# الحماية الجزائية للهوية الرقمية "دراسة مقارنة".

# The penal protection of the digital identity (a comparative study).

بحث مقدم من قبل
المدرس المساعد حسين عباس حميد
كلية الصفوة الجامعة / قسم القانون

**الخلاصــة.**

لقد افرز التطور الهائل في تقنية المعلومات العديد من التطبيقات الناجحة، منها تطبيق الهوية الرقمية؛ الذي يُعد نتاجًا لتطبيق التحول الرقمي في الدولة، ومن الواضح ان الهوية الرقمية تمتاز اليوم باهتمام واسع من قبل العديد من الدول وهي تتجه نحو تحول منظومتها الإدارية نحو التحول الرقمي، والوصول للحكومة الذكية، فالهوية الرقمية هوية تعريفية شخصية تعتمد على مجموعة من الخوارزميات الخاصة، الهدف منها سرعة إنجاز المعاملات اليومية سواء الحكومية أو الخاصة، ويجب ان يضفى لها حماية تِقنية وتشريعية عالية المستوى، حيث إن نظام إلكتروني يعتمد على خوارزمية أنشأها الذكاء الاصطناعي بواسطة الانسان، وتحفظ بها معلومات الشخصية من اسمه وعمره ومحل السكن ووظيفته، وغيرها من تفاصيل الهوية الشخصية التقليدية ورقم تعريفي أو كما يسمى رقم كودي، وتكون تحت حماية حكومية امنية عالية المستوى.

**الكلمــات المفتاحيــة: الحمايــة ، الهويــة ، الرقميــة ، التحــول الرقمــي ، الــذكاء الاصــطناعي ، الجــرائم المعلوماتية.**

**Abstract.**

The tremendous development in information technology has resulted in Al-Aidi from successful applications, including the application of digital identity, which is a product of the application of e-government, and it is clear that the digital identity is characterized today by wide interest by many countries and they are moving towards the application of e-government and access to the smart government, the digital identity is an identity A personal identification based on a set of special algorithms, the aim of which is to speed up the completion of daily transactions, whether governmental or private, and must give them high-level technical protection, as it is an electronic system based on an algorithm created by artificial intelligence by humans, and in which personal information is preserved from his name and age. His age, occupation, and other traditional personal identification details and identification number, or as it is called a code number, are under high-level government security protection.

**Keywords: protection , identity , digital , digital transformation , artificial intelligence , information crimes**.

**المقدمـــة.**

**أولاً / التعريف بالموضوع.**

من الواضح الجلي ان العالم اليوم يتقدم ويتطور نتيجة الثورة المعلوماتية التي كشفت عن افكارِ غير متصورة وبعيدة المنال عن الفكر الجامد، وولدت هذه الحداثة العديد من التطبيقات التي اثرت بصورة واضحة على جميع اوجه النشاطات، وتعد الهوية الرقمية إحدى صور التطور التِقني، وعلى الرغم من تطبيق العديد من الدول لتقنية الهوية الرقمية إلا انها لم تشهد تقدمًا لدى العديد من الدول العربية؛ وهذا بسبب تردد بعض الدول في الأخذ بها لما تسببه من مشكلات قانونية عديدة، منها افتقار التشريعات لنصوص تنظم عمل التطبيقات الرقمية وذلك النصوص المجرمة والتي تكافح الجرائم المعلوماتية.

**ثانيًا / أهمية الموضوع.**

إن موضوع الهوية الرقمية يشكل اليوم أهمية كبيرة لدى الدول، في ظل التسارع الكبير في التحول نحو تطبيقات الحكومة الإلكترونية وكذلك الحكومة الذكية، إذ تعد الهوية الرقمية انعكاسًا للهوية الشخصية التقليدية ولكن بصورة أكثر تطورًا، وما زالت بعض الدول العربية والعالمية تتعامل بالصورة التقليدية أو الإلكترونية للهوية الشخصية، على عكس الكثير من الدول التي انتهجت منهجًا جديدًا وظهرت لديها الكثير من المبادرات نحو التحول الرقمي وانتشار الخدمات المالية الإلكترونية مما يستدعي تطبيق منظومة الهوية الرقمية.

**ثالثًا / اسباب اختيار الموضوع.**

ان السبب الأساس الذي أدى لاختيار موضوع البحث، هو اللحاق بالمتغيرات العالمية ومن ثم الاقليمية والمحلية، وجديرًا لما حصل من مستجدات تقنية من بداية الألفية الثالثة، واهتمامًا من اهتمامات الدول بموضوع التحول الرقمي ووضع أسس قانونية لهذه التقنيات؛ لتلافي المشكلات التي تحيطها، ويقينًا لما تسهل هذه الهوية من التعاملات الإلكترونية، وانعكاسًا لأهمية ما تقوم بها هذه البطاقة في سهولة الاستخدام، وخاصة في العميات اليومية، التي باتت صورتها الرقمية بارزة، وتوضيحًا لدور الدول في الأخذ بالهوية الرقمية وهي تسير نحو الحكومة الذكية التي تعمد في جميع معاملاتها الصورة الرقمية.

**رابعًا / مشكلة البحث.**

تتمثل مشكلة البحث في حداثة موضوع الهوية الرقمية وتطبيقاتها، وأثار تطبيق الهوية الرقمية العديد من التساؤلات لدى المتخصصين بمدى صحة التعامل بالهوية الرقمية في التعاملات الرسمية، وكيف يتم حمايتها سواءً من الناحية التقنية أو الجنائية؟وعلى الرغم من الفوائد التي توفرها التقنية والتحول الرقمي في الدول ألا أنه لا يمكن أن ننكر ان هذا التحول يصاحبه العديد من المشكلات، وابرز ما يواجه هذا التحول هو الجريمة المعلوماتية، والمجرم المعلوماتي، الذي بات يهدد كُلّ القطاعات الحكومية أو الخاصة؛ لما يمتلكه من قدرة على الاختراق أو الاعتداء على النظام الرقمي، كما إن حماية البيانات اليوم وعدم التعدي على الخصوصية تشكل خطورة كبيرة أصابت العالم الرقمي اليوم، إذ تُعد الجريمة المعلوماتية من أبرز تحديات العصور الرقمي، وسعت الكثير من الدول من خلال عقد اتفاقيات دولية أو اقليمية أو تشريع قوانين داخلية تحد وتكافح هذا النوع من الجرائم.كما انه من التحديات التي تبرز هنا ان الهوية الرقمية هي تطبيق محلي فكيف سيتم الاعتماد عليها في دول لا تستخدم التِقنية في تعاملاتها؟، كما كيف سيتم التعرف بموثوقية التحول الكبير في المعرفات الاخرى مثل جواز السفر الرقمي وغيرها من الهويات الرقمية؟

**خامسًا / هدف الدراسة.**

تهدف الدراسة من خلال معرفة ماهية الهوية الرقمية واهميتها، وكذلك المواجهة العقابية في حالة التعدي عليها، مما يسهل على المشرع الجهات القائمة على إصدارها في تبني بناء قانوني وتقني يواجه مخاطر التعدي عليها.

**سادسًا / منهجية البحث:**

سنعتمد في البحث المنهج التحليلي والمقارن، وسيلجأ الباحث لعدم التقيد في المنهج المقارن في تحديد نطاقه؛ يعود السبب في ذلك إلى أن الباحث إستشف أن من اللازم أن يحيط بعدد كبير من التجارب بما يتعلق بالهوية الرقمية، ومن هذا البحث نبين الدور الإيجابي والمحسوس وأيضًا المهم للتحول الرقمي ليشمل جميع القطاعات والاستخدامات.

**سابعًا / خطة البحث.**

المبحث الأول: ماهية الهوية الرقمية.

المطلب الأول: مفهوم الهوية الرقمية.

المطلب الثاني: خصائص الهوية الرقمية.

المبحث الثاني: جريمة الاعتداء على الهوية الرقمية.

المطلب الأول: الحماية الوقائية للهوية الرقمية.

المطلب الثاني: الجزاءات الجنائية في التعدي على الهوية الرقمية.

الخاتمة:

أولًا: الاستنتاجات.

ثانيًا: المقترحات.

**المبحث الأول / ماهية الهوية الرقمية .**

لا يخفى على الجميع التطور الذي شهده العالم وخاصة في المجال المعلوماتي، فدخلت التقنية في مجالات الحياة كافة، وكان من اللازم ان تنتهج الدول هذا الطريق، وفي محور بحثنا ومع دخول التقنية في كُلّ المجالات صار من اللازم ان تتجه نحو الهوية التعريفية للشخص، فتحول العالم نحو حكومات بلا ورق ينهي الاستخدام الكبير للأوراق وما شابهها في التعاملات اليومية، فالهوية الرقمية ما هي سوى تقنية حديثة تستخدم الذكاء الاصطناعي في هيكلتها وبناءها، لذا سنقسم هذا على مطلبين نذكر في المطلب الأول ماهية الهوية الرقمية، في حين سنخصص المطلب الثاني لخصائص الهوية الرقمية.

