كلية الحقوق
القسم العام
قسم القانون الجنائي

"حماية خصوصية البيانات الشخصية الحساسة في القانون العماني"

(بحث مقدم كمتطلب لمناقشة رسالة الدكتوراه في القانون الجنائي)

مقدم من الباحث

منصور بن سيف بن محمد بن سيف الكعبي

إشراف

الأستاذ الدكتور

أكمل يوسف السعيد يوسف

أستاذ القانون الجنائي

كلية الحقوق – جامعة المنصورة

١٤٤٥هـ – ٢٠٢٤م

ملخص البحث باللغة العربية:

إن إصدار قانون حماية البيانات الشخصية في عمان هو خطوة تشريعية بارزة تعكس تحولًا كبيرًا نحو تعزيز حماية خصوصية الأفراد في العصر الرقمي. يأتي هذا القانون ليعوض النقص الذي كان في التشريعات السابقة، والتي لم تواكب بشكل كافٍ تطورات معالجة البيانات الشخصية إلكترونيًا، بدءًا من جمعها وتخزينها وصولاً إلى معالجتها.

يؤكد هذا القانون على أهمية حماية حق الأفراد في بياناتهم الشخصية من خلال فرض إطار قانوني صارم. فهو يجرّم جمع البيانات بطرق غير قانونية أو دون موافقة واضحة من أصحابها، ويمنع أي معالجة للبيانات تتجاوز الأغراض المصرح بها أو تشمل ممارسات احتيالية.

علاوة على ذلك، ينظم القانون كيفية نقل ومعالجة البيانات عبر الحدود، مما يعزز من حماية الاستثمارات الوطنية ويدعم الاقتصاد المحلي، مع الحفاظ على التزامه بالمعايير الدولية في حماية البيانات الشخصية.

لضمان تطبيق فعال لهذه القواعد، تم إنشاء مركز متخصص يركز على تنفيذ القانون ومتابعة التزام الجميع بالقوانين والاشتراطات الجديدة. هذا المركز سيعمل على ضمان تطبيق القانون بكفاءة وفعالية، مما يعزز من ثقة الأفراد في النظام التشريعي ويشجع على حماية أوسع للبيانات الشخصية.

Abstract:

The enactment of the Omani Personal Data Protection Law marks a significant legislative milestone in safeguarding the personal data of citizens. This law addresses a critical gap in the current legal framework, which previously did not adequately regulate the protection of electronically processed personal data during its collection, storage, or processing. The law upholds individuals' rights to protect their personal information, making it a crime to collect data unlawfully or without the consent of the data owners. It also criminalizes the processing of data in ways that involve fraud, deception, or are inconsistent with the stated purposes by the data owner. Furthermore, the law governs the transfer and processing of data across borders, benefiting both citizens and the national economy, while aligning with international standards for personal data protection through the rules, standards, and requirements it establishes.

المقدمة

مع تنامي الاعتماد على البيئة الرقمية لممارسة العديد من الأنشطة الاقتصادية والاجتماعية والتجارية، ورغم الفوائد الكبيرة التي جلبتها هذه الممارسات من حيث سهولة إنجاز المهام مقارنة بالطرق التقليدية، إلا أنها أدت أيضاً إلى بروز أنشطة ضارة تستهدف في كثير من الأحيان انتهاك البيانات والمعلومات الشخصية. إن تأثير التوسع في استخدام تقنيات الاتصالات والمعلومات على الخصوصية جعل من السهل جمع كميات هائلة من المعلومات، سواء كانت شخصية أو غير شخصية، حيث باتت قواعد البيانات تمتلك معلومات شاملة تقريباً عن الأفراد. وفي هذا السياق، ظهرت تجارة غير مشروعة تعرف بـ "تجارة المعلومات"، والتي لم تعد مقتصرة على الأفراد الذين يخترقون أجهزة الحاسوب وقواعد البيانات، بل باتت تقودها شركات ومواقع إلكترونية كبيرة وذات نفوذ في مجال تقنيات المعلومات. ومع غياب وسائل كافية لحماية المعلومات الشخصية في العصر الرقمي، برزت الحاجة الماسة إلى قوانين تحمي البيانات الشخصية المتداولة في البيئة الرقمية. ونتيجة لذلك، ظهرت تشريعات متخصصة تحمي الأنظمة الإلكترونية والبيانات الخاصة، بالإضافة إلى القوانين الجزائية التي تعالج الجرائم الإلكترونية تحديداً، نظراً لطبيعتها المختلفة عن الجرائم التقليدية التي تعاقب عليها القوانين الجزائية التقليدية.

إصدار قانون حماية البيانات الشخصية في عمان يمثل خطوة محورية نحو تأمين خصوصية المواطنين. هذا القانون يسد فجوة كبيرة في التشريعات السابقة التي لم تعالج بشكل كافٍ حماية البيانات الشخصية التي تُعالج إلكترونيًا، سواء عند جمعها أو تخزينها أو معالجتها.

يعكس هذا القانون أهمية حماية حقوق الأفراد في بياناتهم الشخصية، حيث يجرم جمعها بطرق غير قانونية أو دون الحصول على موافقة صريحة من أصحابها. كما يحظر معالجتها بطرق تتضمن الغش أو التزوير أو تتعارض مع الأغراض التي تمت الموافقة عليها.

علاوة على ذلك، ينظم القانون نقل البيانات ومعالجتها عبر الحدود، مما يعود بالنفع على المواطنين والاقتصاد الوطني بشكل عام. فهو يعزز حماية الاستثمارات والأعمال، ويضمن الالتزام بالمعايير الدولية لحماية البيانات الشخصية. ولتنفيذ هذه القواعد بفعالية، تم إنشاء مركز

متخصص يتولى الإشراف على تطبيق القانون وضمان التزام جميع الأطراف بالاشتراطات الجديدة.

١. أهمية الدراسة:

الحق في حماية البيانات الشخصية والحفاظ على خصوصيتها يعد من أبرز الحقوق التي تتعلق بالشخصية القانونية للفرد، وهو أقرب ما يكون لكرامته الشخصية. إن هذا الحق يعكس مدى تقدم الأمم وتحضرها، لأنه يرتبط ارتباطًا وثيقًا بالجوانب المادية والمعنوية للإنسان، ويتداخل بشكل كبير مع حقوق وحريات أخرى.

