مجلة الكوفة للعلوم القانونية والسياسية

ISSN

٢٠٧٠٩٨٣٨ (مطبوع) ٣٠٠٦٧٦٧٧ (إلكتروني)

العدد الرابع / المجلد السابع عشر

تاريخ النشر

٢٠٢٥/١٢

الحماية الجنائية الموضوعية للإرث الرقمي

Objective criminal protection of digital heritage

ا.م.د هدى عباس محمد رضا

Hudaa.alshamaa@uokufa.edu.iq

الاء علي عبدالله

Alaaa.alfatlawy@student.uokufa.edu.iq

subject-matter protection،digital legacy،criminal protection

حماية جنائية ،ارث رقمي ،حماية موضوعية

Abstract:

Digital legacy is considered a product of digital life only. The development that occurred at the digital level led to an Increase in human connection to it, so most of the world has digital accounts and social networking sites. Therefore, the idea of digital legacy began to appear and was launched from the United States of America in the case of the American soldier, Corbal Elsworth. Accordingly, digital legacy Is considered one of the Important topics that have been raised In recent studies In order to provide criminal protection and what Is the fate of the legacy after the death of the user

الملخص:

الارث الرقمي يعتبر وليد الحياه الرقمية فقط ادى التطور الذي حصل على المستوى الرقمي الى زياده ارتباط الانسان فيه فاصبح معظم العالم يملكون حسابات رقميه ومواقع التواصل الاجتماعي لذا بدأت فكره الارث الرقمي بالظهور وانطلقت من الولايات المتحدة الأمريكية في قضيه الجندي الامريكي كوربال السورث وعليه يعتبر الارث الرقمي من المواضيع المهمة التي طرحت في الدراسات الأخيرة من اجل توفير الحماية الجنائية و ما هو مصير الارث بعد وفاة المستخدم

المقدمة:

إن القوانين والمواثيق الدولية والشرائع الإلهية المتعلقة بحقوق الإنسان لها عدد كبير من القواعد المرتبطة بها، وتعتبر هذه القواعد من أبسط تقاليد المجتمع، وهي التي توفر الأساس لتنظيم هذا الحق. فقد كان يعتمد في السابق على الملكية الشخصية المادية، كالعقارات والممتلكات القابلة للنقل والأموال وغيرها، أما اليوم، وبسبب تطور الحياة الاجتماعية والثورة الرقمية، لم يعد الأمر كذلك. بل أصبح الحصول على الملكية الرقمية يتم عن طريق الحسابات الشخصية والبريد الإلكتروني ومنصات التواصل الاجتماعي، والغرض منها التواصل مع الآخرين على الفيسبوك وتويتر وإنستغرام، وكذلك إجراء المعاملات التجارية على المواقع والقنوات، كل هذا يتم بالإضافة إلى وسائل الإعلام التقليدية والأنشطة البدنية، وهذا ما يسمى بالوراثة الرقمية.

أهمية الرسالة: مع تطور المجتمع، أصبح الإنترنت عاملاً مهماً في الحياة الاجتماعية، خاصة في العقدين الماضيين، ومع ظهور العديد من التطبيقات، مثل يوتيوب وتويتر وانستغرام وغيرها من التطبيقات، أصبح عاملاً مهماً في الحياة الاجتماعية عوامل الحياة، حيث أصبحت أحد أسباب كسب العيش من خلال النشر والإعلان والترويج والاشتراكات، مما أدى إلى ظهور فكرة التراث الرقمي. وتعتبر هذه الفكرة قد ظهرت مؤخراً حيث أن أول ظهور لها في الولايات المتحدة الأمريكية كان تطوراً حديثاً من قبل مركز تطوير التطبيقات وبدأ ينتشر في جميع أنحاء البلاد في حالة من الفوضى وهناك حاجة إلى إنشاء قوانين تنظم العمل الرقمي الميراث وجعل ذلك الميراث واضحا كيانا ينتقل إلى كيان عند وفاة صاحبه سواء كان حقيقيا

أو افتراضيا، ويوفر بالتالي الحماية اللازمة وفقا للقوانين والأسس التي بموجبها يتعرض التراث الرقمي للهجوم، مع جعله من الواضح أن المشروع رقميا هو الوضع المعتاد على الأرض.

مشكلة الدراسة: تكمن مشكلة هذه الدراسة في توفير الحماية الجنائية للتراث الرقمي من الهجمات التي تتعرض له بعد وفاة صاحبه.

منهجية الدراسة: وفيما يتعلق بموضوع الحماية الجنائية للتراث الرقمي، اعتمدنا أسلوب التحليل المقارن بين تشريعات الولايات المتحدة وفرنسا ومصر والعراق..

خطة الدراسة: سنقسم هذه الدراسة على مبحثين المبحث الأول الحماية الجنائية الموضوعية للإرث الرقمي مقسم على مطلبين المطلب الاول جريمة افشاء المعلومات الما المطلب الثاني جريمة إعادة نشر المعلومات اما المبحث الثاني سنخصصه حماية الحق في سلامة البيانات الشخصيه مطلبين المطلب الاول جريمة الدخول الغير مصرح به في ما يخص المطلب الثاني فسنخصصه لجريمة الاعتداء على الحق في طي النسيان

المبحث الأول:- الحماية الجنائية الموضوعية للإرث الرقمي: سنتناول في هذا المبحث الحماية الموضوعية للإرث الرقمي و سنقسمه على مطلبين المطلب الأول جريمة افشاء المعلومات اما المطلب الثاني سنخصصه لجريمة إعادة نشر المعلومات

المطلب الأول:- جريمة افشاء المعلومات: يحدث الإفصاح عندما يكشف الشخص المتحكم في البيانات الشخصية عن البيانات الشخصية لأسباب مهنية أو عن طريق الوصول بشكل غير قانوني إلى جهاز كمبيوتر أو نظام هاتف ونقلها إلى شخص أو كيان غير مؤهل لتلقي البيانات، وهو ما يعتبر خرقًا للمعلومات. ( ).

تعتبر جريمة تسريب المعلومات جريمة مقصودة، وتتكون من ركنين: جريمة مادية، وجريمة معنوية، وهما موضحان على النحو التالي.

الفرع الاول:- الركن المادي لجريمة افشاء المعلومات: إن عنصر جريمة تسريب المعلومات هو نقل البيانات الشخصية (والتي قد تكون صورًا أو رسائل أو مقاطع فيديو أو بيانات أخرى مرتبطة بالثقافة الرقمية) إلى شخص لا يحق له الاطلاع عليها، ونتيجة لذلك، فإن النشاط يعتبر جريمة. ويتم ذلك من خلال توفر صورتين. ( ).

اولا ـ السلوك الاجرامي و الذي يتحقق عن طريق فعل افشاء الاصول الرقمية المتعلقة بالإرث الرقمي التي حازها الجاني من اجل المعالجة او نقلها او تصنيفها و غيرها و قام بأفشائها الى شخص ليس لديه الصفة القانونية للاطلاع عليها فإن فعله هذا يشكل جريمة( ) لذلك، قام المشرعون الأمريكيون بتجريم التسرب، حيث تنص المادة ١٠٣٠ من قانون حماية الكمبيوتر على معاقبة أي شخص يصل عن علم إلى نظام كمبيوتر أو يستغل فرصة الوصول لتحقيق أغراض غير مصرح بها. ويعاقب على ذلك إذا تمكن عمدًا من استخدام أو تعديل أو تدمير أو الكشف عن المعلومات المخزنة فيه من خلال هذا السلوك (٤) وعلى نحو مماثل، أقر المشرع الفرنسي أيضا عقوبات على نشر الصور أو الرسائل أو مقاطع الفيديو (إذا كان نشر هذه العناصر يشكل اعتداء على الشرف أو حرمة الحياة الشخصية) بموجب المادة (٤٣) من قانون