**المطلب الأول / مفهوم الهوية الرقمية .**

إن الهوية الرقمية تطبيق حديث أنتجته التِقنية في سبيل مواكبة التطور والتحول نحو الرقمنة في جميع العمليات الحكومية، وكذلك الشخصية، إذ ان العالم الرقمي، اليوم بأكمله محكوم بالشبكة العالمية - الإنترنت-، إذ إنه ومن خلالها حولت البيانات المدونة على الورق لصورة رقمية، فالفائدة من نقل المعلومات رقميًا هي إدارة المصداقية بين الجانبين (المرسل والمستقبل)، لإجراء تحويل موثوق عبر الشبكة العالمية -الإنترنت-. إذ تعد الهوية الشخصية الرقمية، هوية وطنية لجميع المواطنين، وكذلك يمكن تنشأ هكذا هوية للمقيمين في الدولة، إذ تسمح بوصول المستخدمين إلى خدمات الهيئات الحكومية المحلية والاتحادية، ومزودي الخدمات الآخرين، لذا تقدم الهوية الرقمية بطبيعة الحال حلولاً يسيرة في الولوج للخدمات عبر الهواتف الذكية دون الحاجة إلى كلمة سر أو اسم مستخدم، فضلاً عن إمكانية التوقيع على المستندات رقمياً، والتحقق من صحتها دون الحاجة لزيارة مراكز الخدمة، إن الانطلاق الاول في الدول العربية كان لدى دولة الامارات العربية، إذ اطلقت تطبيق الهوية الرقمية في معرض جيتكس للتقنية 2018، وهو مشروع مشترك بين دبي الذكية وهيئة تنظيم الاتصالات والحكومة الرقمية وهيئة ابو ظبي الرقمية، إذ كان الهدف المرجو من هذا التطبيق الجديد هو خدمة لأهداف حكومة دولة الإمارات الرامية إلى تحقيق التحول الرقمي والتخلص من المعاملات الورقية [1]. وحسب ما ارفد معهد ماكينزي لتعريف الهوية الرقمية حيث عرفها بانها الهوية التي تصادق عن بُعد بواسطة القنوات الرقمية، ويتم التحقيق من الهوية والمصادقة عليها بدرجة عالية من التأكيد وبمعرّف رقمي فريد ويكون إنشاء هذه الهوية بموافقة

فردية، كما وتضمن خصوصية للمستخدم في التحكم في البيانات الشخصية [2].وعرفت الهوية الرقمية من قبل المشرع المصري بانها "أي بيانات معالجة تقنيًا تتعلق بشخص طبيعي أو اعتباري محدد أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات واي بيانات أخرى كالاسم، أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر الإنترنت، على ان تسمح هذه البيانات بالتقييم أو المصادقة على المعاملات التي تتم من خلال المنصات الرقمي" [3]. فالهوية الرقمية عبارة عن صورة فوتوغرافية لحاملها، وتحمل توقيعه واسمه وكود هويته الشخصية -القومية- وتاريخ ومكان ميلاده ونوعه وجنسيته وتفاصيل محل إقامته، حتى وإن كان مقيمًا في تلك الدولة بصفة مؤقته بموجب تصريح إقامة، بالإضافة إلى مجموعة شاملة للصفات التي تحدد هويته القانونية، كما إن هذه البطاقة يجب أن يتوفر بها رقمًا خاصًا وتاريخًا للإصدار والانتهاء، وتضم هذه البطاقة مفتاحين وشهادتين واحدة للتوثيق، وواحدة للتوقيع الإلكتروني [4]. إن الثورة الجديدة المتمثلة باستخدام الذكاء الاصطناعي والبيانات الضخمة قد فتحت بالفعل بوابة لإثراء حياتنا اليومية وإمكانياتها، ففي مثل هذه الأمور تستثمر البلدان المتقدمة بشغف قدرًا كبيرًا من الموازنة العامة للدولة، إذ يحصل الابتكار والتقدم في المجالات الأكاديمية والصناعية، مثل الذكاء الاصطناعي، البيانات الضخمة، والصحة الطبية، وتقنية المعلومات والاتصالات على وجه الخصوص، إذ وافقت حكومة اليابان على ان تبلغ الميزانية الإجمالية حوالي (700 مليون دولار أمريكي) لأبحاث الذكاء الاصطناعي في 2018، أما الولايات المتحدة تستعد بالفعل لما لا يقل عن (4.5 مليار دولار أمريكي) الاستثمار في الذكاء الاصطناعي، ويبدو أن الصين تستثمر أيضًا أكثر من (4.0 مليار دولار أمريكي) للاستثمار في الأبحاث والتطورات المتعلقة بالذكاء الاصطناعي، ومن المؤكد أن تزيد البلدان عن ستة أضعاف حجم استثمار اليابان في الذكاء الاصطناعي [5]. تُعد الهوية الرقمية اليوم من الموضوعات المهمة في الخدمات المالية، إذ تعمل أنظمة الهوية الحالية على الابتكار في التقنية المالية، وكذلك تقديم خدمات آمنة وفعالة في الخدمات المالية والمجتمع على نطاق أوسع، فالهوية الرقمية معترف بها على نطاق واسع؛ لأنها الخطوة التالية في أنظمة الهوية، ومع ذلك فأن العديد من الجهود جارية لحل أجزاء من تحدي الهوية وإنشاء هوية رقمية حقيقية [6].من بين الأسئلة المثارة في هذا المجال هو موضوع كيفية تعرف الدولة على مواطنيها، فالهوية الرقمية ما زالت في بداية نضجها، إذ ان الحكومة التقليدية قادرة على التعرف على مواطنيها من خلال جواز السفر أو الهوية الورقية، اما في البطاقة الرقمية كيف ستتمكن من الحكومة الالكترونية والحكومة الذكية في التعرف على مواطنيها؟

للإجابة عن ذلك وبكل سهولة هو ان هنالك هوية رقمية أو إلكترونية قادرة على التعريف بالأشخاص، وغير قابلة للنقل من شخص لآخر، وتمتاز بمأمونيتها وموثوقيتها، كما أن هنالك العديد من الدول بالفعل تدرس إمكانية استخدام مكونات مادية، وليس فقط مكونات منطقية لمعالجة كُلّ الجوانب المحيطة بالهوية الرقمية [7]، من الواضح أن جواز السفر الإلكتروني السويدي هو الأكثر أمانًا وتقدمًا [8]. فمن الضروري الاعتماد بصورة كبيرة على الخوارزميات في سبيل تحقيق هوية رقمية جديدة أسهل، وأسرع في الاستخدام؛ لان البطاقة المادية في طريقها أيضًا للأفول، إذ من الصعب أن يحمل الشخص أكثر من بطاقة تعريفية، سواء شخصية، أو للاستخدامات الأخرى مثل إجازة السوق، والبطاقة المصرفية، وغيرها من بطاقات الإلكترونية، فالهوية الرقمية تجعل بطاقات الاستخدام كافة في حافظة رقمية في الهاتف المحمول، وهي مؤمنة بكل وسائل الحماية من الاختراق. والجدير بالذكر بأن الحافظة الرقمية الموجودة في الهاتف والتي باتت أغلب شركات الهاتف المحمول تعتمدها، فقد جعلت العديد من الشركات بطاقتها المصرفية بصورة رقمية في حافظة مؤمنة، لذا لا بد للدول في التحول نحو هكذا حافظات في سبيل التحول الكبير في الهوية الرقمية.إن موضوع الهوية الرقمية من قبل أن تسرع الجائحة من التحول إلى عالم أكثر ترابطًا، كانت الهوية الرقمية تُعدّ من أبرز التوجهات العامة التقنية، وخاصة بالنسبة للعالم النامي، ووفقًا لما أوردته مجموعة البنك الدولي، هناك (١,١ مليار) نسمة حول العالم لا توجد لديهم وثائق أو مستندات موثوقة