علاوة على ذلك، فإن هذا الحق يخضع لمبادئ الدين والأخلاق والأعراف السائدة في المجتمع. تتعدد أشكال هذا الحق وطرق حمايته، حيث تبذل المجتمعات جهودًا كبيرة لاحترامه كحق مستقل ومميز. ولهذا، لم تكتفِ المجتمعات بسن القوانين المحلية فقط، بل عملت أيضًا على ترسيخه في الوعي العام، مدعومة بجهود الهيئات والمنظمات الدولية والدساتير والنظم القانونية.

في جوهره، يُعد الحق في حماية البيانات الشخصية وصونها من أهم أوجه الحق في الخصوصية. الحفاظ على أسرار الإنسان يمثل الأساس الذي يضمن حرية الخصوصية ويقيها من الانتهاكات.

٢. أهداف الدراسة:

تهدف هذه الدراسة إلى توضيح أن أي معلومات تخص فرداً معيناً تُعتبر بيانات شخصية وفقاً للقانون. وبذلك، فإن أي معلومة تمكن من تحديد هوية شخص ما تدخل في نطاق البيانات الشخصية المحمية قانونياً. كما تهدف الدراسة إلى توضيح أن أي جهة تقرر طريقة جمع البيانات الشخصية والتصرف فيها، وهي ما يُعرف قانوناً بمعالجة البيانات، تتحمل مسؤولية الالتزام بالشروط القانونية في جمع البيانات والتصرف فيها. وبالتالي، يتعين على كل مؤسسة أو شركة أو جهة تحصل على معلومات شخصية لعملائها من خلال تعاملاتها أن تلتزم بالمعايير القانونية لحماية هذه البيانات.

المطلب الأول

أهداف قانون حماية البيانات الشخصية العماني

والاستثناءات الواردة على البيانات المشمولة بالحماية

تمهيد وتقسيم:

من أبرز ما يقوم عليه القانون هو فرض التزامات واضحة على كل من المتحكم في البيانات والمعالج لها، وذلك لضمان تطبيق معايير حوكمة تكنولوجيا المعلومات داخل المؤسسات المتنوعة. هذه الالتزامات تهدف إلى تعزيز الحماية والحد من الانتهاكات المتعلقة بخصوصية البيانات الشخصية. من خلال هذه الخطوة، يساهم القانون في ضمان الالتزام بمعايير الأمان وحماية المعلومات، مما يقلل من فرص تسرب البيانات أو إساءة استخدامها، ويعزز الثقة في كيفية إدارة البيانات الشخصية.

يستعرض هذا المطلب في فرعين الأهداف المبتغاة من قانون حماية البيانات الشخصية العماني، وأيضاً ما استثناه المشرع العماني من البيانات غير المشمولة بالحماية القانونية، وذلك على النحو التالي:

الفرع الأول: أهداف قانون حماية البيانات الشخصية

الفرع الثاني: الاستثناءات الواردة على البيانات الشخصية المشمولة بالحماية

الفرع الأول

أهداف قانون حماية البيانات الشخصية

جاء القانون متوخيًا تحقيق الأهداف التالية:

في إطار قانون حماية البيانات الشخصية العماني رقم ٠٦ لسنة ٢٠٢٠، من الضروري اتخاذ تدابير شاملة لضمان الحماية القانونية والتقنية للبيانات المعالجة إلكترونياً. يتطلب الأمر تبني آليات فعالة للتعامل مع المخاطر المحتملة التي قد تطرأ نتيجة استخدام هذه البيانات، مع العمل بجدية على مكافحة أي انتهاك للخصوصية. يهدف هذا إلى ضمان سلامة البيانات وحمايتها من الاستغلال أو التلاعب، وتعزيز الثقة في كيفية إدارتها والتعامل معها بما يتوافق مع القوانين والمبادئ الأخلاقية.

في إطار حماية البيانات الشخصية وفقاً لقانون عماني رقم ٠٦ لسنة ٢٠٢٠، يجب أن تتماشى التدابير المتخذة مع المعايير الدولية المتقدمة التي تحمي حقوق الأفراد وتضمن احترام خصوصيتهم. لتحقيق هذا الهدف، يجب على المتحكمين في البيانات ومعالجيها الالتزام بمسؤوليات محددة خلال جميع مراحل التعامل مع البيانات، بما في ذلك جمعها ونقلها وتخزينها وتحليلها.

من الضروري أيضاً أن تُلزم المؤسسات والجهات المعنية بتعيين مسؤول مختص لحماية البيانات الشخصية، مما يضمن الحفاظ على حقوق الأفراد وحمايتها وفقاً للقانون. كما يجب وضع ضوابط صارمة لتنظيم استخدام البيانات الشخصية في الإعلانات والتسويق الرقمي، وفي البيئة الرقمية بشكل عام.

عند التعامل مع البيانات عبر الحدود، يجب إنشاء إطار تنظيمي يضمن عدم نقل بيانات المواطنين إلى دول تفتقر إلى مستويات كافية من الحماية. يجب أيضاً إصدار التراخيص اللازمة للأطراف التي تتعامل مع البيانات الشخصية، خاصة تلك التي تتسم بحساسية خاصة.

في هذا السياق، تقوم وزارة النقل والاتصالات وتقنية المعلومات بدورها كجهة تنظيمية ومشرفة على تنفيذ أحكام القانون من خلال الهيئات والمراكز التابعة لها، مثل هيئة تقنية المعلومات ومركز الدفاع الإلكتروني.

قانون حماية البيانات الشخصية في عمان يقدم توجهاً شاملاً ومميزاً في حماية جميع أشكال البيانات الشخصية، بما يتجاوز حدود المعالجة الإلكترونية. إذ يوضح القانون أن نطاق تطبيقه لا يقتصر فقط على البيانات التي تتم معالجتها إلكترونياً، بل يمتد ليشمل أيضاً البيانات المكتوبة أو المخزنة ورقياً، وكذلك البيانات التي يتم معالجتها إلكترونياً جزئياً. هذه المرونة في نطاق التطبيق تعكس حكمة المشرع العماني في تقديم حماية قانونية شاملة لجميع أنواع البيانات الشخصية، مهما كانت طريقة معالجتها.

في هذا الإطار، يضمن القانون حماية قانونية متكاملة للبيانات الشخصية، سواء كانت معالجة بطرق آلية أو يدوية، كاملة أو جزئية. هذا التوجه يعكس الفرق بين القانون العماني ونظيره المصري. حيث يقتصر تطبيق قانون حماية البيانات الشخصية المصري رقم ١٥١

لسنة ٢٠٢٠ على البيانات المعالجة إلكترونياً فقط، ولا يمتد إلى البيانات المكتوبة أو المخزنة ورقياً بشكل كامل، كما لا يتناول معالجة البيانات التي تتم جزئياً باستخدام الوسائل الإلكترونية.