معالجة المعلومات وحرية المعلومات. وفي حالة نشر صور أو رسائل أو مقاطع فيديو دون موافقة الشخص المعني، يعاقب المجرم بالحبس من شهرين إلى ستة أشهر وغرامة مالية تتراوح بين عشرين ألفاً وعشرين ألف دولار فرنسي، أو بإحدى هاتين العقوبتين[٥]. كما يعاقب المشرع الفرنسي كل من يتلقى صورا أو تسجيلات أو غير ذلك من أشكال الاتصال، ويعتبر كل من يتلقى أو يستقبل بيانات شخصية في إطار المعالجة الإلكترونية، كما هو منصوص عليه في المادة (٢٢٦-٢٢) من قانون العقوبات الفرنسي، أن لديه ارتباطا اسميا بالبيانات، وهذا الارتباط يضر بسمعة الفرد أو يتسبب في فقدانه لحياته الشخصية ونقلها إلى أفراد ليس لهم الحق في معرفتها[٦]. ويبدو أن المشرع الفرنسي قد كرس جريمة تسريب المعلومات من خلال الفعل الإجرامي المتمثل في تخزين البيانات الشخصية، بغض النظر عن الغرض من تخزينها، سواء كان معالجة أو نقل أو تخزين صور أو مقاطع فيديو أو أي شكل آخر من أشكال المحتوى، والمعلومات التي يحتفظ بها الشخص هي التي تجعل البيانات متاحة لشخص غير مؤهل كفرد كفء، وهذا يعني أنه لا يمكن الاطلاع على البيانات، وإذا كان التخزين يتعلق ببيانات مرتبطة بالإرث الرقمي، سواء كانت صورًا أو مقاطع فيديو أو أي شكل آخر من أشكال المحتوى، وحصل عليها الممثل ونقلها لغرض معالجتها أو نقلها أو تخزينها، فإذا تم ذلك علنًا، فإنه يعد جريمة.[٧] كما يعاقب المشرع المصري على ممارسة نشر المعلومات، بغض النظر عن دقة أو عدم دقة المعلومات التي ينشرها الفرد (كما هو منصوص عليه في المادة (٢٥) من قانون مكافحة جرائم تقنية المعلومات (بالسجن)). ولا يعد من الجرائم التي تضر بالأسرة المصرية أو المجتمع بأي شكل أو بأي وسيلة، بما في ذلك العنف أو انتهاك الخصوصية، تهديدًا مشروعًا لحياة أو شخص، أو من يقوم بإرسال عدد كبير من الرسائل الإلكترونية دون إذن الفرد، أو توفير بيانات الفرد للأنظمة والمواقع الإلكترونية بغرض الترويج للسلع أو الخدمات، أو نشر معلومات أو أخبار أو صور أو أي محتوى آخر يخالف أحكام القانون من خلال تقنية الحاسب الآلي أو شبكات المعلومات دون موافقة الفرد، يعاقب بالسجن مدة لا تقل عن ستة أشهر وغرامة لا تقل عن ٥٠ ألف دولار. ويحظر انتهاك خصوصية أي شخص، بغض النظر عن دقة المعلومات.[٨] ومن هنا يتبين لنا أن المشرع المصري قد عاقب كل من يتعدى على حرمة الحياة الشخصية بنشر معلومات على شبكة الإنترنت أو أي وسيلة إعلامية أخرى أو صور أو غيرها من الأشياء الشخصية تؤدي إلى انتهاك خصوصيته، سواء كان ذلك صحيحاً أم لا. فإذا أفشى الجاني أصولاً رقمية مرتبطة بالإرث الرقمي عبر شبكة الإنترنت أو غيرها من وسائل المعلومات، فإن فعله يعد جريمة لأنه انتهك خصوصية الإرث الرقمي، ويعتبر ذلك جزءاً من خصوصية الإرث الرقمي. أما بالنسبة للعراق، فإن "قانون العقوبات العراقي" يحتوي على المادة (٤٣٨) التي تنص على: "يعاقب بالحبس مدة لا تزيد على سنة وبغرامة لا تزيد على مائة دولار أو بإحدى هاتين العقوبتين".

١- كل من نشر بأي وجه عام أخباراً أو صوراً أو تعليقات تتعلق بأسرار الحياة الخاصة أو العائلية لشخص ما، ولو كان محتواها صحيحاً، وكان من شأن نشرها الإساءة إليه.

٢- كل شخص غير الأشخاص المنصوص عليهم في المادة ٣٢٨ يتصل برسالة أو برقية أو هاتف ويكشفها لشخص غير المرسل إليه إذا كان من شأن ذلك إلحاق ضرر بأي شخص).[٩]

يتبين ان قانون العقوبات العراقي عاقب على افشاء اخبار او صور متعلقة بالحياة الخاصة للمجني عليه من شأنها ان تضره او تضر عائلته حتى وان كانت صحيحة كذلك عاقب من اطلع على مكالمات الهاتف او الرسائل او برقية من غير الموظف او المكلف بخدمة عامة الذي ذكرته المادة (٣٢٨) وقام بإفشاء الرسائل او المكالمات اذ كان هذا الافشاء قد لحق ضرر. وقد عاقب مشروع قانون مكافحة الجرائم المعلوماتية العراقي كل من خالف القانون بنشر معلومات أو صور أو تسجيلات أو غير ذلك، حيث نصت المادة (٨-٢) على فرض عقوبة لا تقل عن المدة اللازمة لتنفيذ عقوبة انتهاك الخصوصية، ويفترض أن تستخدم هذه الأجهزة بما في ذلك الحاسبات الآلية أو المحمولة أو الهواتف أو غيرها من التقنيات المحمولة لأغراض شخصية فقط، ويعاقب بالسجن مدة لا تزيد على ١٠ سنوات وبغرامة لا تزيد على ١٠ ملايين دولار عراقي أو بغرامة لا تزيد على ١٥ مليون دولار عراقي، للأفراد الذين لهم حياة خاصة أو عائلية، بالتقاط صور أو نشر أخبار أو محتوى صوتي أو مرئي حتى لو كان حقيقياً. [١٠]. ويتبين مما سبق أن المشرع العراقي قد عاقب جريمة تسريب المعلومات عبر نشر الأخبار والتسجيلات والصور وغيرها، لأن ذلك من شأنه المساس بالحياة الخاصة أو العائلية للأفراد، بغض النظر عما إذا كانت الأخبار أو الصور أو التسجيلات صحيحة أم لا لذلك، إذا قام الجاني بنشر معلومات تتعلق بالتراث الرقمي للضحية، فإن القيام بذلك يعتبر جريمة لأن أفعاله تؤدي إلى انتهاك خصوصية الضحية، وهو ما يحظره المشرع العراقي انتهاك خصوصية الضحية إلا بعد الحصول على موافقة الشخص. قلق.