لإثبات هويتهم، ولأجل ذلك سعت العديد من الدول لعقود طويلة في محاكاة تجربة الهند الناجحة في تنفيذ برنامج آدهار (Aadhaar) لتحديد الهوية الرقمية، ونظام تحديد الهوية الوطنية في إستونيا المعروف باسم "إستونيا الإلكترونية" (e-Estonia)، ومن المزايا المتوقعة في هذا الخصوص ازدياد الشفافية الحكومية فيما يتعلق بالموازنة والانتخابات، على سبيل المثال، وسهولة الحصول على المساعدات الحكومية، واتساع فرص الاستفادة من الخدمات المالية الأساسية، لا سيما بالنسبة للمواطنين النازحين والذين لا يحملون وثائق لإثبات هويتهم، وعلى مدار سنوات، تباطأت عملية اعتماد هذه التقنية نتيجة عدة تحديات، تراوحت بين عدم كفاءة التنسيق على المستوى الوطني، وبين محدودية الإلمام بالتقنية الرقمية، كذلك كانت قضايا الأمن الرقمي، والشواغل المتعلقة بخصوصية البيانات، وانعدام الثقة في الأدوات التقنية التي توفرها الحكومة وراء تأجيل تفعيل الهوية الرقمية في كثير من البلدان، وما تزال التحديات التي لم تتم تسويتها غالبًا وراء إقصاء برامج الهوية الرقمية إلى الصفوف الخلفية في ترتيب الأولويات، ولكن جائحة كورونا دفعت الحكومات إلى سرعة تجاوز هذه القضايا أو تنحيتها جانبًا لتقديم المساعدات المالية التي توجد حاجة ماسة إليها، وغير ذلك من صور الدعم للمواطنين الأشد تعرضًا للمخاطر، وقد حان وقت العمل، فالمزايا المترتبة لتفعيل برامج الهوية الوطنية الرقمية، بما في ذلك ما تنطوي عليه من إمكانات لبناء قواعد بيانات موثوقة مزودة بمؤشرات اجتماعية- اقتصادية، تفوق حاليًا في أهميتها بعض الشواغل الموضوعات القائمة [9]. كما ان تجربة المملكة العربية السعودية في تنفيذ التحول الرقمي وما يخص الهوية الرقمية، تُعد من التجارب الحديثة والمتطورة في مجال الهوية الرقمية، إذ أعتمد تطبيق توكلنا [10] وسيلة رقمية آمنة وموثوقة لاستعراض الهوية الرقمية للمواطن والمقيم، إذ أطلقت وزارة الداخلية بالتعاون من الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) مشروع (الهوية الرقمية) عن طريق تطبيق توكلنا، وقد شملت (الهوية الوطنية للسعوديين وهوية مقيم للمقيمين)، لتمكّن الاستخدام الرسمي لها بصفتها وسيلة إثبات إلكترونية؛ وقد جاء هذا ضمن تعاون مشترك الهدف منه رقمية الوثائق الثبوتية الحكومية، في اشارة إلى ذلك نوّهت الوزارة إلى ان الهوية الرقمية في تطبيق توكلنا، مطابقة للهوية الرقمية في تطبيق وزارة الداخلية الالكتروني [11]. إن الهوية الرقمية ما هي سوى وسيلة تعريفية تستخدم كبطاقة تعريفية رقمية، تسهل الكثير للمستخدم في الوصول للخدمات الحكومية دون الحاجة للآليات المتبعة في الحكومات التقليدية، فهي هوية تعريفية شخصية تعتمد على مجموعة من الخوارزميات الخاصة، الهدف منها سرعة إنجاز المعاملات اليومية، سواء الحكومية أو الخاصة، ويجب ان يضفى لها حماية تِقنية عالية المستوى، ومن خلال ذلك يمكننا ان نرفد تعريفًا للهوية الرقمية فتعرف بإنها "نظام رقمي يعتمد على خوارزمية أنشأها الذكاء الاصطناعي بواسطة الانسان، وتحفظ بها معلومات الشخص الشخصية من اسمه وعمره ومحل سكنه، ووظيفته، وغيرها من تفاصيل الهوية الشخصية التقليدية ورقم تعريفي أو كما يسمى رقم كودي، وتكون تحت حماية حكومية أمنية عالية المستوى".

**المطلب الثاني / خصائص الهوية الرقمية.**

إن الهوية الرقمية هي خدمة للتعريف عن الشخص لدى الحكومة أو اي جهة أخرى وبالتالي الولوج داخل الحدود الرقمية، فالخصائص التي تتميز بها الهوية الرقمية هي نتيجة مهمة ومتطورة في التطور العلمي والتقني وصلت له البشرية في العصر الرقمي والذكاء الاصطناعي. إن غالبية الدول وهي في طور البحث عن أفضل وأنجع الطرق في مواكبة التِقنية على الصعيد العالمي وذلك بالأساليب والبيانات والطرق المتاحة كافة لمواجهة العديد من التحديات التي فرضها الواقع وتطورات العصر، كما هو المعروف ان القطاع الحكومي في الدولة وجد ليلبي احتياجات مواطنيها ويقدم الخدمات التي ترتقي بيه عاليًا، لذا نجد ان هذا القطاع ذا أهمية لدى الحكومات وذلك من خلال الشعور لتحقيق التحسن المستمر فيه في مجال تقديم الخدمات والسعي بصورة دؤوبة لتحقيق التطور في مختلف المجالات والاستفادة من التقنيات الحديثة وخاصة ما يتعلق بتقنية المعلومات، إذ أدت تقنية المعلومات والإتصالات تطورات كبيرة -لربما لم تكن

لتتصور- سواء على مستوى الافراد ورغبتهم في الحصول على خدمات بصورة حديثة، أم على مستوى المؤسسات والهيئات القائمة تقديم على تلك الخدمات، إذ بات إدخال تقنية المعلومات في الأعمال الحكومية في أعمالها كافة من أولويات الحكومات التي تبحث عن التمييز والريادة [12]. إن وجود الحكومة المتنقلة (Government Mobile) يكون الاستخدام الواسع فيها للأجهزة المحمولة، إذ يمكن الوصول إلى الشبكة العالمية -الإنترنت- في كُلّ مكان تقريبًا، وفي الحقيقة أن هنالك نسبة الكبيرة من المواطنين تستخدم الأجهزة المحمولة مثل الهواتف الذكية والأجهزة اللوحية للوصول إلى الشبكة العالمية -الإنترنت- مما يؤدي هذا الاستخدام للكثير من المشكلات، تعزز الحكومة المتنقلة، ووسائل التواصل الاجتماعي بعضها بعض في طريق تطوري مشترك، وهذا في نهاية المطاف يحقق للمواطن تحسين الاستجابة العامة [13].

التحول الرقمي يمتلك القدرة على تحسين وتسريع أمن الحدود الرقمية من خلال بوابات التحكم الآلي والحد من الاحتيال على الهوية الرقمية من خلال القياسات الحيوية، وتقديم خدمات جديدة وسريعة على الشبكة العالمية -الإنترنت- للمواطنين، تُعدّ إمكانات المعالجة السريعة غير المادية ضرورية جدًا في التعامل، لا سيما مع التطبيقات المتعددة مخططات تجمع بين وظيفة إصدار التذاكر والدفع، ويتوقف مستقبل وثائق الهوية الحكومية الرقمية على الأمان والاداء والقدرة على التكييف مع تمكين رقائق الأمان المضمنة [14]. إن الوصول لتِقنية الهوية الرقمية تُعد من مراحل تطوير الدولة الرقمية، وتعد تقنية Near Field Communication -NFC من أبرز التقنيات المستخدمة في هذا النوع من البطاقات الرقمية، وتتضمن هذه الواجهة برمجيات خاصة لقراءة البيانات من الشريحة الذكية في بطاقة الهوية والقيام ببعض العمليات المحوسبة لتأكيد هوية المستخدم الرقمي، وبناءً على آلية تصميم هذا التطبيق، فأن المستخدم على سبيل المثال سيقوم فقط بتمرير بطاقة الهوية الذكية على الجهاز المحمول الذي يتطلب أن تتوافر فيه خاصة الاتصال اللاسلكي (NFC)، وبعدها يقوم التطبيق بقراءة البيانات في الشريحة الذكية بالبطاقة -أو البطاقة الرقمية غير المادية- والتأكد من الشهادات الرقمية، وطلب إدخال الرمز السري والتحقق منه، ومن ثم إثبات المعاملة بالتوقيع الرقمي، كُلّ ذلك يتم من خلال آليات مشفرة بمعايير أمنية عالمية يمكن أن تلبي متطلبات الحكومة الرقمية في ضمان سرية وموثوقية عمليات تأكيد الهوية [15]. إن التحول نحو نظام الهوية الرقمية يَمتازُ بالعديدِ من المميزاتِ التي تجعل التعامل الرقمي أسهل وأيسر، فلا محيص من الالتجاءِ إليه اليوم من خلال ما يتيح هذا النظام من فوائدِ جمة، في الحقيقةِ أن الاستعانةِ بالوسائلِ التِقنية واستعمالها في التعاملات هو أمرٌ ضروري في ظلِ هذا التدفقُ الهائلِ من الأجهزةِ المعلوماتية واستعمالاتها. ومن البديهي أن توفير المعلومات اللازمة وإمكانية الوصول إلى الخدمات بيسر وسهولة وتوضيح التعليمات والارشادات اللازمة وبهذا يمكن اجمال العديد من الخصائص التي تتميز بها الهوية الرقمية: [16]

- تطوير وصول رقمي متكامل للمعلومات والخدمات الحكومية.
- تسهيل عملية دفع الرسوم المختلفة عبر الشبكة العالمية -الإنترنت-.