هذا الفرق في النهج بين التشريعين يظهر التزام المشرع العماني بتوسيع نطاق الحماية القانونية ليشمل جميع أنواع البيانات الشخصية، في حين اقتصر المشرع المصري على حماية البيانات الإلكترونية فقط. تجدر الإشارة إلى أن القانون المصري قد اقتدى باللائحة العامة لحماية البيانات الأوروبية، التي تنص المادة (٢ / ١) منها على تطبيقها على معالجة البيانات الشخصية سواء كانت كلياً أو جزئياً باستخدام الوسائل الآلية.

فيما يتعلق بنطاق تطبيق قانون حماية البيانات الشخصية العماني، يقتصر القانون حالياً على حماية بيانات الأشخاص الطبيعيين فقط، متجاهلاً بذلك بيانات الأشخاص الاعتبارية، سواء كانت عامة أو خاصة. من وجهة نظر الباحث، فإن هذا النهج يستدعي إعادة تقييم من قبل المشرع العماني، خاصة أن الشخص الاعتباري يتمتع بشخصية قانونية ويخضع للحقوق والالتزامات التي يحددها القانون، ما عدا تلك الحقوق التي تقتصر بطبيعتها على الأفراد الطبيعيين.

إغفال حماية بيانات الأشخاص الاعتبارية يمثل نقصاً ملحوظاً، خاصة وأن هذه البيانات قد تكون حساسة ولها تأثير كبير على الأنشطة التجارية والإدارية. لذلك، من الضروري أن يقوم المشرع العماني بتوسيع نطاق القانون ليشمل حماية بيانات الأشخاص الاعتبارية. هذا التعديل سيكون له تأثير إيجابي على تعزيز الأمان والثقة في بيئة الأعمال، ويعكس اهتماماً شاملاً بحماية جميع أنواع البيانات الشخصية.

الفرع الثاني

الاستثناءات الواردة على البيانات الشخصية المشمولة بالحماية

القانون العماني لحماية البيانات الشخصية قد استبعد العديد من المجالات من نطاق تطبيقه، سواء من حيث نوعية المعالجة أو الأطراف المستفيدة من الحماية القانونية. في المادة (٠٣)، يقدم القانون قائمة شاملة للبيانات الشخصية التي لا تشملها أحكامه، حتى وإن كانت تتعلق بالأشخاص الطبيعيين وتتم معالجتها إلكترونيًا بالكامل أو جزئيًا. هذه البيانات، رغم أهميتها، لا تتمتع بالحماية التي يوفرها القانون لأسباب متعددة.

الحماية القانونية المقررة بموجب هذا القانون تقتصر على البيانات الشخصية التي تُعالج في سياق مهني أو تجاري، بينما تستثني البيانات المتعلقة بالأمن القومي والمصلحة العامة، أو تلك ذات الطابع الشخصي البحت، وكذلك البيانات المرتبطة بمكافحة الجرائم وتنفيذ العقوبات وأعمال السلطة القضائية.

من الجدير بالذكر أن المشرع العماني اختار استبعاد فئات كبيرة من البيانات الشخصية من نطاق الحماية القانونية، وهو قرار يبدو أنه يفتقر إلى تبرير كافٍ. على سبيل المثال، البيانات المتعلقة بالدعاوى القضائية، والتي كانت تستحق حماية قانونية خاصة تأخذ في اعتبارها حساسيتها، تم استبعادها بالكامل. كان من الأفضل أن يتضمن القانون آليات حماية تتناسب مع طبيعة هذه البيانات بدلاً من إغفالها تماماً.

المطلب الثاني

حماية البيانات الشخصية الحساسة

تمهيد وتقسيم:

البيانات الشخصية الحساسة هي تلك التي تكشف بشكل مباشر أو غير مباشر عن تفاصيل دقيقة تتعلق بشخص الفرد، مثل معلومات عن خلفيته العائلية أو الأصل العرقي، بالإضافة إلى آرائه السياسية والفلسفية، ومعتقداته الدينية، وسجل سوابقه الجنائية. تشمل أيضاً البيانات البيومترية مثل قياسات بصمات الأصابع أو ملامح الوجه، وأية معلومات تتعلق بصحة الفرد، بما في ذلك حالته الجسدية والنفسية والعقلية والجينية والجنسية. علاوة على ذلك، تتضمن المعلومات المتعلقة بالخدمات الصحية المقدمة له، والتي قد تكشف عن حالته الصحية بوضوح.[١]

في المادة (٨) من المبادئ التوجيهية للاتحاد الأوروبي، تم تحريمه معالجة البيانات الشخصية الحساسة التي تكشف عن الأصل العرقي، الآراء السياسية، المعتقدات الدينية، وكذلك البيانات المتعلقة بالصحة والحياة الجنسية. ومع ذلك، تسمح هذه المبادئ بوجود استثناءات حيث يمكن للتشريعات الوطنية أن تضع قواعد مخالفة، شريطة أن يتم الحصول على موافقة مسبقة من الشخص المعني قبل معالجة هذه البيانات الحساسة[٢] .

بناءً على ذلك، يُفهم أن البيانات الشخصية الحساسة هي تلك التي تتعلق بالعرق، الديانة، المعتقدات، الآراء السياسية، والسجل الإجرامي. تُعتبر هذه البيانات ذات طابع خاص وحساس للغاية بالنسبة للفرد، حيث يسعى للحفاظ على سريتها وعدم كشفها للآخرين بسبب طبيعتها الحساسة. تختلف خطورة وأهمية هذه البيانات عن البيانات الأساسية مثل الاسم، تاريخ الميلاد، والعنوان، مما يجعلها بحاجة إلى مستويات حماية أعلى لضمان عدم استخدامها بشكل غير مناسب أو الكشف عنها.[٣]

---

[١] نائلة عادل محمد فريد، جرائم الحاسب الالي الاقتصادية، دار النهضة العربية، القاهرة، ٢٠٠٤ ، ٩٧ .

[٢] محمد لطفي عبد الفتاح، الاطار القانوني لحماية الخصوصية الجينية، مجلة جامعة الملك عبد العزيز، العدد ٠١ ، ٢٠١٣ ، ص ٣٣٠ .