ثانيا - العواقب الجنائية، لأن إفشاء المعلومات من شأنه أن يؤثر سلباً على الضحية من خلال الاعتداء على سمعته أو سمعتها أو شرفها، فيجب أن يتم ذلك دون موافقة الضحية إذا تم إفشاء المعلومات بموافقته، وبموافقة الضحية وعلمه تزول أركان الجريمة المادية، كما تزول جريمة إفشاء المعلومات. (١١) بموجب المادة ١٠٣٠، سيعاقب المشرعون الأمريكيون إذا أدى الكشف عن المعلومات دون علم الضحية وموافقتها إلى الإضرار بالضحية. يعاقب كل من قام بالدخول إلى نظام الحاسب الآلي عن علم أو استغل فرصة الدخول لتحقيق غرض لم يتحقق بالإفصاح إذا كان قادراً على تحقيقه بهذا السلوك. (١٢) كذلك المشرع الفرنسي فأنه ايضا اورد ان يكون الافشاء دون رضا المجنى عليه وان يؤدي الى الاضرار بسمعته و شرفه حيث نصت المادة (٤٣) يشكل الافشاء تعرضا لحرمة الحياة الخاصة دون موافقة صاحب العلاقة كذلك نص المادة (٢٢٦- ٢٢) (.... اذا كان من شأن الافشاء الأضرار بأعتبار صاحب الشإن و حرمة حياته الخاصه و قام بنقلها الى من لا حق له في العلم) (١٣) أما المشرع المصري فقد نص أيضا على أنه لتحقيق نتائج جنائية يجب أن يكون الكشف دون موافقة المجني عليه، بغض النظر عما إذا كانت المعلومة صحيحة أم كاذبة، ولكن لم يذكر ما إذا كان الكشف يسبب ضررا أو ضررا. الأضرار التي لحقت بالضحية. ولم ينص عليه في المادة ٢٥ من قانون مكافحة جرائم تقنية المعلومات. وفي العراق، جرم المشرع العراقي أيضاً إفشاء المعلومات دون موافقة الضحية وإلحاق الضرر بها، على النحو المنصوص عليه في المواد (١٣) و(٤٣٨) و(٢/٨) من قانون العقوبات العراقي. مشروع مكافحة الجرائم الإلكترونية (١٤) ومما سبق يتضح أن التشريع المقارن يجرم إفشاء المعلومات إذا كان من شأنه الإضرار بالضحية سواء بسمعته أو سمعته أو شرفه،

وكان دون موافقة الضحية. الفرق بين التشريع المصري والعراقي هو أن الفعل يعتبر جريمة حتى لو كانت المعلومات التي أفصح عنها مرتكب الجريمة دون موافقة المجني عليه صحيحة، على عكس تشريعات الولايات المتحدة وفرنسا، إذا وقع الضرر، فإنه سيتم يعاقب. ولم يذكر ما إذا كان قد تم الكشف عن تلك المعلومات. لذلك، إذا كان محور جريمة تسرب المعلومات هو البيانات والمعلومات التي تؤثر على التراث الرقمي للضحية دون رضاه وعلمه، وكان سبب التسرب هو الضرر، فإن الفعل يعتبر جريمة لأن التراث الرقمي هو لا يجوز الكشف عن البيانات الشخصية التي تعتبر تخص الضحية دون إذن الضحية، وإلا فسيتم اعتبار الجاني معتديًا لأنه اقتحم الحياة الخاصة وسيعاقب بموجب قانون الولايات المتحدة. والتشريع الفرنسي والمصري والتشريع العراقي .

٣. العلاقة السببية: يجب أن تكون هناك علاقة مباشرة بين الفعل الإجرامي لجريمة تسريب المعلومات والجريمة الناتجة عنها، وهذا يكفي لإثبات أن الفعل الإجرامي لجريمة تسريب المعلومات تسبب في الجريمة. من المعلومات التي تم تسريبها. الآثار الضارة لجريمة إفشاء المعلومات المرتبطة بالتراث الرقمي لا يمكن الشروع في جريمة إفشاء المعلومات لأنها متعمدة (١٥).

الفرع الثاني:- الركن المعنوي لجريمة افشاء المعلومات: وتتجسد الأركان المعنوية لجريمة تسريب الأسرار في شكلين: الإهمال والقصد الجنائي، ويتحققان من خلال وجود عنصري المعرفة والإرادة.

أولا العلم :- أي أن الجاني يعترف للضحية بأنه يمتلك بيانات شخصية، مثل الصور والفيديوهات وغيرها، مما ينتهك سمعة الضحية واحترامها وخصوصيتها، أي أن الجاني على علم بالجريمة التي يرتكبها من خلال الكشف عن البيانات الشخصية والمعلومات المتعلقة بالإرث الرقمي دون موافقة الضحية.

ثانياً الارادة:- على الرغم من علم الجاني بأن ما يقوم به يشكل جريمة يعاقب عليها الا ان ارادته تتجه الى تحقيق جريمة افشاء المعلومات التي تتعلق بلارث الرقمي مع علمه ان ما قوم به يترتب مسؤولية جنائية و يعاقب عليها(١٦) لكن إذا كانت تصرفاته خطأ أو سهواً، فسيعاقبه المشرعون بموجب المادة (٢٢٦-٢٢) من قانون العقوبات الفرنسي، والتي ستحكم عليه بالسجن ثلاث سنوات وغرامة قدرها ١٠٠ ألف يورو. أما المشرعون الأمريكيون، فلم يعاقبوا المعلومات التي تم الكشف عنها عن طريق الخطأ أو السهو. كما أن المشرعين المصري والعراقي لم يعاقبوا الإفصاح بسبب الإهمال أو الخطأ. ولم يذكر ما إذا كان هذا صحيحًا أم خطأ. الإفصاح بالخطأ أو الإغفال (١٧) ومع ذلك، إذا كان الطرف يعلم أن معلوماته الشخصية المتعلقة بالميراث الرقمي قد تم تسريبها، وكان راضيًا تمامًا عن التسريب، فبما أنه تم الحصول على موافقة صاحب الحق، سينتفي القصد الجنائي وتسقط جريمة التسريب. لن يتم تشكيلها. ويشكل محتوى المعلومات أحد أسباب الإباحة، فيزول الصفة غير المشروعة للسلوك ويصبح السلوك مباحًا.(٨) .

المطلب الثاني:- جريمة إعادة نشر المعلومات: تعد جريمة إعادة إنتاج المعلومات من أكثر الجرائم ضرراً على الثقافة الرقمية، فهناك معلومات وصور ورسائل لا يستطيع المستخدمون مشاركتها، على الرغم من أنها تتعلق بسمعتهم وسمعتهم وأمور أخرى من المفترض أن تبقى سرية. ويستغل آخرون جهاز الكمبيوتر أو الهاتف المحمول أو الأجهزة الإلكترونية الأخرى للضحية، فإذا أعادوا نشر معلومات عن الضحية، فيجب

التحقيق معهم للمسؤولية الجنائية وفقاً للقانون. وبالتالي، تعتبر جريمة إعادة نشر المعلومات متعمدة، وهي مكونة من شقين: جسدي ومعنوي.