في مجال الخصائص التي تتميز بها الهوية الرقمية فإنها تقلل الاعتماد على الهوية الورقية كما تحقق الهوية الرقمية الاتصال الفعال بين العديد من الخدمات [17]. إذ يمكن وبصورة واضحة ان تسهم الهوية الرقمية في العديد من تسهيل الوصول للخدمات بضغطة زر، فلا يكلف الوقت سوى بضع ثوان للتقديم على خدمة أو غيرها من الاستخدامات. كما ان الخصيصة التي تمتاز بها الهوية الرقمية، مرونة وسهولة في التواصل، إذ تسهل ربط العلاقات وبناء التعاقدات مع فاعلين كان من الصعب أو المستحيل الوصول إليهم في الفضاء الحقيقي، هذه المرونة في التواصل بطبيعة الحال تجعل المؤسسة أكثر حرية في تعاقداتها؛ لأن الفضاء الرقمي يفتح الأبواب لفضاء رحب مليء بالمتعاملين، وهذا يزيد فرصها في أختيار أحسن العملاء بأحسن الشروط، مما يسمح للمؤسسة بتشكيل شبكة علاقاتها وتحديثها بصورة مستمرة حسب التطورات التي يعرفها الفضاء الرقمي والذي في كُلّ مرة يزيد من حجم الفاعلين وينشأ آليات رقمية

تسهل التواصل [18]. فالهوية الرقمية بخصائصها المتعددة تكون خطوة نحو التحول الرقمي في الدول، إذ بها تسعى الدول في تقدمها نحو الريادة العالمية في التحول الرقمي، فخصائص الهوية الرقمية نتيجة متكاملة لخصائص الحكومة الإلكترونية، فالفوائد التي تصلنا من الهوية الرقمية هي بطبيعة الحال فوائد الحكومة الإلكترونية باختلاف جزئيات صغيرة، إذ إن الهوية الرقمية جزء من التحول الحكومي نحو الحكومة الإلكترونية والوصول للحكومة الذكية، التي يكون فيها التعامل بالمطلق رقميًا، فلا ورق هنا، ولا يعتمد نهائيًا في جميع التعاملات، وما نشاهده اليوم في تبني العديد من الدول الهوية الرقمية هو لإيمانها الكامل والمطلق بأن التحول الرقمي هو سمة العصر الحديث، فالدول التي لا تعمد آليات التحول الرقمي ستبقى دول عالم ثالث لا تتقدم إلّا ببطء شديد. ان التحسين في مستوى الخدمات، فالإشارة الرقمية أقل عرضة للضوضاء والتشويش والتداخل، كما إن التقنية تتسم بقدر عال من الذكاء في التعامل مع المعلومات والبيانات أي كان نوعها والتحكم في اوضاعها واستخداماتها، كتصحيح الاخطاء رقميًا، كما تمكن التقنية من تخزين واسترجاع عدد لا يحصى من البيانات في ذاكرة صغيرة نسبيًا، وأيضًا تقلص حجم المعدات ووسائل الاتصال، وكذلك المرونة التي تسمح بتحقيق قدر عال من جودة الاستخدام وذلك بخضوع النظم الهوية الرقمية للتحكم من جانب برامج الحاسوب الإلكتروني [19]. ومن تلك الخصائص التي ذكرت، فلا مجال للحكومات للتهاون بتطبيق الهوية الرقمية، إذ من خلالها تستطيع أن تقدم الخدمات بكل يسر، كما لا بُدَّ لها وهي في طور السعي أن تقتدي الدول بمجموعة التجارب لدى الدول التي تستخدم الهوية الرقمية في تعاملاتها.

**المبحث الثاني/ جريمة الاعتداء على الهوية الرقمية.**

إن التطور الكبير الذي نلاحظه في الوقت الحالي وبروز التقنية في غالبية المجالات، قد أحدث نوعًا جديدًا من الجرائم ما تسمى اليوم (بالجرائم المعلوماتية) التي تحمل خصوصية جديدة في عالم الجريمة ومكافحتها، ومن بين هذه الجرائم جريمة الاعتداء على الهوية الرقمية، لذا من خلال هذا المبحث سنحاول ان نركز على طرق حماتها الجنائية من خلال مطلبين نخص الاول بالحماية الوقائية للهوية الرقمية، أما في الثاني سنذكر فيه الجزاءات الجنائية في التعدي على الهوية الرقمية.

**المطلب الأول/ الحماية الوقائية للهوية الرقمية.**

إن طبيعة الهوية الرقمية تحتم علينا البحث عن طرق حماية جديدة بعيدة عن طرق الحماية السابقة المتبعة في عالم التصدي للجريمة التقليدية، ففي هذا النوع من الجرائم يجب أن نخصص حماية تقنية، وهو ما يطلق عليه بالحماية الوقائية التي تتميز في منع محاولة ارتكاب الجريمة، أو ايقافها حال وقوعها؛ مما سيقلل من الاضرار، ثم بعد ذلك وفي افتراض وقوع الجريمة نجد هنالك حماية موضوعية جديدة ستظهر هي وضع العقوبات لحالة الاعتداء. إن القوانين المقارنة في غالبيتها كانت تعتني بهذا النوع من الجرائم حتى تضع الاجراءات الوقائية والعقوبات المناسبة لمرتكبها، ففي فرنسا أصدر المشرّع القانون رقم (١٧ لسنة ١٩٧٨) الخاص بالمعالجة الآلية للبيانات والحريات، إذ تضمن الباب الأول منه مجموعة من المبادئ القانونية التي أشارت إلى أن المعالجة الإلكترونية للبيانات يجب أن تكون لخدمة المواطن فقط، ولا يجوز أن تتضمن اعتداءات على شخصيته، أو حياته الخاصة وحرياته، أما في بابه الثاني انشئ ما اطلق عليه اللجنة القومية الخاصة بمراقبة تنفيذ أحكام هذا القانون ووجوب استشارة اللجنة قبل معالجة البيانات، وتطبيقًا لذلك قضت محكمة (Nantes) بتاريخ (١٩٨٥/١٢/١٦) بإدانة شخص قام بإجراء معالجة إلكترونية للبيانات الشخصية، دون الإخطار السابق لهذه اللجنة، كما أن الاستثناء الذي ورد في القانون يشمل نقطتين الأولى: تتعلق في حالة جمع البيانات الضرورية في اثبات الجرائم، واشترط المشرع في هذه النقطة أن يكون هذا التخزين لدى جهات قضائية أو لدى السلطات العامة، فلا يجوز لجهات القطاع الخاص وغير الجهات المشار اليها بصفة عامة ادخال مثل هذي البيانات إلى الحاسوب الخاص بها، أما الثانية تتعلق بحرية الصحافة بنشر البيانات الشخصية المعالجة في موضوع معين في إطار حرية التعبير

[20] وحسب التوجه الاوربي رقم (٢٠٠١/٢٩) عبر عن التدابير التقنية بأنها "أي تِقنية، سواء أجهزة، أو أدوات، مصممة لأداء غرض المنع، أو التقييد اعمال غير المصرح به من قبل صاحب الحق، وتُعدّ هذه التدابير فعالة عندما يتم التحكم في استخدام عمل محمي أو موضوع آخر من قبل اصحاب الحقوق من خلال تطبيق التحكم في الوصول، أو عملية الحماية، مثل التشفير" [21]وقد عرف قرر رقم (109 لسنة 2005) المصري الخاص بإصدار اللائحة التنفيذية لقانون التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات التشفير بإنه "منظومة تِقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة إلكترونيًا بحيث تمنع استخلاص هذه البيانات والمعلومات إلّا عن طريق استخدام مفتاح، أو مفاتيح فك الشفرة" [22]والحماية التقنية تركز على وجود أمن معلوماتي قويم، فقد عرف أمن المعلومات من ناحية تقنية بأنه العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها، ومن أنشطة الاعتداء عليها، أو هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الاخطار الداخلية والخارجية، أما من الناحية القانونية بانه "محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفير المعلومات ومكافحة أنشطة الاعتداء عليها واستغلال نظمها في ارتكاب الجريمة، وهو هدف وغرض تشريعات حماية المعلومات من الانشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها" [23] فمن الوسائل الأمنية التي لا بُدَّ من الاستعانة بها في تأمين الهوية الرقمية هو اتباع طرق علمية رصينة في التأمين، ونخص بذلك:

- وسائل الأمن من حيث الطبيعة والغرض: [24]

وسائل أمن المعلومات هي مجموعة من الآليات والإجراءات والادوات والمنتجات التي تستخدم للوقاية من أو تقليل المخاطر والتهديدات التي يتعرض لها الحاسوب والشبكات وبعامة نظم المعلومات وقواعدها، ووسائل الأمن متعددة من حيث الطبيعة والغرض، لكن يمكن بصورة أساس تصنيف هذه الوسائل من منظار غرض الحماية.

- مجموعة وسائل الأمن المتعلقة بالتعريف بشخص المستخدم، وتوثيق الاستخدام، ومشروعيته Identification and authentication: وهي الوسائل الهادفة لضمان استخدام النظام أو الشبكة من قبل الشخص المخول بهذا الاستخدام، وتضم هذه المجموعة كلمات السر بأنواعها، والبطاقات الذكية المستخدمة للتعريف، ووسائل التعريف البيولوجية التي تعتمد على سمات معينة في شخص المستخدم متصلة ببنائه البيولوجي، ومختلف أنواع المنتجات التي تزود كلمات سر آنية أو وقتية متغير رقميًا، والمفاتيح المشفرة، بل وتضم هذه المجموعة ما يعرف بالأقفال الرقمية التي تحدد مناطق النفاذ.

