدة تعد أكثر قربا وملائمة من البيئة الافتراضية والتقنية الذي تباشر فيه اجراءات التحقيق فمثالً استخدام مصطلح الولوج بدلاً عن مصطلح التفتيش واستخدام مصطلح النسخ بدلاً عن مصطلح الضبط وهذه المصطلحات تتلاءم مع البيئة الافتراضية عنها في الجرائم التقليدية (يونس 2004م)

فاذا كان التحقيق يعتمد على ذكاء المحقق وفطنته وقوة ملاحظته ومحاولته بكل جهد، يمكن أن يقوم بالتحقيق في الجريمة ومتابعتها والبحث عنها وصولاً للكشف عن الحقيقة فإنه يتطلب تطوير اساليبه من أجل مواكبة حركة الجريمة وتطور اساليب ارتكابها في البيئة الافتراضية (عبد المنعم 2005م)

3- غالباً ما يتخذ الدليل في الجرائم الالكترونية شكلاً مغايراً للشكل التقليدي للدليل فالجريمة التي ترتكب بواسطة الحاسوب تنشأ في الخفاء وينصب الاعتداء فيها على معطيات الحاسوب فالتعامل مع مسرح الجريمة الإلكترونية والتحفظ على الدليل يجعلها تتميز بالتحقيق عنها في الجرائم التقليدية وبالتالي يصعب على المحقق التقليدي أن يفهم حدودها الإجرامية وما تخلفه من آثار غير مرئية (الحلبي، 2011م).

4- التحقيق في الجرائم الإلكترونية يختلف عن التحقيق في الجرائم التقليدية إذ يصعب توضيحها لهيئة المحكمة ويسهل زرع الشك في وجدانها ويرجع ذلك إلى صعوبة إدراك المفاهيم التي يشملها موضوع التحقيق والبحث محل الادعاء سيما عدم وجود سلطات تحقيق ومحاكمة متخصصة للتحقيق والفصل في الجريمة الإلكترونية (المراغي،2017م).

المطلب الثاني: مفهوم قواعد البيانات:

يعود مفهوم قواعد البيانات إلى ستينيات القرن الماضي (1960 م)، عندما أصبحت أجهزة الحاسوب أكثر قوة وقدرة على معالجة كميات كبيرة من البيانات، والنوع الأول من قواعد البيانات التي ظهرت هو قاعدة البيانات الهرمية (hierarchical database). على سبيل المثال، يمكن أن تحتوي قاعدة بيانات الهرمية لشركة على سجل للمدير التنفيذي (CEO) يحتوي على سجلات للمديرين الآخرين كعناصر فرعية (children) والتي تحتوي على سجلات للموظفين كعناصر فرعية (children)، وهكذا. (2) ويأتي هذا المطلب في فرعين:

الفرع الأول: تعريف قواعد البيانات في التشريعات الداخلية:

قاعدة البيانات هي مجموعة منظّمة من المعلومات المهيكلة أو البيانات المخزّنة عادةً بصيغة إلكترونيّة أو في نظام حاسوب، وعادةً ما تكون قاعدة البيانات تحت تحكم نظام إدارة قاعدة

بيانات (DBMS)، ومعًا تتم الإشارة إلى البيانات ونظام إدارة قواعد البيانات جنبًا إلى جنب مع التطبيقات المرتبطة بها باعتبارها نظام قواعد بيانات وغالبًا ما يتم اختصاره إلى قاعدة بيانات فقط. (https://almdrasa.com/)

وكانت قواعد بيانات التنقل مثل قواعد البيانات الهرمية (والتي اعتمدت على نموذج شبيه بالشجرة وسمحت فقط بعلاقة من واحد لكثير)، وقواعد البيانات الشبكية (وهي نموذج أكثر مرونة سمح بعلاقات متعددة) الأنظمة الوحيدة المُستخدمة في تخزين البيانات ومعالجتها. وبالرغم من بساطتها، فإن هذه الأنظمة المبكرة لم تكن تتسم بالمرونة، في الثمانينيات، أصبحت قواعد البيانات الترابطية شائعةً، تليها قواعد البيانات كائنية التوجه في عقد التسعينيات. ومؤخرًا، ظهرت قواعد بيانات NoSQL نتيجةً لنمو الإنترنت والحاجة إلى سرعة أكبر ومعالجة البيانات غير المنظّمة بشكل أسرع. واليوم، تكسب قواعد البيانات السحابية وقواعد البيانات الذاتية التشغيل أرضية جديدة عندما يتعلق الأمر بكيفية جمع البيانات وتخزينها وإدارتها والاستفادة منها (https://www.oracle.com/)

وإذا أردنا أن نعرف قواعد البيانات في التشريعات الداخلية للدول العربية يمكننا أن نورد بعض التشريعات مع أن جميع التشريعات لا تخرج عن المعنى العام الذي ورد في تعريف قواعد البيانات.