[٣] طارق جمعة السيد راشد، الحماية القانونية للحق في خصوصية البيانات الجينية، المجلة القانونية، كلية القانون، جامعة قطر، ٢٠٢٢ ، ص ٣٩١١

ويتناول هذا المطلب أنواع البيانات الشخصية الحساسة، من خلال الفروع التالية:

الفرع الأول: البيانات الجينية أو الوراثية

الفرع الثاني: البيانات الصحية

الفرع الثالث: البيانات الحيوية

الفرع الأول

البيانات الجينية أو الوراثية

بالإضافة إلى البيانات الشخصية العامة، من الضروري أن نركز بشكل خاص على البيانات الشخصية الحساسة، لأنها تُعتبر من الفئات الأكثر أهمية وتتطلب مستوى حماية أعلى. تتضمن هذه البيانات الجينية، البيومترية أو الحيوية، وأيضًا المعلومات الصحية. كما تشمل البيانات التي تكشف عن الأصل العرقي والإثني، والآراء السياسية، والمعتقدات الدينية أو الأيديولوجية. نظرًا لطبيعتها الحساسة، تحتاج هذه المعلومات إلى إجراءات حماية مشددة لضمان الحفاظ على خصوصية الأفراد ومنع استخدامها بطرق قد تؤثر على حياتهم الشخصية أو المهنية.[٤]

تُعتبر المعلومات الجينية من أكثر المعلومات خصوصية، لأنها تتعلق بالحمض النووي الخاص بكل فرد والذي يشكل بصمة فريدة لا تتطابق مع أي شخص آخر. لكن من الجدير بالذكر أن بعض التغيرات الجينية قد تكون مشتركة بين الأقارب، مما يضفي طابعًا خاصًا على البيانات الجينية. هذا الطابع المختلط يجعل البيانات الجينية مزيجًا فريدًا يجمع بين الخصوصية الفردية والروابط العائلية. لذلك، أصبح من الضروري حماية خصوصية هذه البيانات بعناية، وتقييد جمعها وتداولها، لضمان احترام الحقوق الفردية وحماية المعلومات الشخصية بشكل فعال .[٥]

---

[٤] حمد بن عبدالله السويلم، انعكاسات استخدام المادة الوراثية وتأثيرها المحتمل على الامن الوطني، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠١١ ، ص ١٧٦

[٥] اشرف توفيق شمس الدين، الجينات الوراثية والحماية الجنائية للحق في الخصوصية، مؤتمر الهندسة الوراثية بين الشريعة والقانون، كلية الشريعة والقانون، الامارات، مايو ٢٠٠٧ ، ص ١١٠ .

١. مفهوم البيانات الجينية:

البيانات الجينية تتعلق بالسمات الوراثية للفرد، سواء كانت موروثة أو مكتسبة، ويتم استخراجها من خلال تحليل الحمض النووي. تعد هذه البيانات من بين أكثر البيانات الشخصية حساسية بسبب المعلومات الدقيقة التي تحتويها عن الجوانب الصحية وغير الصحية للفرد. فهي لا تقتصر فقط على تحديد الخصائص الفردية، بل قد تكشف أيضًا عن معلومات هامة تتعلق بالصحة العامة والميول الوراثية للأمراض. لذا، يتطلب الأمر اتخاذ إجراءات مشددة لحماية هذه البيانات وضمان سرية استخدامها، وذلك لتجنب أي انتهاك لخصوصية الأفراد وضمان حماية معلوماتهم الشخصية بفعالية.[٦]

في إطار قانون حماية البيانات الشخصية العماني، تُعرّف البيانات الجينية على أنها "البيانات الشخصية المتعلقة بالخصائص الموروثة أو المكتسبة جينياً، والتي تُستخلص من تحليل العينة البيولوجية". نظرًا لطبيعتها الحساسة، اعتبر المشرع العماني هذه البيانات من بين البيانات التي تستحق حماية قانونية خاصة.

يُشدد القانون العماني على أهمية حماية البيانات الجينية بشكل كبير، حيث يحظر معالجتها إلا بعد الحصول على تصريح رسمي من الجهات المعنية. تعد المادة (٥) من قانون حماية البيانات الشخصية العماني حجر الزاوية في هذا السياق، إذ تحدد شروط معالجة البيانات الجينية جنبًا إلى جنب مع البيانات الحيوية والصحية، والأصول العرقية، والحياة الجنسية، والآراء السياسية والدينية.

فرض المشرع العماني قيدين رئيسيين على معالجة البيانات الجينية: أولاً، يتعين الحصول على ترخيص من وزارة النقل والاتصالات وتقنية المعلومات، التي تُعنى بإصدار هذه التصاريح. ثانيًا، يجب أن تتم المعالجة وفقًا للضوابط والإجراءات المحددة بالقانون.

---

[٦] احمد حسام طه، الحماية الجنائية لاستخدام الجينات الوراثية في الجنس البشري، دار النهضة العربية، القاهرة، ٢٠٠٥ ، ص ١٢ .

وفي حال انتهاك أحكام المادة (٥)، يواجه المخالفون غرامة مالية تتراوح بين خمسة عشر ألف ريال عماني وعشرين ألف ريال عماني، مما يعكس جدية المشرع في حماية هذه البيانات الحساسة وضمان معالجتها بشكل قانوني وصحيح.

البيانات الجينية والحمض النووي تمتلك القدرة على كشف معلومات حساسة تتجاوز مجرد التفاصيل الجينية. فهي يمكن أن تكشف عن اضطرابات جينية أو استعداد الشخص للإصابة بأمراض معينة، بالإضافة إلى تحديد أصوله العرقية ومعلومات أخرى شديدة الحساسية.

الأمر الأكثر إثارة للقلق هو أن ربط قواعد بيانات الحمض النووي بالمعلومات الشخصية مثل الأسماء والعناوين قد يؤدي إلى تتبع الأفراد بشكل دقيق. لذا، تبرز أهمية حماية هذه البيانات الجينية بشكل صارم لضمان الحفاظ على خصوصيتها وأمانها.[٧]

الحمض النووي والبيانات الجينية لا توفر فقط معلومات حيوية عن الفرد نفسه، بل تتيح أيضاً كشف الروابط الجينية بين الأفراد. هذه القدرة على تحديد الصلات الأسرية تعني أن آثار استخدام هذه البيانات تتجاوز الفرد المعني لتصل إلى العائلة بأكملها. فبدلاً من اقتصار المعلومات الجينية على تحليل بيانات الشخص وحده، توفر أيضاً إمكانية تحديد علاقات الأسرة والتعرف على أفرادها من خلال الروابط الجينية المشتركة.[٨]

٢. **تأثير التطورات في جمع واستخدام البيانات الجينية على الخصوصية**:

في السنوات الأخيرة، شهدنا زيادة هائلة في حجم البيانات الجينية التي يتم جمعها واستخدامها عبر مجموعة متنوعة من القطاعات، بما في ذلك الرعاية الصحية، والأبحاث، والصناعة. هذا النمو السريع يثير قلقاً متزايداً حول كيفية حماية خصوصية هذه المعلومات الشخصية الحساسة من الناحيتين القانونية والتقنية.