- مجموعة الوسائل التقنية المتعلقة بشخص المستخدم: حيث إن الهدف من هذه المجموعة لضمان استخدام الهوية الرقمية من قبل الشخص المخول بهذا الاستخدام، كما وتهدف هذه المجموعة لضمان عدم قدرة الشخص المستخدم من إنكار أنه هو الذي قام بهذا التصرف [25] إن هذه المجموعة تحتوي على العديد من أمن الأدوات منها كلمات السر الخاصة بالهوية الرقمية وبصمته الشخصية، وتعد بصمة الابهام من البصمات التقليدية في استخدامها، إذ اعتمدت العديد من الدول والمؤسسات بصمة الوجه والعين بديل لها، كما تحتوي على مفاتيح الشفرات الخاصة بالبطاقة السابقة والحالية. ومن أجل ذلك سيتطلب تهديد الهجمات السيبرانية المدعومة من الذكاء الاصطناعي الاستثمار في الدفاع السيبراني للمنتجات الجديدة المدعومة من الذكاء الاصطناعي، وهي مصدر قلق كبير للعديد من الدول في العالم، كما أن التحقق من الهوية الرقمية عن بُعد استنادًا إلى التعرف على الوجه قد يفتح الباب لسرقة الهوية الممكّنة للذكاء الاصطناعي [26] ومن بين وسائل التقنية المتعلقة بحماية الهوية الرقمية ما يعرف (بالتشفير)، إذ يُعد من أبرز الوسائل والأدوات لحماية الهوية الرقمية، وذلك من خلال توفير أمن وسلامة وسرية المعلومات والمعاملات والصفقات في الشبكة العالمية -الإنترنت- وقد عرف التشفير في الفقه "بانه آلية بمقتضاها

تترجم معلومة مفهومة لمعلومة غير مفهومة، من خلال تطبيق بروتوكولات سرية قابلة للانعكاس، أي يمكن إرجاعها إلى حالتها الطبيعية" [27]. كما إن التشفير قد عرف بأنه "منظومة تِقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة إلكترونيًا بحيث تمنع استخلاص هذه البيانات والمعلومات إلّا عن طريق استخدام مفتاح أو مفاتيح فك الشفرة" [28]. والتشفير يؤدي مهمة كبيرة ان لم نقل بإنها أفضل طرق حماية الهوية الرقمية لغاية هذه اللحظة، إذ يمكن حماية هذه البطاقة من خلال تشفير البيانات، إذ لا يمكن لأي شخصٍ غير المخول بذلك في الاعتداء على الهوية الرقمية، سواء من خلال الاختراق، أو إساءة الاستخدام منً قبل المستخدم، لا من اللازم أن تُعتمد هذه التقنية، وبصورة كبيرة من قبل الحكومات، وهي ترمي في التحول نحو استخدام الهوية الرقمية في تعاملاتها وتوجها نحو الحكومة الذكية. بلا شك إن لأمن المعلومات أهمية كبرى، وتتجلى هذه الأهمية في كون هذا المجال يقوم بتأمين المعلومات وحمايتها من الاخطار التي تحيط بها، كما يقوم بتوفير الحماية والأمان للحاسوب والشبكات، حيث عرّفت توصيات أمن أنظمة المعلومات والاتصالات لوكالة الأمن القومي في الولايات المتحدة الامريكية أمن انظمة المعلومات بأنها "حماية أنظمة المعلومات ضد أي وصول غير مرخص أو تعديل المعلومات أثناء حفظها، معالجتها أو نقلها، وضد ايقاف عمل الخدمة لصالح المستخدمين المخولين أو تقديم الخدمة لأشخاص غير مخولين، بما في ذلك جمع الإجراءات الضرورية للكشف، توثيق ومواجهة هذه التهديدات" [29]. ومن خلال ذلك من اللازم أن تتشكل هيئات وجهات متخصصة في هذا النوع من الأمن ويمكن ان يطلق عليها -الأمن الرقمي-، لمواجهة أي هجمة تصيب النظام المعلوماتي للمحافظة على سرية البيانات، وأيضًا من أجل ان لا تخترق وتكون عرضة للمساس بالأمن القومي للدولة.

**المطلب الثاني/ الجزاءات الجنائية في التعدي على الهوية الرقمية.**

إن الهوية الرقمية تعتمد بصورة كبيرة على الشبكة العالمية -الإنترنت-، إذ تعد هذه البيئة الخصبة للمجرم المعلوماتي في ارتكاب جرائمه الخطرة التي تهدد الأمن الرقمي للدول، وقطاعاتها الحرجة، لذا حاولت وسعت الكثير من الدول في سبيل الحد من هذا الجرائم، وذلك من خلال تشريع القوانين المناسبة للحد ومكافحة الجرائم التي تقع في البيئة الرقمية. وقد عرفت البنية التحتية المعلوماتية الحرجة كما جاءت بها (المادة الأولى) من قرار رئيس مجلس الوزراء المصري (رقم ١٦٩٩ لسنة ٢٠٢٠) بإصدار اللائحة التنفيذية للقانون رقم (١٧٥) لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، بأنها "مجموعة من أنظمة أو شبكات أو اصول معلوماتية أساسية يؤدي الكشف عن تفصيلاتها تعطيلها أو تغيير طريقة عملها بطريقة غير مشروعة، أو الدخول غير المصرح به عليها، أو الدخول أو الوصول بشكل غير قانوني للبيانات والمعلومات التي تحفظها أو تعالجها، أو يؤدي القيام بأي فعل غير مشروع آخر بها إلى التأثير على توافر خدمات الدولة ومرافقها الاساسية أو خسائر اقتصادية أو اجتماعية كبيرة على المستوى الوطني، ويُعدّ من البنية التحتية المعلوماتية الحرجة على الاخص ما يستخدم في الطاقة الكهربائية الغاز الطبيعي والبترول، الاتصالات، والجهات المالية والبنوك، والصناعات المختلفة، والنقل والموصلات والطيران المدني، والتعليم والبحث العلمي، والبث الاذاعي والتليفزيوني، ومحطات مياه الشرب والصرف الصحي والموارد المائية، والصحة، والخدمات الحكومية وخدمات الإغاثة وخدمات الطوارئ، وغيرها من مرافق المعلومات والاتصالات التي تقد تؤثر على الأمن القومي، أو الاقتصاد القومي والمصلحة العامة وما في حكمها". إن جريمة انتهاك سرية وخصوصية البيانات تُعد من أكثر الجرائم شيوعًا وأكبرها انتهاكًا، كما يمكن عدها من بين النقاط المهمة في حماية نظام المعلومات، إذ إنه يعتمد على عوامل عديدة، أبرزها السرية، وأيضًا من بين العوامل هذه حرية تداول البيانات، ثم اتاحتها وفي النهاية سلامة البيانات، فالسرية تعني عدم معرفة غير أطراف التعامل ببيانات العملية، في حين تعني الخصوصية ارتباط هذه البيانات بالأطراف، وهي نتيجة حتمية في عدم اطلاع الغير عليها [30]. إن سرية بيانات الهوية الرقمية ما هي الا اولوية حكومية لا بد من حمايتها تقنية وتشريعيًا، إن الهوية بصورتها