فالمشرع الأردني مثلاً لم يورد لها تعريفاً محدداً تاركاً الأمر لاجتهادات الفقه والقضاء وذلك على خلاف الوضع القائم في التشريعات المقارنة والتي تضمنت نصوصها وضعاً تعريفياً لقواعد البيانات. (https://jordan-lawyer.com/2021)

أما في المملكة العربية السعودية فنجد أنها ركَّزت منذ عام 2020 على أهمية سنّ تشريعات متخصّصة لحماية البيانات وإنفاذها، ولكنها لم تورد تعريفاً محدداً لقواعد البيانات مكتفيةً بما ورد في الفقه والقضاء في هذا الشأن وقد وأدى تزايد الوعي بحماية بيانات الأفراد وحقوق الوصول للبيانات وملكيتها إلى نشوء تحديات جديدة تؤثر على الشركات داخل المملكة وخارجها. وتماشيًا مع العديد من الأنظمة القانونية في المنطقة، تنص الأحكام العامة للنظام السعودي على حماية خصوصية الأفراد وبياناتهم الشخصية عوضًا عن سنّ تشريعات

مخصّصة لمسألة "خصوصية البيانات" أو "حماية البيانات". (https: / /www.my.gov.sa)

وفي مصر فإن قواعد البيانات لم تنل حظا وافراً من التعريف وباستعراض آليات حمايتها التشريعية والحقوق المتعلقة بها، نجد أن المشرع لم يعن بتعريفها ولا بوضع النظام القانوني الخاص بها إلى أن ظهرت قواعد البيانات الإلكترونية الحديثة التي لم تترك مجالاً من مجال التكنولوجيا والتقنيات الحديثة إلا وغزته (السيد، 2004م)

لكننا نجد أن المشرع المصري عرف قواعد البيانات بوصفها مصنفاً محمياً بقانون حق المؤلف بأنها: (أي تجميع للبيانات يتميز بالابتكار في الترتيب والعرض أو يعكس مجهوداً شخصياً جديراً بالحماية، سواءً كان هذا التجميع بلغة، أم رمز، أم بأي شكل آخر على أن يكون مخزناً بواسطة الحاسب الآلي وقابلاً للاسترجاع بواسطته أو بأية وسيلة الكترونية أخرى)

أما في القانون السوداني فإنه لم يعرف قواعد البيانات كذلك، ولكنه رتب اثرا قانونيا على عدم الالتزام بذلك، فانه أوجب القانون ان تكون المعلومات ثابتة بالكتابة، واستخراجها لاحقا عن طريق البث أ والطباعة أو غير ذلك، المعلومات في سجل الكتروني يفي بمتطلبات هذا القانون بشرط أن تكون المعلومات قابلة للوصول اليها

الفرع الثاني: تعريف قواعد البيانات القوانين العالمية:

عرفها المشرع الألماني في المادة (4) من قانون حماية حق المؤلف بأنها (تجميع لأعمال أو بيانات لأي عناصر منفصلة أو منظمة على نحو منهجي أو بشكل معين وتمكن الوصول لعناصر هذا التجميع بشكل فردي إما من خلال الوسائل الالكترونية أو بأية وسيلة أخرى) (https: / /jordan-lawyer.com /2021)

أما المشرع الفرنسي فقد عرفها في المادة (1) من القانون رقم 98/ 536 لسنة 1998م بأنها مجموعة المصنفات أو العناصر الأخرى المستقلة يجري ترتيبها وتخزينها بصورة منظمة ومنهجية والتي يمكن الوصول اليها واسترجاع المعلومات منها بالوسائل الالكترونية أو بأية وسيلة أخرى)

وتم تعريفها أيضاً بموجب المادة الأولى من الميثاق الأوروبي الجديد الصادر بالقانون رقم 24/ 9 بأنها (مجموعة المصنفات أو المعلومات أو أي عناصر أخرى معدَّة بطريقة منسقة ومنظمة تدار بواسطة نظام إلكتروني أو أي نظام آخر) (الميثاق الأوروبي الجديد رقم 24/ 9)، أما المشرع الأمريكي فإنه يعدها نوعاً من مصنفات التجميع والذي يعرفها بأنها: (مصنف تم تكوينه من خلال تجميع وتنسيق مواد، أو بيانات مختارة، أو معدة، أو منظمة على نحو يجعل من المصنف الناتج بأكمله مصنفاً مبتكراً) (4)

ومن خلال ما تقدم يرى الباحث أنه لا بد للمشرع في الدول العربية أن يسير على ما سار عليه المشرع في دول العالم المتقدم في تعريف قاعد البيانات لأن تعريفها بصورة دقيقة يمنحها حماية من التعدي عليها أو التلاعب بها

المبحث الثاني

نطاق الحماية الجنائية لقواعد البيانات

لهذه الثورة المعلوماتية والتكنولوجية إيجابيات لو استخدمت في نفع الانسان، لكنها أحيانا وباستخدامها في غير ذلك تشكل تهديداً خطيراً للبشرية مثل الاعتداء على قواعد البيانات بإتلافها مثلاً أو الدخول غير المشروع عليها الأمر الذي نتج عنه خلق جرائم مستحدثة غير معتادة عكست هذا الواقع تنال الحق في المعلومات، مما يستدعي مواجهة أخطار الاعتداء على وسائل تقنية المعلومات، لذلك تبدوا أهمية البحث في إظهار جوانب الحماية الجنائية لقواعد البيانات من الاعتداءات التي يمكن أن تقع عليها.