هذا التطور يستدعي منا تقييم التهديدات الحالية والمستقبلية التي قد تهدد خصوصية البيانات الجينية، وفحص كيفية تكيّف الأنظمة القانونية، خاصة في المجال الجزائي، مع هذه التحديات. يجب علينا أيضاً دراسة الضمانات التقنية التي يمكن أن تقلل من المخاطر المرتبطة

---

[٧] أشرف توفيق شمس الدين، الجينات الوراثية والحماية الجنائية للحق في الخصوصية، مرجع سابق، ص ١١٣

[٨] طارق جمعة السيد راشد، الحماية القانونية للحق في خصوصية البيانات الجينية، مرجع سابق، ص ٣٩١٦

بالتعدي على البيانات الجينية للأفراد. تحقيق التوازن بين حماية البيانات الشخصية والفوائد المترتبة على جمع وتبادل المعلومات الجينية يعد أمراً ضرورياً.

الأضرار الناتجة عن الاعتداء على البيانات الجينية تبرز أهمية هذا الموضوع. بينما تُعتبر البيانات الجينية مصدراً ثميناً في مجالات مثل الرعاية الصحية والبحث العلمي، فإن تزايد اهتمام الدول بإنشاء قواعد بيانات ضخمة واستخدامها لأغراض متعددة يمكن أن يؤدي إلى تدخلات تؤثر على الخصوصية. من الضروري أن يكون هناك وعي كافٍ بالمخاطر المحتملة وتطوير استراتيجيات لمواجهتها لضمان حماية البيانات الجينية وتحقيق أقصى استفادة منها دون انتهاك حقوق الأفراد.[٩]

تتجلى إحدى المشكلات الكبيرة في مجال البيانات الجينية في كيفية التعامل معها بعد استخدامها في التحقيقات الجنائية. على سبيل المثال، قد يتم الاحتفاظ بالبيانات الجينية التي تُجمع خلال التحقيقات الجنائية حتى بعد براءة الأفراد المعنيين. في بعض الحالات، تسعى هيئات إنفاذ القانون إلى استخدام هذه الملفات الجينية لاحقًا لحل الجرائم المستقبلية. هذا قد يؤدي إلى تدخل غير مبرر في خصوصية الأفراد الأبرياء، حيث يتم الاحتفاظ ببياناتهم الجينية رغم عدم ثبوت أي جرم عليهم.

تفتح بعض اتفاقيات تبادل البيانات غير المعلنة أبوابًا لتبادل البيانات الجينية بين الإدارات الحكومية والشركات دون الحاجة للحصول على إذن صريح من الأفراد المعنيين. هذه الممارسات قد تفضي إلى تمييز ضد الأفراد بناءً على خصائصهم الجينية من قبل الأطراف التي تصل إلى هذه البيانات.

استخدام البيانات الشخصية بدون إذن يمكن أن يؤدي إلى أضرار كبيرة. بينما قد تكون البيانات المجمعة من مجموعات كبيرة أقل تأثيراً، فإن البيانات الشخصية التي يمكن تحديد هوية الأفراد من خلالها تشكل خطراً أكبر. الكشف غير المصرح به عن معلومات صحية قد يعرض الأفراد لمخاطر مثل المساس بالسمعة، فقدان الوظائف، وصعوبات في الحصول على التأمين والخدمات الأخرى.

---

[٩] طارق جمعة السيد راد، الحماية القانونية لخصوصية البيانات الشخصية في القانون القطري والمقارن، المجلة القانونية والقضائية، وزارة العدل القطرية، العدد ٠٢ ، السنة ١١ ، ص ٢٢ .

هذا يعزز الحاجة الملحة لحماية الخصوصية وتأمين البيانات الجينية، خصوصاً عندما تُستخدم في أبحاث تجمع بين البيانات الجينية وأنواع أخرى من المعلومات مثل البيانات الديموغرافية والعوامل الاجتماعية والسلوكية المتعلقة بالصحة. في ظل هذه التحديات، يجب أن تكون هناك ضوابط قوية تضمن استخدام البيانات الجينية بشكل يحافظ على حقوق الأفراد ويحمي خصوصيتهم.[١٠]

إن تبادل البيانات الجينية على مستوى الأفراد يفتح المجال لإعادة تعريف الهوية بطرق جديدة. على سبيل المثال، يستطيع المتلقون تحليل المعلومات الجينية لاستنباط معلومات عن السمات الظاهرة التي يمكن استخدامها لإعادة تحديد الهوية. من خلال تسلسل الجينات الكامل، يمكن للباحثين التعرف على الأفراد بناءً على التنبؤ بالخصائص المرئية مثل لون العين والجلد. وبالمثل، يمكن استخدام السمات المرئية لاستنتاج المعلومات الجينية، بما في ذلك الاضطرابات التي تظهر جسديًا، أو السمات البصرية، أو حتى الهياكل الوجهية ثلاثية الأبعاد، لتحقيق أغراض إعادة تحديد الهوية. بالإضافة إلى ذلك، قد تتيح المعلومات الديموغرافية التي غالبًا ما تُشارك مع البيانات الجينية استنتاج معرفات محتملة من خلال الربط بمصادر بيانات أخرى متاحة بسهولة.

علاوة على ذلك، يمكن استنتاج المعرفات المحتملة من المعلومات الديموغرافية التي غالبًا ما تُرفق بالبيانات الجينية، من خلال الربط مع مصادر بيانات أخرى يسهل الوصول إليها .[١١]

بفضل التشابه بين السجلات الجينية للأقارب، حتى وإن لم يُشارك السجل الجيني لشخص معين أو حتى لم يُنشأ، يمكن استنتاج الأنماط الجينية والاستعداد لأمراض معينة بناءً على الأنماط الجينية المشتركة بين أقاربه.

لحماية الخصوصية، يعد منع الوصول إلى البيانات من قبل غير المخولين أحد العناصر الأساسية. لمواجهة خطر القرصنة الإلكترونية الذي يهدد البيانات الجينية، من الضروري تنفيذ

---

[١٠] حسين طاهر داود، الحاسب وأمن المعلومات، دار الفجر للنشر والتوزيع، القاهرة، ٢٠٠٠ ، ص ٦٤

[١١] عبد الله مجيد حساني، التقنيات الحديثة في التحقيق الجنائي ودورها في ضبط الجريمة، رسالة ماجستير، جامعة النهرين، ٢٠١٤ ، ص ٢٨

تدابير أمان صارمة. يشمل ذلك إدارة الوصول بعناية، وتطبيق تقنيات التشفير المتقدمة، وتقييد الوصول إلى الأطراف الموثوقة فقط.