الفرع الاول:- الركن المادي لجريمة إعادة نشر المعلومات: تتجلى أركان جريمة إعادة نشر المعلومات في السلوك الإجرامي والنتائج والعلاقات السببية. السلوك الإجرامي: يتمثل السلوك الإجرامي المحدد المرتبط بجريمة إرسال المعلومات في وصول الأطراف إلى الحساب الإلكتروني أو نظام المعلومات، وإرسال معلومات لا يرغب الضحية في مناقشتها، وذلك وفقًا لما نصت عليه المادة ١٤ من "القانون الجنائي" لجمهورية الصين الشعبية. وقد حدد قانون جرائم تقنية المعلومات المصري (كل من تورط عمدًا في جريمة يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن ٥٠ ألف دولار أو ١٠٠ ألف دولار أو بكلتا العقوبتين). ومن العقوبتين، تهدف إحداهما عمدًا إلى الوصول إلى مواقع الويب أو الحسابات الشخصية أو أنظمة المعلومات. وإذا تم رفض الوصول إلى البيانات، مما يؤدي إلى إتلاف أو تغيير أو إعادة إنتاج أو إعادة نشر المعلومات أو البيانات الموجودة على الموقع الإلكتروني أو الحسابات الشخصية أو أنظمة المعلومات، فإن العقوبة لا تقل عن الحبس. غرامة لا تقل عن سنتين، بالإضافة إلى غرامة لا تقل عن مائة ألف دولار، ولا تزيد على مائتي ألف دولار، أو إحدى هاتين العقوبتين (١٩). ونؤكد بشكل واضح أنه إذا تمكن الجاني من الوصول إلى نظام المعلومات وإعادة نشر المعلومات والبيانات المرتبطة بالإرث الرقمي للضحية دون موافقة الضحية أو موافقته، فإن السلوك يعتبر إجراميًا، وهو فعل إجرامي. ونتيجة لذلك، لم يعاقب المشرعون الأمريكيون، ولا المشرعون الفرنسيون، ولا المشرعون العراقيون على جريمة إعادة نشر المعلومات، وهو خلل تشريعي ناتج عنهم . بالإضافة إلى ذلك، نتيجة الجريمة: أدرج المشرع المصري المادة (١٤) من قانون العقوبات في قانون القانون المصري، والتي تنص على أن نتيجة الجريمة هي الدخول إلى نظام المعلومات وإطلاقه دون موافقة الضحية أو علمه، وهذا يعتبر عمدًا. أو أكاذيب عرضية. قانون جرائم تقنية المعلومات (... كل فرد يعلم أو يزور عن غير قصد موقعًا محظورًا أو حسابًا شخصيًا أو نظام معلومات محظورًا). (٢٠) ونتيجة لذلك أوضحنا أنه إذا نتج عن هذا الدخول إتلاف أو تدمير أو تغيير أو إعادة إنتاج أو إعادة نشر الموقع أو الحساب، تكون العقوبة الحبس مدة لا تقل عن سنتين وغرامة لا تقل عن مائة ألف جنيه ولا تزيد على مائتي ألف جنيه أو إحدى هاتين العقوبتين) (٢١) ونتيجة لذلك أوضحنا أنه إذا نتج عن الدخول العرضي أو الخبيث إلى الحسابات الإلكترونية أو المعلومات والبيانات المتعلقة بالتاريخ الرقمي إعادة إنتاج المعلومات دون موافقة المجني عليه، فإن ذلك يعد جريمة ويحاسب مرتكبوها. السبب العادل: لإنجاز المهمة يجب أن تكون هناك علاقة مباشرة بين الفعل الإجرامي والنتائج الإجرامية التي تسبب جرائم المعلومات التي تؤثر على الثقافة الرقمية (٢٢)

الفرع الثاني:- الركن المعنوي لجريمة إعادة نشر المعلومات: ويتجلى الركن المعنوي في جريمة إعادة نشر المعلومات بقصد إجرامي وعلم وإرادة إجرامية.

أولاً: المعرفة: ويتجلى عنصر المعرفة في علم والدة مرتكب الجريمة بأن الوصول إلى الحساب أو عنوان البريد الإلكتروني محظور، وبالتالي سيتم إعادة نشر المعلومات دون رغبة صاحب البيانات، أو أن المعلومات

يتم ذلك. وسواء أكان ذلك عن قصد أو عن خطأ، فإن أفعاله تعتبر إجرامية، أي أن مرتكب الجريمة كان مخطئا وكان يعلم أن قيامه بإعادة نشر معلومات تتعلق بالتراث الرقمي يشكل جريمة (٢٣)

ثانياً، الإرادة: على الرغم من أن الفاعل يعلم أن أفعاله هي إعادة نشر المعلومات والبيانات المتعلقة بالتراث الرقمي عبر وسائل غير مصرح بها، سواء بقصد أو بغير قصد، ودون موافقة صاحب التراث الرقمي، إلا أنه غالباً ما يتم انتهاك إرادته من هذا النوع من السلوك يشكل الركن المعنوي للجريمة (٢٣).

ومما سبق يتبين لنا بوضوح أن جريمة إعادة طبع المعلومات هي من جرائم الاعتداء على التراث الرقمي من خلال إعادة طبع بيانات ومعلومات لا يرغب مرتكبها في الإفصاح عنها، إلا أن الولايات المتحدة وفرنسا لم يعاقبا عليها يعاقب. ويعتبر تقاعس المشرع العراقي عن معاقبة هذه الجريمة خللاً تشريعياً يجب معالجته من خلال التشريعات للحد من هذه الانتهاكات.

المبحث الثاني:- حماية الحق في سلامة البيانات الشخصية: تُعرف البيانات الشخصية بأنها أي معلومة يمكن استخدامها لتحديد هوية شخص ما من خلال هويته أو رقم التواصل معه أو بطاقة الائتمان أو عنوان الشبكة أو ممتلكاته الشخصية أو صورته سواء كانت ثابتة أو متحركة. على سبيل المثال، البيانات التي تؤدي إلى معرفة شخصية سواء بشكل مباشر أو غير مباشر) (٢٤). توجد عدة قوانين تعزز حماية البيانات الشخصية للأفراد، منها المادة (١) من قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠، حيث يتم ربط البيانات الشخصية (والتي تشمل أي بيانات مرتبطة بشخص طبيعي محدد أو قابل للتحديد) بهذه البيانات أو ببيانات أخرى (مثل الصوت أو الصورة أو الاسم أو الرقم أو أي بيانات تحدد هوية الفرد أو حالته الصحية أو الاقتصادية أو الاجتماعية) بهدف تحديد هويته بشكل مباشر أو غير مباشر (٢٥). وبالمثل، تُعرف اللائحة العامة لحماية البيانات في الاتحاد الأوروبي البيانات الشخصية بأنها أي معلومات تتعلق بشخص ما ترتبط به، سواء كان ذلك واضحًا بشكل مباشر أو غير مباشر، أو خاصًا بواحدة أو أكثر من سماته المميزة. العناصر، مثل السمات الفسيولوجية والوراثية والنفسية والمعلومات الاجتماعية والأسماء وبيانات الموقع أو معلومات الاتصال عبر الإنترنت (٢٦). ومن خلال ما سبق، يمكن ملاحظة أن البيانات الشخصية مرتبطة بكل فرد ويتم التعرف عليها من خلال الاسم أو الصورة أو الملف الشخصي الخاص به، مما يعني أنها تؤدي بشكل مباشر أو غير مباشر إلى التعرف على ذلك الفرد، مثل تطبيق Facebook الذي يتطلب من المستخدمين إدخال معلومات حول رخصة القيادة الخاصة بهم. ونتيجة لذلك، يصنف هذا القسم الجريمة الرقمية إلى نوعين: الأول هو الوصول غير المصرح به إلى الموارد الرقمية، والثاني هو انتهاك الحق في النسيان الرقمي.

المطلب الأول:- جرمية الدخول غير المصرح به: إن الدخول إلى أنظمة المعلومات الإلكترونية جريمة في جوهرها، ويشكل انتهاكاً لحرمة الخصوصية الإنسانية. ويرتكب هذه الجريمة كل من يرتبط بالكمبيوتر أو تكنولوجيا المعلومات، بغض النظر عن مجال عمله. ولا توجد آلية للدخول إلى الجريمة، سواء من خلال كلمة مرور أو من خلال عملية تشفير، وحتى لو كانت مثل هذه الآلية موجودة، فإن الدخول البسيط يعد جريمة بالفعل. لا ضرر ولا ضرار (٢٧). إن المحاولات الجارية لحماية البيانات من خطورة هذه الجريمة دفعت المفوضية

الأوروبية ولجنة من خبراء تكنولوجيا المعلومات إلى الإعلان في ٢٧ أبريل ٢٠٠٠ عن مشروع اتفاقية بشأن هذه الجريمة. ويطلب مشروع الاقتراح من الدول الأطراف تجريم الاعتداءات على البيانات الإلكترونية، بما في ذلك الدخول غير المصرح به الذي يحدث من خلال انتهاك تدابير أمن النظام، ويتم ذلك إما لاستخراج البيانات أو لأي غرض آخر (٢٨) إن الدخول في سياق المعلومات الإلكترونية هو فعل استخدام الهاتف المحمول أو الكمبيوتر للوصول إلى المعلومات المخزنة دون موافقة مالك المعلومات الإلكترونية. إن إساءة استخدام الحاسب الآلي من قبل أشخاص غير مصرح لهم بالدخول إليه أمر متغير، كما أن طريقة الدخول إلى أنظمة المعلومات متغيرة أيضًا، وقد تتطلب تفعيل الحاسب الآلي أو الهاتف أو أي جهاز آخر. وتتطلب بعض حالات إساءة الاستخدام هذه الحصول على رمز خاص للقيام بذلك. وبمجرد الاعتراف بها، تعتبر موجودة بغض النظر عن سبب الاعتراف. فقط من أجل المتعة، أو كوسيلة للسرقة، أو قد يكون الغرض التحايل على أمان الحاسب الآلي من خلال تعطيل ميزاته وأسباب أخرى للدخول غير المصرح به (٢٩). وتعتبر جريمة الدخول غير المشروع جريمة مؤقتة ومتعمدة تمتلك مكونات معنوية ومادية. وسيتم تناولها وفقًا للدول التي لديها مشكلة الدخول غير المشروع وتأثير هذه الجريمة على الموارد الرقمية.