وقد أكد البحث في نطاق الحماية الجنائية لقواعد البيانات على شمول محتويات قواعد البيانات ومضمونها بالحماية متى كانت في مضمونها وترتيبها تمثل جهداً مبتكراً وذلك بعد أن كشف البحث عن الموقف التشريعي من حمايتها في التشريعات محل الدراسة، كما تم تحديد الأفعال التي تشكل اعتداء عليها سواء ممن ساهم فيها أو من قبل الغير، وبعد أن بينا مدلولها وركزنا على الاتجاه التشريعي الذي يعالج موضوع هذه الحماية الجنائية نتناول في هذا المبحث نطاق الحماية الجنائية في مطلبين كالآتي:

المطلب الأول: قواعد البيانات الحكومية:

يشمل نطاق الحماية الجنائية لقواعد البيانات الرسمية (الحكومية) وغير الرسمية وهي قواعد بيانات القطاع الخاص

وتعد قواعد البيانات الحكومية هي اللاعب الرئيس في التحول الرقمي والانتقال من مفهوم الحكومة التقليدية إلى مفهوم الحكومة الإلكترونية والحكومة الذكية، والذي اضحى ضرورة في بلداننا العربية على وجه الخصوص والتي تقوم بإنتاج كمية كبيرة من البيانات يمكن استخدامها في تطوير البنية التحتية وتنمية مختلف القطاعات كالاقتصاد والصحة والتعليم. وتقوم الجهات الحكومية المختلفة بإنتاج وتجميع كميات ضخمة من البيانات التي تشمل شتى جوانب الحياة فتتنوع البيانات ما بين بيانات قانونية وبيانات متعلقة بالصحة والتعليم وبيانات جغرافية وإحصاءات العمالة والتوظيف ... إلخ وهذه البيانات الحكومية قد تكون ذات قيمة كبيرة للمؤسسات غير الحكومية، ومنظمات المجتمع المدني، والقطاع الخاص، والمواطنين الذين يمكنهم استخدامها لأغراض سياسية، وتجارية.

وقد اتجهت الحكومات في السنوات الأخيرة لنشر تلك البيانات الحكومية على الإنترنت معتمدة على استثمار التطور في تكنولوجيا المعلومات والاتصالات وبموجب رخصة مفتوحة تسمح لأي شخص أن يقوم باستخدامها، وإعادة استخدامها ومعالجتها، وإعادة توزيعها دون قيود قانونية أو تقنية بشرط الإشارة إلى مصدرها (1) (بحوث القانون والتكنولوجيا، ،2020م)

وبالتالي لا يجوز لأي شخص القيام بأي تصرف دون إذن كتابي أو تفويض رسمي بالدخول على قواعد بيانات حكومية واستنساخها مثلاً سواءً كانت بصورة دائمة أو مؤقتة لأن قواعد البيانات الحكومية تعد من المصنفات الفكرية التي تخضع للحماية الجنائية (جميعي، 2024م) وقد عرف قانون مكافحة جرائم تقنية المعلومات رقم 75 لسنة 2018 البيانات الحكومية بأنها بيانات متعلقة بالدولة، أو إحدى سلطاتها، أو أجهزتها، أو وحداتها، أو الهيئات العامة، أو الهيئات المستقلة، أو الأجهزة الرقابية، أو غيرها من الأشخاص الاعتبارية العامة وما في

حكمها، والمتاحة على الشبكة المعلوماتية أو على أي نظام معلوماتي أو على حاسب أو ما في حكمها (2018 https://manshurat.org)

وهناك قواعد بيانات حكومية تسمح القوانين بالدخول على بياناتها والاطلاع عليها ونشرها مثل البيانات المتعلقة بالموازنة المالية للدولة ومعلومات الصحة ومعلومات البيانات الجغرافية وقواعد بيانات القوانين، كما أن هناك قواعد بيانات لا يسمح الدخول عليها ولا نشرها ولا تداولها مثل البيانات المتعلقة بالأمن القومي.

وقد تبنت الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) سياسة تحدد الأطر التنظيمية للبيانات المفتوحة.

كما قام مكتب إدارة البيانات الوطنية بإصدار ضوابط ومواصفات إدارة البيانات الوطنية وحوكمتها وحماية البيانات الشخصية

وتحتوي قواعد البيانات على مجموعة البيانات المفتوحة مختلفة المحتوى (صور، مواد سمعية وبصرية، ومواد صوتية على سبيل المثال)، وبالتالي فإن هذه الرخصة تحكم حقوق قاعدة البيانات فقط وليس محتوى قاعدة البيانات بشكل فردي.