الرقمية نموذج حديث يكون من خلال تطبيق رقمي خاص يكون تحت انشاء وحماية الجهات المختصة في الدولة، فمن خلاله يستطع المواطن أو المقيم في استخدام هويته الرقمية من خلال هذا التطبيق الرقمي فالمحافظة على سرية وأمن المعلومات والبيانات داخل التطبيق أولوية تقنية لا بُدَّ أن تحظى بقوة رادعة في القانون، ومن خلال ذلك نجد ان الكثير من الدول قد نظمت وحمت البيانات الحكومية من خلال قوانينها الخاصة. فقد عالج القانون المصري ذلك في نص المادة ٢٠ من قانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات المصري، بعقوبة الحبس مدة لا تقل عن سنتين، وبالغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو إحدى هاتين العقوبتين، كُلّ من دخل عمدًا، أو دخل بخطأ غير عمدي وبقى بدون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول أو اختراق موقعًا أو بريدًا إلكترونيًا أو حسابًا خاصًا أو نظامًا معلوماتيًا يدار بعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكًا لها، أو يخصها. وقد عالج مقترح قانون مكافحة الجريمة الإلكترونية هذا الموضوع من خلال رفده لعقوبة الحبس مدة لا تقل سنتين ولا تزيد على خمس سنوات وبغرامة لا تقل ٣ مليون دينار عراقي ولا تزيد عن ٥ مليون دينار عراقي، كُلّ شخص دخل عمدا دون ان يكون مصرحا له بالدخول لموقع إلكتروني أو نظام معلوماتي أو أحد أجهزة الحاسوب أو ما في حكمها وقام بالاطلاع على محتواها أو نسخها أو قام بإلغاء البيانات أو المعلومات المملوكة للغير أو قام بحذفها أو تدميرها أو افشائها أو تغييرها. **وحري بنا التطرق للسرقة المعلوماتية** فسرقة البيانات والمعلومات الرقمية تمثل اليوم إشكالية كبيرة في تطبيق مثل هذا النوع من التطبيقات، فمن بادر القول لا بُدَّ من تعريف بالبيانات الرقمية حتى يتسنى لنا معرفة مفهوم هذه البيانات وكيف يتم التفتيش عنها، فحسب ما جاء في قانون مكافحة جرائم تِقنية المعلومات المصري بأنها "كُلّ ما يمكن إنشاؤه أو تخزينه أو معالجته أو تخليقه أو نقله أو مشاركته أو نسخه، بواسطة تِقنية المعلومات، كالأرقام والأكواد والشفرات والحروف والرموز والإشارات والصور والأصوات، وما في حكمها"، وفي مشروع قانون مكافحة الجريمة الإلكترونية في العراق عرفت بأنها "الأرقام والحروف والرموز والاشكال والأصوات والصور وكل ما يتم تخزينه ومعالجته وتوليده وإنتاجه ونقله بالحاسوب أو أيه وسائط إلكترونية أخرى"، فالبيانات الإلكترونية يثور بشأنها خلافًا وجدالًا فقهيًا حول مدى صلاحية المكونات المعنوية لأن تكون محلًا للتفتيش باعتبار ان البيانات الإلكترونية أو البرامج في حد ذاتها تفتقر إلى مظهرٍ مادي محسوس في المحيط الخارجي، بين هذا الرأي والنقيض منه نذهب برأينا إلى إن البيانات والمعلومات تخضع لقواعد الخاصة بالسرقة ولا بُدَّ من خضوعها للنصوص العقابية المُجرمة لهكذا أفعال.ما يمكن توضيح اختلاف الآراء من خلال ما يثار من تساؤلات، فهل المعلومات والبيانات من الممكن أن تكون محلًا للسرقة، أي هل أن المعلومات والبيانات صالحة لان تكون محلًا للسرقة؟ أختلف الفقه في ذلك بين مؤيد ومعارض، فمنهم من قال أنها ليس مالًا، وبهذا لا يمكن ان تكون محلًا يخضع للسرقة، إذ ذهب مؤيدو هذا الرأي أن المقومات المعنوية من النظام المعلوماتي يمكن أن تستغل ماليًا، فالقابلية للاستغلال المالي لا تعني انها واردة على شيء يُعدّ مالا في ذاته، ومن هنا لا يمكن وقوعها محلا لجريمة السرقة، كما نجد من قال في هذا الرأي ان المعلوماتية لا تصلح ان تكون مالًا أو محلًا للسرقة إلّا إذا اقترنت بالمادية، لذلك فان البرامج المعلوماتية التي يتعدى عليها بالسرقة لا يعتد بها لا في حالة وجودها مسجلة على دعامات، أو أسطوانات، فهي تصبح بذلك اموالًا تصلح محلًا للسرقة ([31]). اما الرأي النقيض من ذلك تبناه جانب من الفقه الفرنسي أمثال الفقيه (كاربونيه Carbonnier) على افتراض مقتضاه ان طبيعة الشيء، أو كيفية الاستفادة منه، واسلوب استخدامه تحدد الطريقة، أو الأسلوب الذي يتبعه الجاني للقيام بالنشاط المحقق للاختلاس، فاذا قام شخص بالدخول إلى جهاز الحاسوب واطلع على البرامج والمعلومات، فان هذا الفعل يعد سرقة استنادًا إلى ما يأتي:([32])

- إن البرامج والمعلومات لها كيان مادي يمكن رؤيته على الشاشة مترجمة إلى أفكار.

- يمكن حيازة هذه البرامج والمعلومات بواسطة نسخها على قرص أو شريط ممغنط عن طريق تشغيلها بوضعها في جهاز الحاسوب، -كما يمكن ذلك في حالة تخزينها في الحوسبة السحابية iCloud.
- امكانية حيازة المعلومات عن طريق الالتقاط الذهني عن طريق البصر، إذ ان موضوع الحيازة المعلومات غير مادي، فالتالي تكون واقعة الحيازة من الطبيعة نفسها، أي غير مادية (ذهنية) مثلها مثل الكهرباء، فالتيار الكهربائي قابل للانتقال رغم عدم حيازته المادية.
- كما يستند اصحاب هذا الرأي إلى آخذهم بالنظرية الموضوعية في التفسير متبعين بذلك المنهج المنطقي بالقول إلى انه لا يمكن تجريم سرقة الشريط الممغنط برغم قيمته البسيطة دون تجريم سرقة ما عليه من برامج ومعلومات ذات قيمة مالية كبيرة.
- كما انه يمكن الفصل التام بين الشيئين، اي الهيكل المسجل عليه والمحتوى المعلوماتي ولا يمكن ان نعد ان هنالك ثنائية في السرقة.

ونحن بجانبنا نميل وبكل تأكيد للرأي الثاني وما ارفده الفقه من أسباب وموجبات تستدعي منا الأخذ به، لما يحتويه من أفكار تواكب التطور التقني، فالهوية الرقمية ما هي سوى خوارزمية معتمدة من قبل الدولة، وارفدت لها مجموعة من عمليات التشفير للمحافظة عليها من الاختراق أو عملية اعتداء، وكل ذلك تم من خلال تقنية الذكاء الاصطناعي الذي بات اليوم المحرك الاساس في السرعة نحو التحول الرقمي. وقد عاقبت التشريعات المقارنة هذا النوع من الجرائم فمثلًا نجد المشرع في (المملكة العربية السعودية) قد عاقب على جرائم القرصنة والتهكير والاختراق للمعلومات الشخصية لإيقاف 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، بالسجن لمدة لا تتجاوز أربع سنوات وبغرامة لا تتجاوز 3.000.000 ريال سعودي [33]. وفي (التشريع الاماراتي) يُعاقب على عقوبة دخول موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلومات، أو وسيلة تقنية معلومات بدون تصريح وبصورة غير مشروعة، الحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم، أو بإحداهما، والحبس مدة لا تقل عن ستة أشهر، والغرامة لا تقل عن مائة وخمسين ألف درهم ولا تجاوز سبعمائة وخمسون ألف درهم، أو بإحداهما، إذا ترتب على ذلك حذف، أو تدمير، أو إفشاء، أو إتلاف، أو تغيير، أو نسخ، أو نشر، أو إعادة نشر أي بيانات أو معلومات، وإذا كانت البيانات أو المعلومات محل الأفعال الواردة في الفقرة 2 من هذه المادة (شخصية)، فعقوبتها الحبس مدة لا تقل عن سنة واحدة، والغرامة لا تقل عن مائتين وخمسين ألف درهم، ولا تجاوز مليون درهم أو بإحداهما. ولذا كان من الضروري ان تكون هنالك هيئات عامة متخصصة للحماية من هكذا اختراقات تصيب المعلومات سواء الحكومية أو الشخصية وخاصة ما يصيب الهوية الرقمية. كما تجدر الاشارة للتجربة الناجحة في (المملكة العربية السعودية)، إذ أنشأت الهيئة الوطنية للأمن السيبراني وارتباطها بالملك، وذلك وفق الأمر الملكي على تنظيمها بتاريخ ١٤٣٩/٢/١١ لتكون الهيئة الجهة المختصة في المملكة العربية السعودية بالأمن السيبراني، وقد حصدت المملكة العربية السعودية في عام ٢٠٢٠ المركز الثاني علميًا والأول عربيًا في المؤشر العالمي للأمن السيبراني، ودولة الامارات في المركز الخامس عالميًا، عمان الثالث عربيًا والمركز ٢١ عالميًا، كما حصدت جمهورية مصر العربية على المركز ٢٣ عالميًا والرابع عربيًا، وقد حصد العراق المركز (١٢٩) عالميًا، والأمن السيبراني (Cybersecurity) أو ما يُطلق عليه أيضًا أمن المعلومات الالكترونية (Information security) يُعد فرعًا من فروع التِقنية يهتم بحماية الأنظمة، والممتلكات، والشبكات، والبرامج، من الهجمات الإلكترونية التي تهدف في العادة للوصول إلى المعلومات الحساسة، أو تغييرها أو إتلافها أو ابتزاز المستخدمين للحصول على الأموال أو تعطيل العمليات التجارية والصناعية والخدمات وكل ما يرتبط بالعالم الافتراضي برابطة سواء تشغيلية أو عملية، وما يزال العراق

متأخرًا في استخدام التِقنية وتطوير الأمن المعلوماتي، ومع إقرار الاستراتيجية الوطنية للأمن السيبراني يمكنمن قبل مجلس الامن الوطني العراقي يمكن ان تكون بادرة حقيقية لتطوير قطاع الامن المعلوماتي في العراقي، وتحديث هذه الاستراتيجية يكون من اولويات التطوير الأمني المعلوماتي.