عندما يتطلب الأمر مشاركة بيانات غير محددة الهوية مع طرف ثالث غير موثوق أو مع الجمهور، يجب اتخاذ تدابير لحماية خصوصية الأفراد. يشمل ذلك تقييد أو تعديل البيانات لضمان عدم إمكانية التعرف على الأفراد منها.

علاوة على ذلك، ينبغي أن تتم معالجة البيانات الجينية فقط بناءً على موافقة صريحة من الأفراد المعنيين وتحت إشراف هيئات رسمية. من الضروري أيضاً الكشف عن تفاصيل أي اتفاقيات تتعلق بمشاركة البيانات ومدى احتفاظها، لضمان الشفافية وحماية حقوق الأفراد .[١] الأفراد .[١]

يتعين على الجهات المعنية أن تقتصر على جمع البيانات الجينية لأغراض محددة ومصرح بها فقط، مثل الأغراض الطبية أو التحقيقات الجنائية، وذلك لتقليل فرص انتهاك خصوصية الأفراد. ويجب على الدول التأكد من أن الاحتفاظ بالبيانات الجينية والحمض النووي يتم بطرق مبررة وقانونية، بحيث يكون هذا الاحتفاظ ضرورياً ومتناسباً مع الهدف المحدد.

لتحقيق هذا الهدف، ينبغي إنشاء نظام مراجعة مستقل يتولى تحديد أسباب الاحتفاظ بالبيانات الجينية ومدى الحاجة إلى استمرار الاحتفاظ بها. بالنظر إلى القيمة الكبيرة التي تحملها البيانات الجينية، من المحتمل أن تصبح قواعد البيانات التي تحتوي على هذه المعلومات هدفاً محتملاً لأعمال القرصنة الإلكترونية. لذا، من الضروري تبني تقنيات الحماية الإلكترونية المناسبة لضمان تأمين هذه القواعد وحمايتها من أي اختراقات قد تهدد خصوصية الأفراد.

تتميز البيانات الجينية عن المعلومات المشابهة الأخرى، مثل المعلومات الصحية، بأنها ثابتة ولا تتغير. فالتكوين الجيني للفرد يتم عبر مزج الصفات الوراثية من الوالدين، مما يجعل الرموز الجينية غير مرنة وثابتة. في المقابل، تعتبر التشخيصات الطبية، التي غالباً ما تتأثر

[١] طارق جمعة السيد راشد، الحماية القانونية لخصوية البيانات الشخصية، مرجع سابق، ص ٢٥

بالتغيرات البيئية، والعادات الشخصية، والتغذية، والتدخلات السريرية، أكثر مرونة وتغيرًا بمرور الوقت .[1]

الفرع الثاني

البيانات الصحية

تُعتبر البيانات الشخصية المتعلقة بالصحة التي تُعالج إلكترونيًا من بين المعلومات الأكثر حساسية التي تتطلب حماية قانونية قوية، نظراً لأنها تتعلق بالحق في الخصوصية. هذه البيانات تشمل كل ما يتعلق بالحالة الصحية للفرد، مثل التقارير الطبية، العينات التحليلية، التشخيصات الطبية، تفاصيل الأدوية، والتقارير الخاصة بالأمراض المزمنة. جميع هذه المعلومات محمية بموجب الحق في الخصوصية.

في سلطنة عمان، يُعرّف قانون حماية البيانات الشخصية البيانات الصحية بأنها "البيانات الشخصية المتعلقة بالصحة الجسدية والعقلية والنفسية." هذا التعريف يضمن أن كل ما يتعلق بالصحة يعتبر ضمن نطاق الحماية القانونية.

أما في إطار الاتحاد الأوروبي، فتنص اللائحة العامة لحماية البيانات على أن البيانات الشخصية المتعلقة بالصحة تشمل أي معلومات تكشف عن الحالة الصحية البدنية أو العقلية، سواء كانت حالية، سابقة، أو متوقعة. يشمل ذلك المعلومات التي يتم جمعها أثناء تقديم خدمات الرعاية الصحية، والأرقام أو الرموز التي يمكن أن تحدد الشخص لأغراض صحية. كما تضمّ هذه البيانات المعلومات المشتقة من الفحوصات البيولوجية والاختبارات، بما في ذلك البيانات الجينية والعينات البيولوجية، وأية معلومات متعلقة بالمرض، العجز، تاريخ المرض، العلاج السريري، أو الحالة الفسيولوجية والطبية الحيوية.

في فرنسا، أكدت اللجنة الوطنية للمعلوماتية والحريات أن البيانات المتعلقة بالصحة تُعتبر بيانات شخصية تخضع لحماية قانونية. وقد شددت اللجنة على أن نتائج الاختبارات

[1] محمد امين الرومي، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٣ ، ص ١٨٧

النفسية تُعَدّ أيضاً جزءًا من البيانات الشخصية المحمية، حيث تُعتبر الحالة النفسية جزءاً من الصحة الشاملة، وبالتالي تدخل ضمن نطاق الحماية القانونية لخصوصية الأفراد[1].

لا يُسمح بمعالجة البيانات الشخصية المتعلقة بالصحة إلا بعد الحصول على موافقة واضحة ومباشرة من الشخص المعني، أو بعد إعلامه مباشرة أو من خلال طبيب يتم تعيينه لهذا الغرض. لكن، توجد بعض الاستثناءات التي يفرضها المشرع الفرنسي لحماية هذه البيانات.

في الحالة الأولى، المتعلقة بمتابعة المرضى طبيًا، يُسمح للأطباء بتسجيل بيانات المرضى، سواء كان هذا التسجيل يدويًا أو عبر نظام إلكتروني. وفي هذه الحالة، لا يُطلب الحصول على موافقة منفصلة من المريض لتسجيل هذه البيانات.

أما في الحالة الثانية، التي تتعلق بالبحث العلمي، يمكن لمراكز البحث جمع وتخزين البيانات الصحية للأفراد بشكل مجهول. يُسمح بهذا الاستثناء طالما يتم استخدام البيانات لأغراض البحث العلمي، وذلك ضمن إطار الضرورات العلمية المحددة.