كما يتم تنبيه المستخدم بأن محتويات قاعدة البيانات، أو قاعدة البيانات نفسها، قد تشتمل على حقوق أخرى لم يتم تناولها هنا (مثل العقود الخاصة أو العلامات التجارية على الاسم أو حقوق الخصوصية / حماية البيانات على المعلومات الواردة في المحتوى)، وأنه قد يحتاج إلى الرجوع إلى وثائق أخرى أو استيفاء شروط أخرى قبل الانخراط في أنشطة لا تغطيها رخصة البيانات المفتوحة. (https://www.my.gov.sa)

المطلب الثاني: قواعد البيانات الخاصة:

ساهمت ثورة تكنلوجيا المعلومات بشكل فعال في التحكم في كل ما يخص البشر لا سيما ما يتعلق بخصوصياتهم التي هي محل حماية من الأساس، وقد تطرق الأمر الى أدق تفاصيل الانسان، بل ونشرها وانتقالها ليس فقط بشكل محلي، بل متجاوزةً حدود الدولة دون اعتبار للزمان والمكان وأصناف المطلعين على هذه الخصوصية (المحروقي2018م)

وقد تستلزم حماية قواعد البيانات الخاصة عقد موازنة مع المصالح الخاصة مثل الحق في حرية الصحافة وحرية الوصول للمعلومات وكذلك المصالح العامة كالأمن القومي والتزامات التعاون القضائي والشرطي في المسائل الجنائية، خاصة ما يتعلق بمجال الحرية والأمن والعدالة. (https: / /www.my.gov.sa)

وتمثل قواعد البيانات الخاصة عاملاً مهماً لجودة أعمال المؤسسات الخاصة من حيث الامكانيات والتسهيلات التي تقدمها قواعد البيانات لبيئة العمل وقد تشكل خطرا كبيرا إذا تعرضت للاختراق لذا يجب علينا التركيز على مثل هذه الامور واخذها بمحمل الجد وعمل الإجراءات اللازمة لحمايتها.

وتختلف الادوار التي تلعبها قواعد البيانات في بيئة الاعمال بحسب طبيعة العمل والبيئة التي ستعمل بها وكذلك درجة حساسية البيانات التي تخزن فيها بالإضافة الى امكانية الوصول الى تلك البيانات سواء كانت محلية او قواعد بيانات عبر الانترنت يتم الوصول اليها من عدة جهات أو اشخاص مختلفين وكذلك مدي اهمية الوصول الى تلك البيانات في اوقات محددة فعدم اتاحة قواعد البيانات في الوقت الحقيقي قد يؤثر بشكل كبير على بعض بيئيات الاعمال التي يعتبر الوقت بها عامل اساسي لنجاح اعمالها كأسواق التجارة الالكترونية وقواعد بيانات حجوزات شركات الطيران وانظمة المراسلات الفورية وكذلك المعاملات الالكترونية الخاصة بالمنشئات الحكومية وايضا العمليات المالية التي تعتبر حساسة جدا لدرجه الامان والسرية.

كل هذه الامور تؤثر على الدور الذي قد تلعبه قواعد البيانات في بيئة العمل فلو اخذنا مثلا اسواق التجارة الالكترونية فالدور الذي تلعبه قاعدة البيانات في بيئة عمل التجارة

الالكترونية دورا رئيسيا فبدونها لن تكون هناك تجارة الكترونية لان كافة بيانات المنتجات والأسعار والكميات يجب أن تكون مخزنة ضمن قواعد البيانات فلذلك لا يمكن الاستغناء عن قاعدة البيانات في بيئة اعمال التجارة الالكترونية وكذلك العكس بالنسبة لمتجر صغير يبيع بعض المنتجات بشكل تقليدي، ومن هنا نستنتج ان التطور التكنولوجي ادى الى تغيير الادوار التي تلعبها قواعد البيانات في بيئة الاعمال. (https: / /nano2soft.com)

المبحث الثالث

الأفعال التي تشكل اعتداء على قواعد البيانات

كما ذكرنا سابقاً أن قواعد البيانات من الأمور الضرورية التي لا غنى عنها في المؤسسات العامة والخاصة لأنها تحتوي على معلومات مهمة حول العمل وأقسام المؤسسات ومع التطوّر الكبير والهائل في التقنيات المُستعملة، ومع زيادة التّعويل والاعتماد على شبكة الإنترنت، لا بد من سن تشريعات رادعة لحفظ قواعد البيانات من الأفعال التي تشكل اعتداء عليها وعليه سوف نتناول هذا المبحث في المطالب التالية:

المطلب الأول: جريمة الاعتداء على قواعد البيانات الخاصة بالدولة وعقوبتها:

تعد جرائم الاعتداء على قواعد البيانات من الجرائم التي انتجها التقدم التكنلوجي الحديث وهي من الجرائم ذات الطبيعة الخاصة لأنها تشكل اعتداء على سلامة الشبكات وأنظمة تقنية المعلومات في المؤسسات العامة والخاصة.

فقد جرمها معظم المشرعين على مستوى العالم، لما تنطوي على خطورة من إتلاف أو تعطيل أو إلغاء الإرسال، وغيرها من وسائل الاعتداء. كما جرم المشرع الاعتداء على البريد الالكتروني أو الموقع أو الحسابات الخاصة، والتي تمثل أيضاً اعتداء قواعد البيانات أو سلامة شبكات المعلومات وأنظمة تقنية المعلومات سواءً كان بريداً الكترونياً أو موقعاً أو حساباً خاصاً بآحاد الناس، أم بريد الكتروني أو موقع أو حساب خاص بأحد الأشخاص الاعتبارية الخاصة وقد شدد المشرع العقوبة على مثل هذا الاعتداء. (الدريني، 2021م)