الخاتمة.

وفي الختام وبعد هذا العرض، تبين لنا ما للهوية الرقمية من أهمية كبيرة في مجال التحول الرقمي، وأهمية وجود هوية رقمية شاملة لكل الهويات الشخصية والمالية وجواز السفر الرقمي، حيث سنورد أبرز النتائج التي توصلينا اليها من خلال البحث، أيضًا السعي في ذكر مجموعة من التوصيات التي تكوِّن اجابة لتساؤل الدراسة الرئيس.

**أولًا/ الاستنتاجات:**

1 - اعتمدت الهوية الرقمية في العديد من الدول العربية منها دولة الامارات، والمملكة العربية السعودية.

2 - الهوية الرقمية هي نظام معلوماتي يعتمد على خوارزمية أنشأها الذكاء الاصطناعي بواسطة الانسان، وتحفظ بها البيانات الشخصية للأفراد من الاسم والعمر ومحل السكن وغيرها من تفاصيل الهوية الشخصية التقليدية، وتكون تحت حماية حكومية وأمنية عالية المستوى.

3 - إن الهويةالرقمية تُعد هويةوطنية رقميةلجميع المواطنين والمقيمين،إذ تسمح بوصول المستخدمين إلى خدمات الهيئات الحكومية المحلية والاتحادية، ومزودي الخدمات الآخرين، لذا تقدم الهوية الرقمية بطبيعة الحال حلولاً يسيرة في الولوج للخدمات عبر الهواتف الذكية دون الحاجة إلى كلمة سر أو اسم مستخدم، فضلاًعن إمكانية التوقيع على المستندات رقمياً، والتحقق من صحتها دون الحاجة لزيارة مراكز الخدمة.

4 - التشفير يُعد من أبرز وسائل والأدوات لحماية الهوية الرقمية، وذلك من خلال توفير أمن وسلامة وسرية المعلومات والمعاملات والصفقات في الشبكة العالمية -الإنترنت- وقد عرف التشفير في الفقه بانه آلية بمقتضاها تترجم معلومة مفهومة لمعلومة غير مفهومة، من خلال تطبيق بروتوكولات سرية قابلة للانعكاس، أي يمكن إرجاعها إلى حالتها الطبيعية

**ثانيًا/ الاقتراحات:**

1 - التوسع في التحول بموضوع الهوية الرقمية، لتشمل مستمسكات الشخص كافة، سواء البطاقة الشخصية وجواز السفر ليصبح جواز سفر رقمي، كما ويشمل هذا التحول البطاقات المصرفية وغيرها من البطاقات التقليدية أو الإلكترونية، من خلال إنشاء نظم ذكاء اصطناعي خاصة في انشاء الهوية الرقمية، واعتماد التشفير الذكي لحمايتها من أي خطر أو طارئ.

2 - الإسراع في تشريع قوانين دقيقة وواضحة، تشدد من عقوبة الاعتداء على البيانات والمعلومات الرقمية، من خلال بناء تشريعات قانونية تقنية، إذ يمكن ان يشمل النص العقابي على جميع أوجه الاعتداء أو الولوج للنظم الذكي الخاص بالهوية الرقمية، وتكون عقوبة هذا الفعل مقارنة بأعلى مراتب العقوبة الجنائية لما يحتويه هذا الاعتداء من المساس الكبير بالفرد والمنظومة الحكومية المؤمنة.

3 - إنشاء تطبيقات متخصصة تكون بمثابة حافظة رقمية مؤمنة لجميع هذه البطاقات، إذ يمكن ان تنظم هذه الحافظات الرقمية من خلال إضافة مادة جديدة لقانون البطاقة الوطنية رقم ٣ لسنة ٢٠١٦، لتعريف بالهوية الرقمية، وكذلك تعديل نص المادة ١٥ من القانون ليشمل الاعتداء على بيانات البطاقة الرقمية أو تجاوز حدود الدخول لنظامها عبر التطبيق الإلكتروني.

4 - نؤيد ما ذهب اليه المختصون في المجال القانوني التقني بإنشاء محاكم إلكترونية متخصصة للنظر بكل ما يتعلق بالجرائم المعلوماتية.

5 - التعاون في مجال تقنية الحوسبة السحابية من أجل حفظ الملفات حسابيًا، إذ يمكن هذا التعاون مع شركات التقنية المختصة بالحوسبة السحابية الى إنشاء مراكز داخل الدولة، وتلزم الشركات التقنية بعدم

تصدير البيانات خارج حدود الدولة، إذ لا تتمكن من تصدير البيانات الخاصة، وتجرى المعاملات عبر الحدود، وبهذا يمكن للدولة ان تحافظ على سيادتها الرقمية.

**الهوامش.**

(1) موقع البوابة الرسمية لحكومة دولة الامارات العربية المتحدة، يمكن الوصول عبر الرابط: ae/ar-ae.https://u، تاريخ الزيارة ٢٠٢٢/٧/٥.

(2) McKinsey Global Institute (2019), "Digital Identification: A key to inclusive growth".

(3) قانون رقم 5 لسنة 2022 بإصدار قانون تنظيم وتنمية استخدام التكنولوجيا المالية في الأنشطة المالية غير المصرفية، الجريدة الرسمية، العدد 5 مكرر (د) في 8 فبراير 2022.

(4) د. خالد ممدوح أبراهيم، الإثبات الالكتروني في المواد الجنائية والمدنية، دار الفكر الجامعي، مصر، الاسكندرية، ٢٠٢٠، ص ٢٧٦.

(5) Kazuhiko Shibuya, Digital Transformation of Identity in the Age of Artificial Intelligence, Springer Nature Singapore Pte Ltd. 2020, p. 32.

(6) A Blueprint for Digital Identity ،Part of the Future of Financial Services Series August 2016.

(7) د. مصطفى يوسف كافي، الإدارة الإلكترونية، دار رسلان، سوريا، ٢٠١٢، ص ٤٠٦.

(8) Swedish ePassport and eID programs, accessible at: https://www.thalesgroup.com/sites/default/files/gemalto/gov_sweden_e-pass.pdf, last accessed (10/7/2021).

(9) التكنولوجيا التحويلية، يمكن الوصول اليه عبر الرابط:
pdf.org/external/arabic/pubs/ft/fandd/2021/03/pdf/tourpe.imf.https://www، تاريخ الزيارة ٢٠٢١/٦/٢٣.

(10) توكلنا: هو التطبيق الرسمي المعتمد من وزارة الصحة www.ta.sdaia.gov.sa بالمملكة العربية السعودية للحد من انتشار فايروس كورونا، تم تطويره من قبل مركز المعلومات الوطني.

(11) الموقع الالكتروني وزارة الداخلية السعودية https://www.moi.gov.sa.

(12) د. أشرف جمال محمود عبد العاطي،الإدارة الإلكترونية للمرافق العامة، دار النهضة العربية، مصر، ٢٠١٦، ص ٨٢.

(13) Roland Traunmüller, DEXA Covering 15 Years of E-Government Research, Electronic Government and the Information Systems Perspective 4th International Conference, EGOVIS 2015 Valencia, Spain, September 1–3, 2015 Proceedings, p. 9.

(14) Smart credentials Enabling today's and tomorrow's digital identities, accessible at: https://www.infineon.com, last accessed (10/7/2021).

(15) د. علي محمد الخوري، الحكومة الرقمية "دائرة الاهتمام"، المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، مصر، ٢٠٢٠، ص ٤٦.

(16) أ. مصطفى يوسف كافي، الحكومة الالكترونية في ظل الثورة العلمية التكنولوجية المعاصرة، دار رسلان، سوريا، ٢٠٠٩، ص ٢٧.

(17) مريم خالص، الحكومة الإلكترونية، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، العدد ٤، ٢٠١٣، ص ٤٤٥.

(18) د. مفيدة طاير، مقومات وتحديات تشكيل الهوية الرقمية للمؤسسة في العصر الرقمي، المجلة العلمية للتكنولوجيا وعلوم الاعاقة، المجلد ٢، العدد ٤، المؤسسة العلمية للعلوم التربوية والتكنولوجية والتربية الخاصة، مصر، ٢٠٢٠، ص ٢١٤.

(19) كثير فاطنة، الهوية الرقمية وأثرها على العلاقات الاجتماعية، رسالة ماجستير، جامعة الدكتور مولاي الطاهر سعيدة، كلية العلوم الاجتماعية والإنسانية، الجزائر، ٢٠١٨، ص ٣٢.

(20) عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية، رسالة ماجستير، جامعة الشرق الاوسط، الأردن، ٢٠١٤، ص ٤٢.

(21) "For the purposes of this Directive, the expression "technological measures" means any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorised by the rightholder of any copyright or any right related to copyright as provided for by law or

the sui generis right provided for in Chapter III of Directive 96/9/EC. Technological measures shall be deemed "effective" where the use of a protected work or other subject-matter is controlled by the rightholders through application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective", Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001.