في تونس، حدد قانون حماية المعطيات الشخصية شروطاً دقيقة ومعايير واضحة لمعالجة البيانات الشخصية المتعلقة بالصحة، كما هو موضح في القسم الثاني من الباب الخامس من القانون. ومن أبرز هذه الشروط:

١. الحصول على موافقة الشخص المعني أو ورثته أو وليه.
٢. إذا كانت المعالجة ضرورية لتحقيق أغراض يقتضيها القانون.
٣. إذا كانت المعالجة ضرورية لتطوير وحماية الصحة العامة.
٤. إذا كانت المعالجة تعود بالنفع على الشخص المعني على المستوى الصحي.
٥. إذا كانت المعالجة في إطار البحث العلمي في المجال الصحي.
٦. يتعين أن تُعالج البيانات الشخصية المتعلقة بالصحة فقط بواسطة الأطباء أو الأفراد الملتزمين بالحفاظ على أسرار المهنة. يمكن للأطباء أيضاً نقل هذه البيانات إلى جهات أو هيئات مخصصة للبحث العلمي في المجال الصحي، ولكن هذا يتطلب الحصول على

[1] الشهابي إبراهيم الشهابي الشرقاوي، التزام الطبيب بحفظ اسرار المرضى، مجلة الكويت، جامعة الكويت، مجلس النشر العلمي، عدد ٠٣ ، ص ٢٢١ .

ترخيص من الهيئة الوطنية لحماية المعطيات الشخصية. يجب على الهيئة الوطنية أن تقيم طلب الترخيص الذي يُقدّم إليها من قِبل الجهة البحثية خلال فترة لا تتجاوز ثلاثين يومًا.

٧. لا يجوز أن تتجاوز مدة معالجة البيانات المدة اللازمة لتحقيق الغرض الذي أجريت من أجله.

تثير مسألة عدم الإفصاح عن البيانات الصحية تساؤلًا حول ما إذا كان إبلاغ الطبيب للسلطات الصحية العامة بحالة مرضى فيروس نقص المناعة المكتسب (الإيدز) يعد انتهاكًا للخصوصية. وقد انقسم الفقه في هذا الشأن إلى اتجاهين:

- الاتجاه الأول يرى أن سجلات مرضى الإيدز تعد من البيانات الحساسة التي تستفيد من الحماية القانونية، وبالتالي، فإن إبلاغ الطبيب بأي جهة أو سلطة عن حالة هؤلاء المرضى يعد انتهاكًا للحق في الخصوصية.
- الاتجاه الثاني يجيز للطبيب إبلاغ السلطات الصحية بشأن حالة المرضى بهدف احتواء انتشار المرض، حيث تنص بعض الدول على أن مرض الإيدز يجب التبليغ عنه للسلطات الصحية، مما يخلق واجبًا قانونيًا لإبلاغ السلطات عند اكتشافه .[١]

في الواقع، إذا لم تتوفر حماية كافية للبيانات الشخصية الحساسة، فقد تتسبب هذه الثغرات في نتائج سلبية. على سبيل المثال، قد يتردد الأفراد في إجراء اختبارات الكشف عن الأمراض بسبب القلق من تسرب معلوماتهم الشخصية، مما يمكن أن يؤدي إلى تفشي المرض بشكل أكبر ويقلل من توفر المعلومات الضرورية لمكافحته.

الفرع الثالث

البيانات الحيوية

في إطار قانون حماية البيانات الشخصية العماني، تُعرَّف البيانات الحيوية على أنها "بيانات شخصية تتعلق بالخصائص الجسدية أو النفسية أو السلوكية، مثل صورة الوجه أو البيانات الخاصة بالبصمة الوراثية." تُعد البصمة الوراثية إحدى أهم أشكال البيانات الشخصية، حيث تعكس تفاصيل هامة تتعلق بكل فرد، بدءًا من السمات الشخصية إلى تفاصيل نسبه العائلي

[١] شنيه زواوي، الالتزام بكتمان السر الطبي، مجلة الحقوق والعلوم السياسية، الجامعة اللبنانية، كلية الحقوق والعلوم السياسية والادارسة، عدد ٢٢ ، فبراير ٢٠١٩ ، ص ١٦٧

والأمراض الوراثية التي قد يكون معرضًا لها. يكمن القلق الرئيسي في أن انتهاك هذه البيانات يمثل تعديًا خطيرًا على حق الأفراد في حماية خصوصيتهم.

البصمة الوراثية تُمكّن من تحديد الهوية بشكل دقيق من خلال تحليل العينات البيولوجية، مثل اللعاب أو الشعر أو السائل المنوي. حتى الأثر البسيط الذي يتركه الفرد يمكن استخدامه لتحديد هويته من خلال تحليله. لذا، من الضروري أن يتدخل المشرع لحماية حق الأفراد في خصوصية بياناتهم الشخصية، سواء كانت تلك البيانات في شكلها التقليدي أو كبيانات معالجة إلكترونيًا[1].

في فرنسا، تؤكد اللجنة القومية للمعلوماتية والحريات أن جميع أنواع بصمات الإنسان، سواء كانت بصمات الأصابع، بصمة اليد، بصمة العين، أو أي أنماط أخرى، تُعتبر بيانات شخصية. يمكن الآن جمع هذه البصمات ومعالجتها إلكترونيًا، مما يجعلها خاضعة للحماية القانونية كبيانات شخصية معالجة إلكترونيًا. وهذا يعني أنه لا يمكن استخدام أو دراسة الخصائص الوراثية للأفراد إلا لأغراض طبية أو علمية بعد الحصول على موافقتهم الصريحة، والامتثال للشروط القانونية المنصوص عليها.

على صعيد الاتحاد الأوروبي، تُعرَّف البيانات الشخصية المتعلقة بالبصمة الوراثية بأنها تلك التي ترتبط بالخصائص الوراثية التي تكون إما موروثة أو مكتسبة. يتم الحصول على هذه البيانات من خلال تحليل عينات بيولوجية مثل الصبغيات والحمض النووي، مما يوفر معلومات دقيقة حول الفرد بناءً على بياناته الجينية.

الخاتمة

[1] مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الالكترونية، دار النهضة العربية، القاهرة، ٢٠٠١ ، ص ١٠٤

موضوع الحق في خصوصية البيانات الشخصية المعالجة إلكترونيًا يثير تساؤلات قانونية معقدة، في ظل التحولات الكبيرة التي يشهدها عصر المعرفة والتكنولوجيا. تطور الفضاء الإلكتروني، الذي يعد ساحة لتخزين البيانات، يفرض تحديات جديدة تتطلب حماية جزائية ملائمة تشمل جميع جوانب جمع البيانات، نقلها، تخزينها، نشرها، الاطلاع عليها، ومعالجتها. أصبح من الضروري أن يلتزم مقدمو خدمات معالجة البيانات الإلكترونية والشركات والمؤسسات بسياسات حماية صارمة تتماشى مع القوانين السارية.