وقد عاقب المشرع المصري في قانون مكافحة تقنية المعلومات على جرائم الاعتداء على قواعد البيانات وذلك في المادة 17 والتي تنص على أنه: (يعاقب بالحبس مدة لا تقل عن سنتين

وبغرامة لا تقل عن 100 ألف جنيه أو بإحدى العقوبتين، كل من أتلف أو عطل أو عدل مسار أوألغى كلياً أو جزئياً متعمداً وبدون وجه حق البرامج والبيانات أو المعلومات المخزنة، أو المعالجة أو المولدة أو المخلقة على أي نظام معلوماتي وما في حكمه، أيا كانت الوسيلة التي استخدمت في الجريمة (https: / /manshurat.org 2018 /)

ونجد هنا أن المشرع المصري جعل لقواعد البيانات وغيرها حماية جنائية قوية بالمعاقبة على كل من تثبت عليه جريمة الاعتداء على البيانات أو قواعد البيانات.

أما في القانون الإماراتي فقد نصت المادة 6 من المرسوم بقانون مكافحة الشائعات والجرائم الإلكترونية، في بندها الأول بأنه (يعاقب بالحبس مدة لا تقل عن 6 أشهر والغرامة التي لا تقل عن 20 ألف درهم ولا تزيد على 100 ألف درهم، أو بإحدى هاتين العقوبتين، كل من حصل أو استحوذ أو عدل أو أتلف أو أفشى أو سرب أو ألغى أو حذف أو نسخ أو نشر أو أعاد نشر بغير تصريح بيانات أو معلومات شخصية إلكترونية، باستخدام تقنية المعلومات أو وسيلة تقنية معلومات) (https: / /uaelegislation.gov2021)

وقد نصت المادة (7) الاعتداء على البيانات والمعلومات الحكومية

1. يعاقب بالسجن المؤقت مدة لا تقل عن (7) سبع سنوات والغرامة التي لا تقل عن (500،000) خمسمائة ألف درهم ولا تزيد على (3،000،000) ثلاثة ملايين درهم كل من حصل أو استحوذ أو عدل أو أتلف أو أفشى أو سرب أو ألغى أو حذف أو نسخ أو نشر أو أعاد نشر بغير تصريح بيانات أو معلومات حكومية سرية.

2. وتكون العقوبة السجن المؤقت مدة لا تقل عن (10) سنوات والغرامة التي لا تقل عن (500،000) خمسمائة ألف درهم ولا تزيد على (5،000،000) خمسة ملايين درهم إذا ترتب على الأفعال المنصوص عليها بالبند (1) من هذه المادة أضراراً للدولة، أو إذا ترتب عليها فقدان سرية عمل الأنظمة والبرمجيات الإلكترونية الخاصة بالمنشآت العسكرية والأمنية وما يتعلق بالاتصال ونقل المعلومات السرية.

3 . ويعاقب بالسجن المؤقت كل من تلقى أي من البيانات والمعلومات المشار إليها بالبند (1) من هذه المادة، واحتفظ بها أو خزنها أو قبل التعامل بها أو استخدامها رغم علمه بعدم مشروعية الحصول عليها.

كذلك نصت المادة (8) الاعتداء على بيانات المنشآت المالية أو التجارية أو الاقتصادية يعاقب بالسجن المؤقت مدة لا تقل عن (5) خمس سنوات والغرامة التي لا تقل عن (500،000) خمسمائة ألف درهم ولا تزيد على (3،000،000) ثلاثة ملايين درهم كل من حصل أو استحوذ أو عدل أو أتلف أو أفشى أو سرب أو ألغى أو حذف، أو غير أو نسخ أو نشر أو أعاد نشر بغير تصريح معلومات أو بيانات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية باستخدام تقنية المعلومات أو وسيلة تقنية معلومات.

أما في المملكة العربية السعودية فإننا نجد أن نظام مكافحة جرائم المعلوماتية نص في المادة الخامسة الفقرة الثانية على أنه (إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها) (https: / /laws.boe.gov.sa2021/)

وما دام الهدف الرئيسي لقاعدة البيانات هو تصميم البيانات بحيث تكون خالية من التكرار ويمكن استرجاعها وتعديلها والإضافة عليها دون المشاكل التي يمكن أن تحدث مع وجود التكرار فيها، لذلك تُساعد قواعد البيانات وبشكل كبير على تسريع عمليّة الوصول إلى البيانات التي تتضمّنها بالتالي أضفت عليها القوانين الجنائية حماية بالعقوبات الرادعة عند ثبوت الاعتداء عليها.

ويقع التعدي على قواعد البيانات بسرقتها أو اتلافها، أما سرقة قواعد البيانات وعلى الرغم من أنها صورة من صور التعدي لكن هناك رأي في الفقه يرى أن قواعد البيانات لا تصلح أن تكون محلاً لجريمة السرقة فهي ليست بمال منقول لكن الفقه الفرنسي يرى أنها تصلح للسرقة لأن سرقة البيانات هنا لا تعني السرقة بالمعنى الدقيق فليس شرطا في الفقه الفرنسي أن يخرج المال من ذمة المجني عليه ويدخل في ذمة الجاني، بل المقصود بالسرقة هنا الاستنساخ لقواعد البيانات دول الحصول على إذن من صاحبها.