(22) المادة ١ فقرة ٩ من قرار رقم 109 لسنة 2005 بتاريخ 15/ 5/ 2005 بإصدار اللائحة التنفيذية لقانون التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.

(23) د. ايمن عبد الله فكري، الجرائم المعلوماتية، مكتبة القانون والاقتصاد، الرياض، ٢٠١٤، ص ١٧٥.

(24) د. ايمن عبد الله فكري، مرجع سابق، ص ١٧٨.

(25) د. اسامة فرج الله محمود الصباغ، مرجع سابق، ص ٨٦.

(26) د. ممدوح عبد الحميد عبد المطلب، خوارزميات الذكاء الاصطناعي وإنفاذ القانون، دار النهضة العربية، مصر، القاهرة، ٢٠٢٠، ص ٢٢.

(27) د. مسعودة طلحة، الهوية الرقمية "مأزق الاستخدام والخصوصية"، مؤتمر الدولي "الظاهرة الإعلامية والتالية في ظل البيئة الرقمية"، ٢٠١٨، ص ١٤.

(28) قرار رئيس مجلس الوزراء المصري رقم ١٦٩٩ لسنة ٢٠٢٠، بإصدار اللائحة التنفيذية للقانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، نشر في الجريدة الرسمية، العدد ٣٥ تابع (ج)، ٢٧ اغسطس، ٢٠٢٠.

(29) حسين عباس حميد، نحو اختصاص محكمة إلكترونية خاصة بالجرائم المعلوماتية -دراسة مقارنة-، دار النهضة العربية، مصر القاهرة، ٢٠٢١، ص ٩٤.

(30) د.أيمن رمضان محمداحمد،الحمايةالجنائيةللتوقيع الالكتروني،دار النهضة العربية، مصر، القاهرة، ٢٠١١، ص ١٣٩.

(31) سالم محمد سالم بني مصطفى، جريمة السرقة المعلوماتية، رسالة ماجستير،جامعة جدارا، كلية القانون، الأردن، ٢٠١١، ص ٥٤.

(32) انسام سميرطاهر،جريمة السرقة الالكترونية،مجلة جامعة بابل للعلوم الانسانية، المجلد٢٧،العدد٥،جامعة بابل، ٢٠١٩، ص ١٤٤.

(33) نظام مكافحة جرائم المعلوماتية، مرسوم ملكي رقم (م/١٧) بتاريخ (١٤٢٨/٣/٨)، وقرار مجلس الوزراء رقم (٧٩) بتاريخ (١٤٢٨/٣/٧) المادة (الخامسة): يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية: 1 - الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها. 2 - 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. 3 - إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت.

**ا لمصادر.**

**أولًا/ الكتب العربية:**


- اسامة فرج الله محمد الصباغ، الحماية الجنائية للمصنفات الالكترونية، دار الجامعة الجديدة، مصر، الاسكندرية، ٢٠١٦.
- أشرف جمال محمود عبد العاطي، الإدارة الإلكترونية للمرافق العامة، دار النهضة العربية، مصر، ٢٠١٦.
- أيمن رمضان محمد احمد، الحماية الجنائية للتوقيع الالكتروني، دار النهضة العربية، مصر، القاهرة، ٢٠١١.
- ايمن عبد الله فكري، الجرائم المعلوماتية، مكتبة القانون والاقتصاد، الرياض، ٢٠١٤.
- حسين عباس حميد، نحو اختصاص محكمة إلكترونية خاصة بالجرائم المعلوماتية -دراسة مقارنة-، دار النهضة العربية، مصر القاهرة، ٢٠٢١.
- خالد ممدوح أبراهيم، الإثبات الالكتروني في المواد الجنائية والمدنية، دار الفكر الجامعي، مصر، الاسكندرية، ٢٠٢٠.
- سعيدي سليمة، أمن المعلومات وأنظمتها في العصر الرقمي، دار الفكر الجامعي، مصر، الاسكندرية، ٢٠١٧.
- علي محمد الخوري،الحكومة الرقمية"دائرة الاهتمام"،المنظمة العربية للتنمية الإدارية،جامعةالدول العربية،مصر٢٠٢٠.
- مصطفى يوسف كافي، الإدارة الإلكترونية، دار رسلان، سوريا، ٢٠١٢.
- مصطفى يوسف كافي، الحكومة الالكترونية في ظل الثورة العلمية التكنولوجية المعاصرة، دار رسلان، سوريا، ٢٠٠٩.
- ممدوح عبدالحميد عبد المطلب،خوارزميات الذكاءالاصطناعي وإنفاذ القانون،دارالنهضة العربية،مصر، القاهرة، ٢٠٢٠.

**ثانيًا/ الابحاث ومقالات:**

- انسام سمير طاهر،جريمة السرقة الالكترونية،مجلة جامعةبابل للعلوم الانسانية،المجلد ٢٧، العدد ٥، جامعة بابل، ٢٠١٩.
- مريم خالص، الحكومة الإلكترونية، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، العدد ٤، ٢٠١٣.
- مفيدة طاير، مقومات وتحديات تشكيل الهوية الرقمية للمؤسسة في العصر الرقمي، المجلة العلمية للتكنولوجيا وعلوم الاعاقة، المجلد ٢، العدد ٤، المؤسسة العلمية للعلوم التربوية والتكنولوجية والتربية الخاصة، مصر، ٢٠٢٠.

**ثالثًا/ الرسائل والاطاريح:**

- سالم محمد سالم بني مصطفى، جريمة السرقة المعلوماتية، رسالة ماجستير، جامعة جدارا، كلية القانون، ٢٠١١.
- عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الالكترونية، رسالة ماجستير، جامعة الشرق الاوسط، الأردن، ٢٠١٤.
- علياء صالح محمد بن رشود، المسؤولية الجنائية عن العبث بالنظام المعلوماتي في النظام السعودي دراسة مقارنة بالقانون الاماراتي، رسالة ماجستير، كلية العدالة الجنائية، جامعة نايف للعلوم الامنية، الرياض، ٢٠١٩.
- كثير فاطنة، الهوية الرقمية وأثرها على العلاقات الاجتماعية، رسالة ماجستير، جامعة الدكتور مولاي الطاهر سعيدة، كلية العلوم الاجتماعية والإنسانية، الجزائر، ٢٠١٨.

**رابعًا/ مؤتمرات:**

- مسعودة طلحة،الهوية الرقمية"مأزق الاستخدام والخصوصية"،مؤتمر الدولي"الظاهرةالإعلاميةوالتاليةفي ظل البيئةالرقمية"٢٠١٨.

**خامسًا/ المراجع الاجنبية:**

- A Blueprint for Digital Identity ،Part of the Future of Financial Services Series • August 2016.
- Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001.
- McKinsey Global Institute (2019), "Digital Identification: A key to inclusive growth".
- Roland Traunmüller,DEXA Covering 15 Years of E-Government Research, Electronic Government and the Information Systems Perspective 4th International Conference, EGOVIS 2015 Valencia, Spain, September 1–3, 2015 Proceedings.
- Smart credentials Enabling today's and tomorrow's digital identities, accessible at: https://www.infineon.com, last accessed 10/7/2021.
- Swedish ePassport and eID programs, accessible at: https://www.thalesgroup.com/sites/default/files/gemalto/gov_sweden_e-pass.pdf, last accessed 10/7/2021.

**سادسًا/ مواقع إلكترونية:**

- يمكن الوصول عبر الرابط: https://u.ae/ar-ae
- التكنولوجيا التحويلية، يمكن الوصول اليه عبر الرابط: https://www.imf.org/external/arabic/pubs/ft/fandd/2021/03/pdf/tourpe.pdf، تاريخ الزيارة ٢٠٢١/٧/٥.
- الموقع الالكتروني وزارة الداخلية السعودية https://www.moi.gov.sa.

**- القوانين والقرارات:**

- قانون الامن السيبراني رقم (١٦) لسنة ٢٠١٩ السعودي.
- قانون رقم (١٧٥) المصري لسنة ٢٠١٨في شأن مكافحةجرائم تقنية المعلومات،نشر في الجريدة الرسمية،العدد٣٢ مكرر(ج)،١٤ اغسطس٢٠١٨
- قرار رئيس مجلس الوزراء المصري رقم (١٦٩٩) لسنة ٢٠٢٠، بإصدار اللائحة التنفيذية للقانون رقم (١٧٥) لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، نشر في الجريدة الرسمية، العدد ٣٥ تابع (ج)، ٢٧ اغسطس، ٢٠٢٠.
- قرار رقم (109) لسنة 2005 بتاريخ (15/ 5/ 2005) بإصدار اللائحة التنفيذية لقانون التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.
- نظام مكافحة جرائم المعلوماتية السعودي، مرسوم ملكي رقم (م/١٧) بتاريخ (١٤٢٨/٣/٨)، وقرار مجلس الوزراء رقم (٧٩) بتاريخ (١٤٢٨/٣/٧).