الفرع الاول:- الركن المادي لجريمة الدخول غير المصرح به.

١ .السلوك الإجرامي: جريمة الاختراق غير المشروع هي فعل انتهاك خصوصية شخص ما من خلال الدخول إلى نظام معلوماته، وهذا يشمل جميع حالات الدخول غير المصرح به إلى نظام الكمبيوتر، وكذلك الدخول إلى النظام ببساطة. غير مسموح به (٣٠)

في القوانين المقارنة التي تجرم الدخول غير المصرح به، يحدد القسم ١٠٣٠أ من المشرعين الأمريكيين العقوبة بالسجن لمدة لا تتجاوز ١٠ سنوات، أو غرامة، أو كليهما.

أصدرت فرنسا قانونًا بشأن جريمة الاحتيال والاحتيال على المعلومات في ٥ يناير ١٩٨٨، يحتوي هذا القانون على مواد متعددة، بما في ذلك المادة ٤٦٢/أ التي تجرم الدخول غير المصرح به. يتم تخزين المعلومات غير المصرح بها في أجزاء كاملة أو جزئية من النظام يعاقب عليها بالسجن لمدة لا تزيد عن شهرين وغرامة لا تقل عن ٥٠٠٠ دولار أو كل من هاتين العقوبتين.....(٣١) ويبدو أن المشرعين الفرنسيين، في قانون أقره في ٥ يناير/كانون الثاني، ارتكبوا جريمة الوصول إلى أنظمة المعلومات دون ترخيص كعقوبة لمدة لا تقل عن شهرين وغرامة مالية لا تقل عن ٥٠ ألف دولار أو إحدى هاتين العقوبتين. ونتيجة لذلك، إذا قام المجرم بالوصول إلى التراث الرقمي دون ترخيص أو كان يفتقر إلى ترخيص صاحب الحقوق، فإن سلوكه يعتبر إجراميًا طالما أنه يفتقر إلى الترخيص، لأنه حتى لو لم يشكل جريمة، فإن سلوكه يعتبر غير قانوني. وتعتبر الجريمة مجرد الوصول إلى المورد، كجريمة. وفي عام ١٩٩٤ عدلت المادة ٣٢٣/أ من قانون العقوبات الفرنسي الجديد هذه القاعدة فغيرت العقوبة إلى الحبس سنة وغرامة ١٠٠ ألف دولار فرنسي. أما المشرع المصري فقد جرّم الدخول غير المصرح به في قانون مكافحة الجرائم المعلوماتية حيث تنص المادة ١٤ منه على: "كل من دخل بدون قصد الخروج إلى موقع أو حساب شخصي أو أنظمة معلومات: يمنع الدخول..." (٣٣) أما في القانون العراقي فإن وصف قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ بعدم

وجود نص تجريمي يصف الدخول غير المصرح به إلى أجهزة الكمبيوتر هو خلل تشريعي يجب على المشرعين تداركه. ويشجع مشروع قانون مكافحة الجرائم المعلوماتية الدخول غير المشروع حيث تنص الفقرة (٥) من المادة على الحبس مدة لا تقل عن سنتين ولا تزيد على خمس سنوات وبغرامة لا تقل عن (٣٠٠٠٠٠) ثلاثة ملايين دولار عراقي. كل فرد لا يزيد عدده عن (٥٠٠٠٠٠) خمسة ملايين عراقي يزور المواقع الالكترونية ونظم المعلومات والحواسيب وغيرها عن علم وبدون ترخيص...(٣٤)

ثانيا العواقب الجنائية: وهي العواقب المترتبة على السلوك الاجرامي والتي تشمل الاعتداء على المواقع الالكترونية والمعلومات الشخصية. وتسمى جريمة الدخول الى حساب المستخدم بدون ترخيص جريمة شكلية ولا يشترط العنصر المادي وجود نتيجة. وعلى الرغم من بعض حالات الفساد في المعلومات مثل حذف المعلومات او تغييرها للسماح بالوصول غير المصرح به الا ان هذا لا يغير من طبيعة الجريمة بل تعتبر جريمة شكلية وبالتالي يجب تجريم الدخول غير المشروع فقط ويعتبر هذا جريمة. إنه ينتهك الخصوصية ويشكل خطرًا على البيانات الشخصية للمستخدمين (٣٥) في النهاية، نستنتج أن الآثار الجنائية لجريمة الدخول غير المصرح به ناجمة عن فعل الدخول، الذي يؤدي إلى حذف أو تغيير أو إلغاء البيانات، كما عبر المشرع الفرنسي في المادة ٣٢٣ (...). إذا أدى الدخول غير المشروع إلى نظام المعلومات إلى إتلاف أو تغيير البيانات (٣٦) كما افترض المشرعون المصريون والعراقيون أن النتيجة الجنائية تتحقق عندما يؤدي الدخول إلى المحو أو التغيير أو الإلغاء. بالنسبة للمشرعين الأمريكيين، لم يشيروا إلى ما إذا كان الدخول قد أدى إلى حذف أو تغيير أو رفض الوثيقة. لأنه يكافئ الدخول البسيط إلى موقع ويب أو نظام معلومات أو أصل رقمي مرتبط بالثقافة الرقمية، يعتبر جريمة أن يدخل المستخدم دون إذن أو موافقة الضحية، حتى لو كان هناك ضرر. موافقته.٣. سبب الجريمة: وهو الشكل الثالث من أركان جريمة الاعتداء، حيث إن نشوء الجريمة والسلوك الناتج عنها لا يكفيان لتكوين السلوك الناتج عنها، بل لابد أن يكون هذا السلوك هو السبب، ووجود الجريمة يؤدي بطبيعته إلى النتيجة المرجوة دون أركان إضافية إذا توافرت هذه الأركان.

الفرع الثاني:- الركن المعنوي لجريمة الدخول غير المصرح به: ولإثبات جريمة الدخول إلى شبكات المعلومات دون تصريح، لا بد من توافر العناصر المعنوية للجريمة، حيث أن جريمة الدخول إلى المعلومات هي جريمة متعمدة، ولابد من توافر القصد الجنائي. في عنصري العلم والإرادة.