أما جريمة اتلاف قواعد البيانات فهي المحو أو الطمس أو وضع عوائق من شأنها أن تؤثر في أداء قواعد البيانات مما يترتب عليه إهدار للجهد الذهني
(https: / /jordan-lawyer.com /2021)

المطلب الثاني: جريمة الدخول غير المشروع على قواعد البيانات وعقوبتها:

الهدف من سن قوانين مكافحة الجرائم الإلكترونية في الدول العربية وغيرها هو حفظ حقوق الأفراد المادية والمعنوية وحرياتهم في العالم الافتراضي للشبكات الإلكترونية وذلك من خلال تجريم أفعال الدخول غير المشروع على تلك الحقوق ووضع ضوابط وإجراءات لضبط تلك الأفعال.

والدخول غير المشروع يقصد به الدخول إلى نظام معلومات أو قواعد بيانات أو إلى موقع الكتروني من قبل شخص غير مخول له بالدخول، فينتهز الفاعل هذه الفرصة للاطلاع على قواعد بيانات أو ملفات سرية دون وجه حق.

وقد نصت المادة (1) الفقرة (7) من نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية على تعريف الدخول غير المشروع كجريمة الكترونية بالآتي:

(الدخول غير المشروع: دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع إلكتروني، أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها)
(https: / /laws.boe.gov.sa)

وقد تطور هذا الاعتداء على المواقع الرسمية للدول الصغيرة والكبيرة وأصبح الدخول غير المشروع يكلف الدول المستهدفة خسائر كبيرة تتمثل في كشف أسرارها والاعتداء على هيبتها وكيانها.

ويعد الدخول غير مشروع متى كان ذلك مخالفا لإرادة صاحب النظام أو من له حق السيطرة عليه، ومن الأمثلة على ذلك، تلك الأنشطة المتعلقة بأسرار الدولة أو التي تتضمن بيانات شخصية تتعلق بحرمة الحياة الخاصة ولا يجوز الاطلاع عليها

إن جريمة الدخول غير المشروع على قواعد البيانات تقوم على السلوك الاجرامي عبر الانترنت ويعتبر هذا السلوك مجرماً في كافة الأنظمة المقارنة التي جرمته إلا إن مفهومه يمثل

محل خلاف فِي الأنظمة والفقه والقضاء لا سيما إن النشاط أو السلوك المادي يختلف عما هو الحال فِي العالم المادي، فارتكابها عبر الإنترنت يحتاج بالضرورة إلى منطق تقني وبدونه لا يمكن للشخص حتى الاتصال بالإنترنت، سواء كان يقصد ارتكابها أو لمجرد التصفح أو الدخول فِي الاتصال المباشر كالمحادثة وغيرها، وجريمة الدخول غير المشروع لموقع إلكتروني أو نظام معلوماتي أو شبكة معلوماتية أو قواعد بيانات هي جريمة عمدية، يتمثل ركنها المادي في الدخول بأي وسيلة إلى موقع إلكتروني، أو نظام معلوماتي، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، أو جزء منها، أو تجاوز الدخول المصرح به، أو الاستمرار في التواجد بها بعد العلم بذلك.

(https://al-sharq.com/opinion/31/05/2023/)

ويجب لقيام الجريمة أن يكون الدخول بغير وجه حق. وتختلف هذه الجريمة عن سابقتها في أنها لا تختص فقط بالمواقع والأنظمة التابعة للدولة، بل تشمل جميع المواقع والنظم والشبكات المعلوماتية، كما أنه في هذه الجريمة يتساوى الدخول غير المشروع مع تجاوز حدود الدخول المصرح به أو الاستمرار في التواجد بعد علمه بهذا التجاوز رغم عدم تعمده ذلك في البداية.

وعلى أية حال المجتمعات الآن تعيش في عصر البيانات التي يتم تحويلها فيما بعد الى معلومات قد تستخدم ضد الدولة بعد عمليات جمع تلك البيانات المتفرقة، وفهمها وتحليلها وادراكها.

وفي الوقت الحاضر ومع انتشار ثورة المعلومات وتوالي الاحداث وسرعتها نحتاج الى انظمة قواعد بيانات والتي في القلب منها كما أشرنا سابقا تقع قواعد البيانات كما نحتاج الى قوانين صارمة ذات عقوبات رادعة تمثل حماية جنائية لمواجهة الدخول غير المشروع على هذه البيانات فالعقوبات في بعض التشريعات في الدول العربية تكاد تكون غير رادعة ولذلك سوف نستعرض بعض التشريعات التي تعاقب على هذه الجريمة كالآتي:

أولاً: نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية لعام 1428هـ نص في المادة (3) الفقرة (3) على أنه: يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على

خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين؛ كلُّ شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

(الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع الكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه) (https: / /laws.boe.gov.sa/)

وهنا الدخول غير المشروع على قاعدة بيانات وفقاً للنظام عاقب عليه المنظم السعودي بالسجن مدة لا تجاوز سنة وبغرامة لا تزيد على خمسمائة ألف ريال وفي رأينا أن هذه العقوبة غير رادعة ولا تؤدي الغرض المطلوب لأن هذه الجريمة من الجرائم التي تمس كيان الدولة في أمن معلوماتها.