تلعب التشريعات الخاصة بحماية البيانات الشخصية، مثل قانون حماية البيانات الشخصية العماني الصادر بالمرسوم السلطاني رقم ٦ لسنة ٢٠٢٢، دورًا محوريًا في تأمين الحماية الجزائية للبيانات الشخصية. توفر هذه التشريعات قواعد وإجراءات خاصة لمعالجة البيانات ومدة الاحتفاظ بها، وتحدد حقوق الأفراد في تعديل بياناتهم واستخدامها فقط بعد الحصول على موافقتهم.

أولاً - النتائج:

١. **حماية خصوصية البيانات الشخصية :**يُعترف بحق الأفراد في حماية خصوصية بياناتهم الشخصية كحق أساسي، وهو يعادل أهمية الحقوق والحريات العامة كما نصت عليه الإعلانات والعهود الدولية المتعلقة بحقوق الإنسان.

٢. **امتداد الحماية القانونية :**تشمل الحماية القانونية للبيانات الشخصية جميع الأنواع، سواء كانت بيانات عادية أو حساسة، مثل تلك التي تكشف عن العرق، المعتقدات الدينية، أو الحالة الصحية.

٣. **التشريعات العمانية والمصرية :**كل من قانون حماية البيانات الشخصية العماني وقانون حماية البيانات الشخصية المصري يضمنان حماية البيانات الشخصية المعالجة إلكترونيًا من خلال تجريم جمع ومعالجة وتداول البيانات دون موافقة صاحبها أو في الأوضاع التي يسمح بها القانون.

٤. **الضمانات القانونية العمانية :**يتضمن قانون حماية البيانات الشخصية العماني العديد من الضمانات القانونية التي تنظم حق الاطلاع على البيانات الشخصية.

٥. **القيود على الحق في الاطلاع :**الحق في الاطلاع على البيانات الشخصية المعالجة ليس مطلقًا، حيث توجد قيود تتعلق بحماية سلامة الدولة، سيادتها، والأمن العام.

ثانياً ـ التوصيات:

١. **متابعة التطورات التقنية :**يجب متابعة تطورات تقنيات المعلومات ووسائل معالجة البيانات الشخصية وتطوير التشريعات الخاصة بحماية خصوصية البيانات الشخصية لتواكب هذه التغيرات. يجب تحقيق التوازن بين حماية حق الفرد في خصوصية بياناته والحق في الوصول إلى المعلومات، مع الحفاظ على الأمن القومي.

٢. **توفير الضمانات الإجرائية :**العمل على توافر الضمانات الإجرائية لحماية الحق في خصوصية البيانات الشخصية المعالجة إلكترونيًا، حيث إن غياب هذه الضمانات قد يؤدي إلى الإفلات من العقاب.

٣. **مبادئ الشفافية :**الالتزام بتطبيق مبادئ الشفافية بشأن التدابير المتخذة والتي تؤثر على حق الخصوصية في البيانات الشخصية المعالجة إلكترونيًا، مما يعزز التصدي للثغرات والمشاكل القانونية في حماية الحق في الخصوصية.

قائمة المراجع

١. احمد حسام طه، الحماية الجنائية لاستخدام الجينات الوراثية في الجنس البشري، دار النهضة العربية، القاهرة، ٢٠٠٥

٢. أشرف توفيق شمس الدين، الجينات الوراثية والحماية الجنائية للحق في الخصوصية، مؤتمر الهندسة الوراثية بين الشريعة والقانون، كلية الشريعة والقانون، الامارات، مايو ٢٠٠٧

٣. الشهابي إبراهيم الشهابي الشرقاوي، التزام الطبيب بحفظ اسرار المرضى، مجلة الكويت، جامعة الكويت، مجلس النشر العلمي، عدد ٠٣ ، ص ٢٢١ .

٤. حسين طاهر داود، الحاسب وأمن المعلومات، دار الفجر للنشر والتوزيع، القاهرة، ٢٠٠٠

٥. حمد بن عبد الله السويلم، انعكاسات استخدام المادة الوراثية وتأثيرها المحتمل على الامن الوطني، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠١١

٦. شنيه زواوي، الالتزام بكتمان السر الطبي، مجلة الحقوق والعلوم السياسية، الجامعة اللبنانية، كلية الحقوق والعلوم السياسية والادارية، عدد ٢٢ ، فبراير ٢٠١٩

٧. طارق جمعة السيد راشد، الحماية القانونية للحق في خصوصية البيانات الجينية، المجلة القانونية، كلية القانون، جامعة قطر، العدد ٠٢ ، السنة ١١ ، ٢٠٢٢

٨. عبد الله مجيد حساني، التقنيات الحديثة في التحقيق الجنائي ودورها في ضبط الجريمة، رسالة ماجستير، جامعة النهرين، ٢٠١٤

٩. محمد امين الرومي، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٣ ، ص ١٨٧

١٠. محمد عبد الله أبو بكر، موسوعة جرائم المعلوماتية – جرائم الكمبيوتر والانترنت، المكتب العربي الحديث، الإسكندرية، ٢٠١١

١١. محمد لطفي عبد الفتاح، الاطار القانوني لحماية الخصوصية الجينية، مجلة جامعة الملك عبد العزيز، العدد ٠١ ، ٢٠١٣ .

١٢. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الالكترونية، دار النهضة العربية، القاهرة، ٢٠٠١

١٣. نائلة عادل محمد فريد، جرائم الحاسب الالي الاقتصادية، دار النهضة العربية، القاهرة، ٢٠٠٤

الفهرس

المحتويات	الصفحة
الملخص	٢
المقدمة	٤
أهمية البحث	٥
أهداف البحث	٥
المطلب الأول: أهداف قانون حماية البيانات الشخصية العماني والاستثناءات الواردة على البيانات المشمولة بالحماية	٦
الفرع الأول: أهداف قانون حماية البيانات الشخصية	٦
الفرع الثاني: الاستثناءات الواردة على البيانات الشخصية المشمولة بالحماية	٩
المطلب الثاني: حماية البيانات الشخصية الحساسة	١٠
الفرع الأول: البيانات الجينية أو الوراثية	١١
الفرع الثاني: البيانات الصحية	١٧
الفرع الثالث: البيانات الحيوية	١٩
الخاتمة	٢١
النتائج	٢١
التوصيات	٢٢
المراجع	٢٣