أولاً: التعليم: يتمثل عنصر العلم في جريمة الدخول غير المصرح به في أن يكون الجاني على علم بالفرق بين دخوله إلى حساب مستخدم غير مرخص له وبين الدخول غير المرخص له نفسه.: فالجاني على علم بأفعاله؛ فهو ببساطة يفتقر إلى علم المستخدم. ثم يأتي بعد ذلك فعل الملكية الخاصة، والذي يعتبر غير قانوني ويعاقب عليه بغض النظر عن سبب الضرر. ويفترض أن هذا الإجراء غير قانوني (٣٨)

ثانياً: الإرادة: أن يكون الجاني على علم بدخوله غير المرخص له إلى حساب شبكة المعلومات، ولكن رغبته تتجلى في إجراء هذا النشاط غير القانوني والإجرامي، مثل: أن يكون قصد المجرم هو الدخول غير المرخص له. قبل ذلك كان صاحب الإرث الرقمي على علم بأفعاله التي خالفت القانون ورغبة صاحب الإرث الرقمي (٣٩)

إن الغرض أو الدافع وراء جريمة الدخول غير المصرح به ليس مهما، فمثلا إذا قام الجاني بزيارة نظام معلوماتي من أجل إثبات للمسؤولين أن نظامهم ناقص فإن هذا لا يقلل من نية المجرم في هذه التطبيقات. سعى مهندس كمبيوتر إلى إثبات قدرته الفنية على اختراق النظام المصرفي من أجل الفوز بعقد لتثقيف موظفي البنك، فبغض النظر عن التدابير الأمنية التي يستخدمها البنك. وردا على اقتحام الهاكر، تمكن المهندس من الوصول إلى نظام البنك، الأمر الذي يشكل انتهاكا لنظام البنك (٤٠)

المطلب الثاني:- جريمة الاعتداء على الحق في النسيان الرقمي:- حق النسيان هو رفع الستار عن الأحداث التي يرغب صاحبها في إبقاء الآخرين غير مدركين لها، حيث يُعرَّف الحق الرقمي في النسيان بأنه حق الشخص في التحكم في معلوماته الشخصية عن طريق حذفها أو تغييرها أو الإضافة إليها.(٤١) كما يُعتبر أيضًا حق الشخص في عدم مشاركة المعلومات الرقمية عن نفسه عند الطلب وبعد فترة زمنية محددة (٤٢). يتم التعبير عن الجريمة ضد الحق الرقمي في النسيان بعدة طرق مختلفة سنناقشها أدناه.

الفرع الاول:- جريمة عدم اتخاذ الاحتياطات اللازمة لتأمين حماية البيانات الشخصية

أولاً: عدم اتخاذ الاحتياطات اللازمة لضمان أركان جريمة حماية البيانات الشخصية.

إن العنصر الأساسي للجريمة هو عدم اتخاذ الإجراءات الوقائية.

١ -السلوك الإجرامي: نظراً لأهمية الحفاظ على الأنظمة من أجل صيانة أنظمة المعلومات، فإن معالجي البيانات سيتخذون إجراءات سلبية بعدم إبلاغ المشتركين بالعيوب في النظام أو بعدم الحفاظ على إجراءات التشفير أو عدم إجراء التحديثات اللازمة. وتتحقق الحماية من خلال التحقق من التراخيص الرقمية أو استخدام كلمات المرور أو استخدام أساليب التشفير وغيرها من الأساليب الوقائية. إن عدم قدرة المعالج على القيام بهذا الدور يمكن أن يؤدي إلى أضرار جسيمة لنظام المعلومات، مما قد يؤثر سلباً على البيانات الموجودة في النظام.(٤٣) وقد جرم المشرع الفرنسي ممارسة عدم منعها، حيث تنص المادة (٢٢٦-١٧) على أن كل فرد يرتكب أو يطلب المعالجة الآلية لمعلومات اسمية دون اتخاذ جميع الاحتياطات اللازمة لضمان سلامة هذه المعلومات، وخاصة فيما يتعلق بمنع تسريبها أو إساءة استخدامها أو تدميرها أو الوصول إليها من قبل أفراد غير مصرح لهم (٤٤) كما تنص المادة (٢٢٦-١٧-١) على معاقبة مقدم الخدمة الإلكترونية أو المسؤول عن معالجة البيانات بالسجن لمدة خمس سنوات وغرامة مالية، كما تفرض غرامة مالية قدرها ٣٠٠,٠٠٠ دولار إذا فشل مقدم الخدمة في إبلاغ الهيئة الوطنية للإعلام والحريات بالوصول غير المصرح به إلى البيانات كما هو موضح في المادة ١٤٣٢-٩-١ من قانون الدفاع (٤٥). ٢- تتحقق النتيجة الجنائية لجريمة عدم اتخاذ الاحتياطات اللازمة عندما يقوم المعالج بعمل يفتقر إلى التدابير الوقائية، مما يؤدي إلى أضرار جسيمة لنظام المعلومات، وبالتالي يؤثر على البيانات الموجودة في النظام، كما كتب المشرع الفرنسي في المادة (٢٢٦-١٧). ومع ذلك، يجب اتخاذ جميع التدابير لضمان سلامة هذه المعلومات، بما في ذلك منع إساءة استخدامها أو فقدها أو الوصول إليها من قبل أشخاص غير مصرح لهم (٤٦). كما يتبين مما تقدم فإن المشرع الفرنسي قد سن الضمانات اللازمة للحفاظ على البيانات الشخصية من التهديد المحتمل بالانتهاك، حيث تنص المادة (٢٢٦-١٧) على أنه إذا فشل المشرع في تنفيذ هذه الضمانات

فإنه يعتبر جريمة. كما أن مزودي خدمات الإنترنت ملزمون بإبلاغ الهيئة الوطنية للمعلومات وحرية أصحاب البيانات عند الوصول إلى البيانات أو إصدارها، وللهيئة الوطنية صلاحية القيام بذلك. ولا يشترط المشرع الفرنسي وجود نتيجة جنائية للجريمة، ولكن يكفي أن تقع الجريمة إذا فشل الموظف في اتباع الشروط المنصوص عليها في القانون الفرنسي (٤٧).

٢. السبب والنتيجة: إذا لم تكن هناك علاقة مباشرة بين السلوك ومرتكبه فإنه لا يشكل جريمة إهمال، لأن السببية هي الرابط الذي يربط السلوك الإجرامي بالعواقب الجنائية، حتى لو تدخلت عوامل أخرى. إلا أن هذا لا يشكل عائقًا أمام كون الفعل نفسه قادرًا على إحداث نتائج جنائية، على سبيل المثال. هناك علاقة مباشرة بين نقص المعلومات بشأن العيوب في البيانات المرتبطة بالثقافة الرقمية وفعل المعالجة. النتائج التي تم التوصل إليها عند عدم اتخاذ التدابير اللازمة (٤٨) بالنسبة للمشرعين العراقيين فقد افتقروا إلى الآليات الكفيلة بحماية البيانات والمعرفة من انتهاك القانون الجنائي العراقي، بالإضافة إلى المشرعين الأميركيين والمصريين. المكون الثاني للركن المعنوي هو عدم اتخاذ الجريمة التدابير الاحترازية للحفاظ على البيانات الشخصية. إن جريمة عدم اتخاذ الاحتياطات اللازمة تعتبر جريمة مع سبق الإصرار والترصد وتنطوي على كافة عناصر المعرفة. وهذا سوف

ا -الفهم: يتجلى عنصر المعرفة في إدراك المعالج أن البيانات الشخصية المرتبطة بالتراث الرقمي تحتاج إلى الحماية والمحافظة عليها من أجل تجنب المخاطر المرتبطة بمعلومات النظام والمحتوى المخزن فيه. عدم وجود الفرنسية أوضح المشرع أن المعالجين يجب أن يبلغوا الهيئة الوطنية للمعلومات والحريات للأطراف المعنية، لكنه فشل في اتخاذ التدابير اللازمة لحماية البيانات الشخصية(٤٩). نتيجة لذلك، قرر المشرعون الفرنسيون معاقبة كل من يتم حبسه لمدة خمس سنوات أو أكثر بغرامة قدرها ٣٠٠ ألف يورو وحكم بالسجن.

٢- الإرادة: على الرغم من إدراك المعالج لعدم اتخاذ الاحتياطات اللازمة فيما يتعلق بالبيانات والملكية الفكرية للتراث الرقمي، فإنه غالبا ما يتسبب في أفعال غير قانونية تؤدي إلى سلوك إجرامي ذو مكونات جسدية أو عقلية..

الفرع الثاني:- جريمة الاحتفاظ بالبيانات الشخصية لمدة تتجاوز الحد المصرح به.