أما المشرع المصري فنجد أنه عاقب على هذه الجريمة كذلك بسنة واحدة وغرامة لا تقل عن خمسين ألف جنيه وذلك في المادة 14 من قانون مكافحة جرائم تقنية المعلومات وهي كالآتي:

(يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مئة ألف جنيه أو بإحدى هاتين العقوبتين، كل دخل عمداً أو دخل بخطأ غير عمدي وبقي بدون وجه حق على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه.

فإذا نتج عن ذلك الدخول اتلاف، أو محو، أو تغيير، أو نسخ، أو إعادة نشر للبيانات، أو المعلومات على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي، تكون العقوبة الحبس مدة لا تقل عن سنتين وغرامة لا تقل عن مئة ألف جنيه ولا تجاوز مائتي ألف جنيه أو بإحدى هاتين العقوبتين (2018 https: / /manshurat.org/)

ورغم أهمية هذا القانون للمشرع المصري في مكافحة هذه الجريمة إلا أن الباحث يرى أن عقوبتها تعتبر غير رادعة فجريمة مثل هذه يجب أن تتجاوز عقوبتها الخمس سنوات سجن والغرامة أقل شيء يجب أن تجاوز مبلغ الخمسمائة ألف ريال.

وفي التشريع السوداني عاقب المشرع على جريمة الدخول غير المشروع في المادة (4) من قانون مكافحة الجرائم المعلوماتية لسنة 2007م بالآتي:

كل من يدخل موقعاً أو نظام معلومات دون أن يكون مصرحاً له ويقوم :(أ) بالاطلاع عليه أو نسخه يعاقب بالسجن مدة لا تجاوز سنتين أو بالغرامة أو بالعقوبتين معاً.

(ب) بإلغاء بيانات، أو معلومات ملكا للغير، أو حذفها، أو تدميرها، أو إفشائها، أو إتلافها، أو تغييرها، أو إعادة نشرها، أو تغيير تصاميم الموقع، أو إلغائه، أو شغل عنوانه، يعاقب بالسجن مدة لا تجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معاً.

كما نصت المادة (5) على دخول المواقع وأنظمة المعلومات من موظف عام.

كل موظف عام، يدخل بدون تفويض موقع أو نظام معلومات خاص بالجهة التي يعمل بها أو يسهل ذلك للغير، يعاقب بالسجن مدة لا تتجاوز خمس سنوات أو بالغرامة أو بالعقوبتين معا. (https: / /www.google.com /search?q=1- A+2007)

وفي قانون مكافحة الشائعات والجرائم الالكترونية الإماراتي نجد أنه عاقب على جريمة الدخول غير المشرع على قواعد البيانات في المادة (9) بالآتي:

وتكون العقوبة الحبس مدة لا تقل عن (6) ستة أشهر والغرامة التي لا تقل عن (300،000) ثلاثمائة ألف درهم ولا تزيد على (500،000) خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين، إذا قام من حصل بغير تصريح أو إذن من صاحب الرقم سري، أو الشفرة أو كلمة المرور أو ما في حكمها بالدخول، أو مكن غيره من الدخول على الموقع الإلكتروني، أو نظام المعلومات الإلكتروني، أو الشبكة المعلوماتية، أو وسيلة تقنية المعلومات بقصد ارتكاب جريمة. (2) (https: / /uaelegislation.gov2021)

الخاتمة:

وبعد أن استعرضنا الحماية الجنائية لقواعد البيانات يتبين للباحث مدى اهمية قواعد البيانات وانظمة المعلومات والمعرفة في عالمنا اليوم وعلينا ان نحث الخطى في هذا المجال لكي نلحق بركب الدول المتقدمة نختم هذا البحث بأهم النتائج والتوصيات كالآتي:

أولاً: النتائج:

1- الهدف من سن قوانين مكافحة الجرائم الإلكترونية في الدول العربية وغيرها هو حفظ حقوق الأفراد المادية والمعنوية وحرياتهم في العالم الافتراضي.

2- صعوبة تحديد البيانات التي يجب حمايتها تحت مظلة التشريعات الجنائية على سبيل الحصر

3- اتساع نشاط المستخدمين للإنترنت أدى الى ظهور نوع جديد من الجرائم ترتكب باستخدام التكنلوجيا مثل جريمة اتلاف قواعد البيانات أو سرقتها

4- قواعد البيانات مشمولة بالحماية القانونية متى ما كان مضمونها جهداً مبتكراً وذلك بعد أن كشف البحث عن الموقف التشريعي في الدول العربية من حمايتها.

5- اتجهت الحكومات في السنوات الأخيرة لنشر تلك البيانات الحكومية على الإنترنت معتمدة على استثمار التطور في تكنولوجيا المعلومات والاتصالات وبموجب رخصة مفتوحة تسمح لأي شخص أن يقوم باستخدامها.

6- جرائم الاعتداء على قواعد البيانات من الجرائم ذات الطبيعة الخاصة لأنها تشكل اعتداء على سلامة الشبكات وأنظمة تقنية المعلومات في المؤسسات العامة والخاصة

7- كلما ذادت قواعد البيانات ازدادت أهمية معالجتها وحمايتها وترجع أهمية هذه الحماية للمؤسسات القائمة على الحماية من الأنشطة غير المشروعة

ثانياً: التوصيات: يوصي الباحث بالآتي:

1- العمل على توفير آليات فعالة لضمان أمن وسلامة قواعد البيانات من التعدي عليها أو الدخول غير المشروع.

2- يجب أن تتبنى التشريعات في الدول العربية صياغة قوانين قوية تحمي قواعد البيانات وذلك بتشديد العقوبة في حال التعدي عليها أو الدخول غير المشروع

3- الحكم بمصادرة الأدوات المستخدمة في جريمة التعدي أو الدخول غير المشروع على قواعد البيانات لأن هذا الاجراء غفلت عنه كثير من التشريعات

4- تبصير المواطنين بأهمية قواعد البيانات وحمايتها لأن التعدي عليها قد يسبب ضرراً كبيراً يلحق بهم وذلك من خلال الجهات المعنية كأجهزة الاعلام

5- عند تحديد قواعد البيانات التي تستثنى من المنع للاطلاع عليها يجب أن تخضع لتقييم المصلحة والضرر المترتب على الاستثناء.

المراجع والمصادر:

1. احمد بن محمد الفيومي، المصباح المنير، بيروت، المكتبة العربية، ط3، 1999م
2. أبو طاهر مجد الدين محمد بن يعقوب الشيرازي، الفيروز آبادي، ط2، 1371هـ
3. احمد بن محمد الفيومي، المصباح المنير، ج1، ط2، 1928م
4. د. اقصاص عبد القادر، الحماية الجنائية لحق الطفل في الحياة والسلامة البدنية، مجلة الدراسات القانونية والاقتصادية، الجزائر، 2020م
5. محمد زكي ابو عامر، الحماية الاجرائية للموظف العام في التشريع المصري، الناشر، الإسكندرية الفنية للطباعة والنشر، 1985م
6. د. محمد الأمين البشري، "الأساليب الحديثة للتعامل مع الجرائم المستحدثة من طرف أجهزة العدالة الجنائية"، تحليل الجرائم المستحدثة والسلوك الإجرامي، 2011م
7. عمر محمد أبوبكر يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراه كلية الحقوق جامعة عين شمس 2004
8. محمد صلاح عبد المنعم، الجرائم الالكترونية وتحدياتها، دراسة مقارنة، رسالة دكتوراه، 2005م،
9. خالد عياد الحلبي، اجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، والأردن، 2011م
10. أحمد عبد الاله المراغي "الجريمة الالكترونية ودور القانون الجنائي في الحد منها- دراسة تحليلية تأصيلية مقارنة"، المركز القومي للإصدارات القانونية، القاهرة 2017م
11. فارس محمد السيد، النظام القانوني لقواعد البيانات الإلكترونية، دراسة مقارنة مجلة القانون والاقتصاد، مصر، 2004م
12. قانون المعاملات الالكترونية السوداني لسنة 2007م
13. المادة1/ ط، من اللائحة التنفيذية للكتاب الثالث من قانون حقوق الملكية الفكرية المصري، الصادر بالقانون رقم 82 لسنة 2002م

14. القانون رقم 98-536 المؤرخ 1 يوليو 1998 بشأن نقل الأمر التوجيهي الصادر عن البرلمان الأوروبي والمجلس، رقم 96/ 9 المؤرخ 11 مارس 1996، إلى قانون الملكية الفكرية الخاص بالحماية القانونية لقواعد البيانات
15. الميثاق الأوروبي الجديد رقم 24/ 9
16. د. حسن جميعي، الحماية الدولية لحق المؤلف والحقوق المجاورة، ندوة الوايبو حول الملكية الفكرية، 2004م
17. المادة (1) من قانون مكافحة جرائم تقنية المعلومات رقم 471 لسنة، 2018م
18. د. ميادة محمد مصطفى المحروقي، الحماية الجنائية لبيانات الأفراد الشخصية المعالجة الكترونياً، دراسة في ضوء التشريعات الجنائية المقارنة واللائحة التنظيمية الصادرة عن البرلمان الأوروبي (gdpr)
19. أشرف محمد نجيب السعيد الدريني، جرائم الاعتداء على سلامة شبكات وأنظمة المعلومات، جامعة المنصورة
20. نظام مكافحة جرائم المعلوماتية السعودي 1428هـ
21. قانون مكافحة جرائم تقنية المعلومات المصري لسنة 2018م
22. قانون جرائم المعلوماتية السوداني 2007م
23. قانون مكافحة الشائعات والجرائم الالكترونية الاماراتي لسنة 2021م
24. قانون مكافحة الجرائم الالكترونية الأردني 2023م
25. https://al-sharq.com/opinion/31/05/2023/
26. https://www.my.gov.sa/wps/portal/snp/eParticipation/openData
27. https://almdrasa.com
28. https://www.oracle.com/sa-ar/database/what-is-database/
29. https://jordan-lawyer.com/2021/09/23/database-protection
30. https://www.my.gov.sa/wps/portal/snp/aboutksa/digitaltransformation/dtcontentdetails/legal-and-regulatory-framework
31. https://nano2soft.com/en/posts/posts-post/dor-koaaad-albyanat-fy-alaaml