تعتبر جريمة الاحتفاظ بالبيانات الشخصية لمدة لا تزيد عن المدة المقررة جريمة عمدية ذات غرض إجرامي، ولها مكون جسدي ومعنوي.

أولاً: مكونات جريمة الاحتفاظ بالبيانات الشخصية لمدة زمنية أقصر من المدة المطلوبة قانونًا.

ا -الاحتفاظ الجنائي: ترتكب الجريمة بالاحتفاظ بالبيانات لمدة أطول من اللازم (مثل المدة المشمولة بالإشعار السابق). في هذه الحالة، تكون البيانات الشخصية المرتبطة بالأرشيف الرقمي قد تم الوصول إليها بالفعل. وبغض النظر عن طبيعة البيانات المخزنة، فإن الجاني قد أزالها قانونيًا، لكن الجاني تجاوز المدة الزمنية المقررة لتخزين البيانات، مما يترتب عليه جريمة تخزين البيانات الشخصية بعد انقضاء المدة المسموح بها (٥٠).

سن المشرع الفرنسي تشريعات تتطلب الاحتفاظ بالبيانات الشخصية لفترات زمنية أطول من الإطار الزمني المسموح به في قانون العقوبات الفرنسي. تنص المادة (٢٢٦-٢٠) من القانون على أنه "يعاقب كل من يخزن بيانات شخصية أطول من الإطار الزمني المسموح به". إخطار اللجنة الوطنية بالموافقة على الطلب أو الإخطار المسبق يعاقب عليه بالسجن لمدة خمس سنوات وغرامة ٣٠٠ ألف يورو عن المعلومات والحريات التي يتم تخزينها على النحو الذي يحدده القانون، وذلك عند تقديم الطلب أو اللائحة في الإطار الزمني المسموح به. الحصول على إذن بالمعالجة أو طلب إخطار اللجنة مسبقًا بالمعالجة (٥١) بالنسبة للمشرع المصري، تنص المادة ٢ (٤/٣) من الفصل الثاني من قانون حماية البيانات الشخصية على أنه (يجب جمع ومعالجة وتخزين البيانات الشخصية التي تفي بالمتطلبات التالية، ولا يجوز الاحتفاظ بها لفترة طويلة من الزمن) (٥٢). مما سبق، يتبين أن كل من المشرع المصري والمشرع الفرنسي جرما تخزين البيانات بعد مرور فترة زمنية محددة، وذلك بهدف الحفاظ على البيانات الشخصية. بالنسبة للمشرع العراقي، فشل قانون العقوبات في تضمين جريمة تخزين المعلومات الشخصية بعد الإطار الزمني المخصص. أما بالنسبة لقانون الجرائم المعلوماتية المقترح، فإنه يفشل في النظر في تجريم ممارسة الاحتفاظ بالبيانات المسموح بها لفترة أطول من اللازم. فالمشرعون الأمريكيون لا يضعون حدودًا لأفعالهم.

ثانيًا: العناصر الأخلاقية لجريمة الاحتفاظ بالبيانات المتأخرة: يتجلى العنصر الأخلاقي في رغبة المجرم في الاحتفاظ بالبيانات المخزنة بعد المدة المحددة بقصد وإرادة وعلم متهورة.

١ -الفهم: وهذا يتضمن معرفة المجرم بالبيانات والأصول الرقمية في التراث الرقمي، ففي النهاية يعد الاحتفاظ بهذه البيانات والأصول بعد انقضاء المدة المتفق عليها جريمة (٥٣).

٢ -الرغبة: بسبب الرغبة في الاحتفاظ بالبيانات الشخصية بعد انتهاء فترة الاحتفاظ، مع العلم بأن الاحتفاظ بالبيانات بعد انقضاء المدة جريمة، بدلاً من المفهوم المستحيل أن الجريمة خطأ ولا يمكن اعتبارها سبباً للأخلاق (٥٤)

ومن خلال ما تقدم يتبين أن من قام بحفظ البيانات لمدة زمنية يجب أن يكون قد أخطر بعدها صاحب البيانات بشأن التراث الرقمي ولم يفعل ذلك في الإطار الزمني المتفق عليه فإن سلوكه يعد إجراميا، ويعاقب. ونتيجة لذلك فقد جرّم المشرع الفرنسي أي تخزين للبيانات الشخصية بعد انقضاء المدة المحددة، ويعاقب على ذلك بالسجن خمس سنوات وغرامة قدرها (٣٠٠ ألف) يورو، ومنح القضاة سلطة محو هذه المعلومات، وهي جريمة، وللجنة سلطة القيام بذلك، حيث امتلك المشرع الفرنسي المختص بالمادة (٢٢٦-٢٤) سلطة الإشراف على هذا الإجراء لضمان محاسبة الأشخاص الاعتباريين عن التخزين غير القانوني للبيانات الشخصية (٥٥) أما المشرع المصري فقد اعتبر الاحتفاظ بالبيانات بعد المدة المسموح بها عملاً إجرامياً، إلا أنه لم يحدد بعد العقوبة على ارتكاب الجريمة.

وقد وصفها المشرعون العراقيون والأمريكيون الذين لم يكونوا طرفاً في الجريمة بأنها كتلة تشريعية يجب أن يسدها المشرع.

الشق الثالث:- جريمة عدم الاستجابة لحق المستخدم في الاعتراض على معالجة بياناته الشخصية. إن عنصر الجريمة الذي لا يستجيب لحق المستخدم في الاعتراض على معالجة بياناته الشخصية يسمى تعتيم البيانات. ويتحقق جوهر الجريمة عندما يفشل مزود الخدمة أو معالج البيانات في الاستجابة لاعتراضات المستخدم فيما يتعلق بمعالجة بياناته (٥٦) ونتيجة لذلك، أدرج المشرع الفرنسي المادة (٢٢٦-١٨) في القانون، والتي تنص على أن معالجة البيانات الشخصية عن شخص طبيعي يعاقب عليها بالسجن لمدة خمس سنوات وغرامة قدرها ٣٠٠ ألف يورو. ورغم معارضته لقضية المعالجة التجارية أو لأسباب أخرى (٥٧)، إلا أنه ما زال يؤيد مبادئ التعويض. وهناك دعوى قضائية تؤيد هذا الحق أمام محكمة الدرجة الأولى الباريسية، وخلاصة الدعوى أن امرأة طلبت حذف حسابها على جوجل بعد أن أُبلغت المحكمة بالضرر الذي لحق بها من جراء نشر قضية احتيال قديمة في (٢٠٠٦). واعتبرت المحكمة طلب المرأة مشروعاً بسبب تعريف المادة (٣٨٠) من قانون حماية الحريات المعلوماتية، التي توضح حق المستخدم في الاحتجاج. وأمرت المحكمة جوجل بدفع غرامة قدرها (١٠٠٠) ألف يورو عن كل يوم تأخير إضافي. وليس من الضروري أن تكون الاستجابة لطلبات حق الاعتراض مقبولة دائماً، فللمسئول عن المعالجة الحق في فحص الطلبات ثم البت فيها. ولا يجوز اعتبار الاعتراضات على الطلبات مشروعة إلا بعد إبلاغ المسئول عن معالجة البيانات بالضرر الذي لحق بموضوع البيانات أما المشرع المصري فقد وصف المعالجة الإلكترونية في المادة (٢) من قانون مكافحة جرائم تقنية المعلومات، إلا أنه لم يحدد جريمة عدم الرد على حق المستخدم في التساؤل عن الطريقة التي تتم بها معالجة بياناته الشخصية، حيث وصفت المادة السلوك الإلكتروني كأي عملية إلكترونية أخرى.

الخاتمة

النتائج

١ .جريمة تسريب المعلومات هي سلوك إجرامي يتم ارتكابه بحيازة معلومات شخصية، بغض النظر عن الغرض من تخزين أو نقل أو معالجة المعلومات.

٢. قيام مرتكب الجريمة بالكشف عن معلومات شخصية لطرف ثالث غير مخول له بمشاركة هذه المعلومات، وهذا يعني أن المجرم غير قادر على مشاركة المعلومات الشخصية حول القطع الأثرية الرقمية

٣. تعتبر جريمة إعادة إنتاج البيانات جريمة ضد التراث الرقمي من خلال إعادة طباعة المعلومات والبيانات التي لا يرغب الجاني في مشاركتها. البيانات الشخصية هي البيانات المرتبطة بالفرد والتي تستخدم لتحديد أو وصف أو اختبار خصائص الفرد، مثل تطبيق Facebook الذي يطلب معلومات المستخدم.

٤. بغض النظر عن الضرر المحتمل أو الجريمة المرتبطة بالوصول إلى نظام المعلومات والبيانات الشخصية، فإن الوصول إلى النسخة الإلكترونية من المعلومات يعد جريمة بالفعل.

٥. تسمى جريمة الوصول غير المصرح به بالسرقة، حيث تنطوي على انتهاك خصوصية شخص ما دون إذنه أو دون إذن.

٦. الحق في النسيان يمنح الشخص القدرة على التحكم بالمعلومات، على سبيل المثال، إسدال الستار على الأشياء التي لا يريد أن يعرفها الآخرون.

٧. إن جريمة عدم اتخاذ الاحتياطات اللازمة تسمى جريمة، ومعالجو البيانات مذنبون بهذه الجريمة ولا يبلغون المشتركين عن الإخفاقات التي تؤثر على النظام.

٨. يعتبر الاحتفاظ بالمعلومات الشخصية بعد تجاوز الفترة المسموح بها جريمة ويعاقب عليها.

التوصيات

١. - ضرورة تنظيم التشريعات بحيث تعالج قضايا التراث الرقمي.

٢ .على المشرعين العراقيين وضع قانون يتناول الهجمات السيبرانية ويحد من استخدامها. ٣ .على المشرعين العراقيين وضع قوانين جنائية جديدة تتوافق مع الاتجاهات الحالية والجرائم الجديدة.

٤. إنشاء محاكم متخصصة للتحقيق في الجرائم السيبرانية ولها سلطة في هذا المجال.

المصادر والمراجع:

١. د. علي جعفر، جرائم تكنولوجيا المعلومات المدنية الواقعة على الأشخاص والحكومة (دراسة مقارنة)، ط١، منشورات زين الحقوقية، سنة ٢٠١٣

٢. ضرغام جابر عطوش ال مواش ، جريمة التجسس المعلوماتي ، المركز العربي للنشر والتوزيع مكتبة دار السلام القانونية

٣. عبد الفتاح بيومي حجازي ، جرائم الكمبيوتر والانترنت في التشريعات العربية

٤. د . محمود ابراهيم غازي ، الحماية الجنائية للخصوصية و التجارة الإلكترونية ، ط١، مكتبة الوفاء القانونية ، الاسكندريه ، ٢٠٢٠ ص ٣٧٤

٥. د. خالد ممدوح، امن الجرائم الإلكترونية ، الدار الجامعية ، ٢٠٢٠ ،ص٨٤

الرسائل و الاطاريح

١. علي نعمة جواد الزرفي ، الجريمة المعلوماتية الماسة بالحياة الخاصة ، دراسة مقارنة ، رسالة ماجستير ، معهد العلمين للدراسات العليا ، قسم القانون ، سنة ٢٠١٦، ص ٧٩(٢

ضرغام جابر عطوش ال مواش ، جريمة التجسس المعلوماتي ، المركز العربي للنشر والتوزيع مكتبة دار السلام القانونية ، بلا سنة ، ص ٣١٥

١. د. عادل بن عبد العزيز ، البيانات الضخمة ، اطروحة دكتوراه ، جامعة الامام محمد بن سعود ، ٢٠٢٢ ص ٦٢

٢. د. هبه رمضان رجب ، الحماية القانونية للبيانات الشخصية في عصر التكنولوجيا الرقمية ، أطروحة دكتوراه القوانين

١. حماية البيانات الشخصية ، رقم ١٥١ ، سنة ٢٠٢٠

٢. قانون مكافحة جرائم تقنية المعلومات ، رقم ١٥٧ ، سنة ٢٠١٨

٣. مشروع مكافحة الجرائم الإلكترونية ، سنه ٢٠١٩، فقره ٢

٤.قانون العقوبات الفرنسي

المجلات

١. فادية حافظ جاسم ، هديل علي موحان ، المسؤولية الجزائية عن الاعتداء بطي حق النسيان الرقمي ، المجلة الأكاديمية العالمية للدراسات القانونية ، عدد١٢٧، ص٨٨

٢. د. معاذ سليمان الملا ، فكرة الحق في الدخول في طي النسيان الرقمي في التشريعات الجزائية الإلكترونية الحديثة ، مجلة كلية القانون ، عدد٣ ، ص١٤١

الهوامش

١. د. علي جعفر، جرائم تكنولوجيا المعلومات المدنية الواقعة على الأشخاص والحكومة (دراسة مقارنة)، ط١، منشورات زين الحقوقية، سنة ٢٠١٣، ص٤٤٧.

٢. علي نعمة جواد الزرفي ، الجريمة المعلوماتية الماسة بالحياة الخاصة ، دراسة مقارنة ، رسالة ماجستير ، معهد العلمين للدراسات العليا ، قسم القانون ، سنة ٢٠١٦، ص ٧٩(٢

ضرغام جابر عطوش ال مواش ، جريمة التجسس المعلوماتي ، المركز العربي للنشر والتوزيع مكتبة دار السلام القانونية ، بلا سنة ، ص ٣١٥

٣. زبيحة زيدان ، الجريمة المعلوماتية في التشريع الجزائري و الدولي ، دار الهدى ، الجزائر ، بلا سنة ، ص ٦٤

٤. د. عادل بن عبد العزيز ، البيانات الضخمة ، اطروحة دكتوراه ، جامعة الامام محمد بن سعود ، ٢٠٢٢ ص ٦٢

٥. د. هبه رمضان رجب ، الحماية القانونية للبيانات الشخصية في عصر التكنولوجيا الرقمية ، أطروحة دكتوراه ، بلا سنة ، ص٤٤

٦. عبد الفتاح بيومي حجازي ، جرائم الكمبيوتر والانترنت في التشريعات العربية

٧. د . محمود ابراهيم غازي ، الحماية الجنائية للخصوصية و التجارة الإلكترونية ، ط١، مكتبة الوفاء القانونية ، الاسكندريه ، ٢٠٢٠ ص ٣٧٤

٨. د. خالد ممدوح، امن الجرائم الإلكترونية ، الدار الجامعية ، ٢٠٢٠ ،ص٨٤

٩. قانون مكافحة جرائم تقنية المعلومات ، رقم ١٥٧ ، سنة ٢٠١٨

١٠.مشروع مكافحة الجرائم الإلكترونية ، سنه ٢٠١٩، فقره ٢

١١.فادية حافظ جاسم ، هديل علي موحان ، المسؤولية الجزائية عن الاعتداء بطي حق النسيان الرقمي ، المجلة الأكاديمية العالمية للدراسات القانونية ، عدد١٢٧، ص٨٨

١٢.د. معاذ سليمان الملا ، فكرة الحق في الدخول في طي النسيان الرقمي في التشريعات الجزائية الإلكترونية الحديثة ، مجلة كلية القانون ، عدد٣ ، ص١٤١

١٣.قانون العقوبات الفرنسي

١٤.د. ايمن عبدالله فكري ، الجرائم المعلوماتية ، دراسة مقارنة في التشريعات العربية و الأجنبية ، مكتبة القانون و الاقتصاد ، ط ١، الرياض ، سنة ٢٠١٤ ، ص ٨٢٠

١٥.قانون حماية البيانات الشخصية ، رقم ١٥١ ، سنة ٢٠٢٠