الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة يحي فارس بالمدية
كلية الحقوق والعلوم السياسية

مذكرة نهاية الدراسة للحصول على شهادة الماستر
تخصص: علوم جنائية وقانون جنائي

بعنوان:

جريمة النصب الإلكتروني في التشريع الجزائري

من تقديم الطالبتان:
- بوشيبة حميدة
- بوشيحة جميلة

تحت إشراف الأستاذ:
-أ.د.عمر زرقط

لجنة المناقشة:

الإسم واللقب	المؤسسة الأصلية	الصفة
أ.د.جبار رقية	جامعة يحي فارس بالمدية	رئيسا
أ.د.عمر زرقط	جامعة يحي فارس بالمدية	مشرفا
د. دالي سعيد	جامعة يحي فارس بالمدية	ممتحنا

السنة الدراسية: 2023-2024


بسم الله الرحمن الرحيم

شكر وعرفان

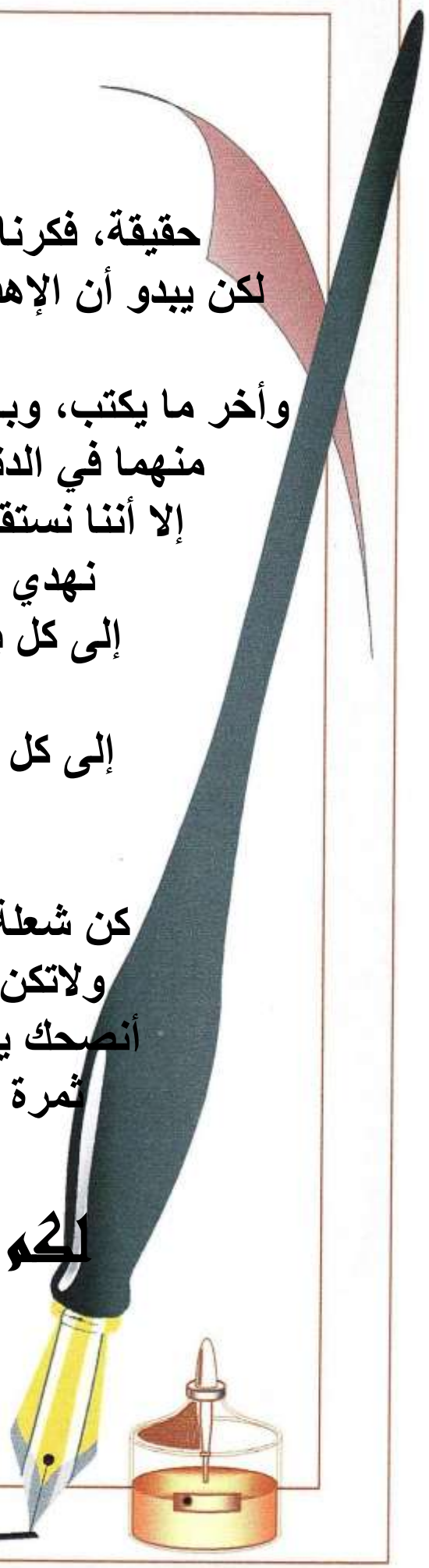
اشكر الخالق عز وجل الذي وفقنا في إتمام هذه المذكرة
هو الله ربي الذي ما أصبح وما أمسى بي من نعمة ما حييت فمنه وحده
فله الحمد وله الشكر
ومصداقا لقول الحبيب المصطفى صلى الله عليه وسلم ــمن صنع إليه معروف فقال لفاعله جزاك الله خيرا فقد ابلغ في الثناء أجازه الترميذي.
نتوجه بالشكر الجزيل الأستاذ المشرف " د. عمر زرقط " أستاذ بجامعة يحيى فارس المدية على قبوله الإشراف على هذه المذكرة
بكل إحترافية مهنية وبدون أية قيود
بل جعل لنا كل صعب سهلا وهينا
كما نتوجه بالشكر الجزيل إلى أساتذة لجنة المناقشة على تفضلهم وقبولهم تقييم مذكرتنا
وإلى كل من تعاون، وقف معنا ودعمنا من بعيد أو قريب على إنجاز هذه المذكرة بجهده ووقته ودعائه...

الإهداء

حقيقة، فكرنا كثيرا في إهداء هذا العمل المتواضع
لكن يبدو أن الإهداء شأنه شأن مقدمة البحوث هي أول ما يقرء
وأخر ما يكتب، وبالرغم من أن الوالدين لايوجد من هو أغلى منهما في الدنيا ومن بعدهم الزوج والأبناء والأهل
إلا أننا نستقطع من إهدائهم ونستسمحهم في أن
نهدي هذا العمل أيضا إلى طلبة العلم
إلى كل باحث في مجال القانون أو غيره من الإختصاصات
إلى كل قارئ مرّ على الموضوع صدفة أو بهدف البحث،
لكل محب للعلم نقول:
كن شعلة في مشكاة تضيء الدنيا بنورها
ولاتكن سيفا حادا لكن في غمده يصدأ
أنصحك يا من كنت طالبا أن تجعل مذكرتك ثمرة جهدك ولا تجعلها سلعة جيبك
وشكرا

لكم كل التقدير والاحترام

حميدة وجميلة



مقدمة:

شهد العالم ثورة تكنولوجية كبيرة شملت كل مجالات الحياة لاسيما عالم الكمبيوتر والأنترنت فأخذ رواجا كبيرا فلم تعد تخلو منها لاشركات ولا مؤسسات عامة أو خاصة بل حتى الأفراد العاديون لا يستطيعون الإستغناء عن هذا العلم وأصبح الجاهل اليوم ليس الذي لايعرف القراءة والكتابة بل الجاهل الذي لايعرف لغة الكمبيوتر، فبات العالم قرية صغيرة من حيث الأحداث والوقائع التي يمكن متابعتها في أي زمان ومكان.

إلا ان الأنترنت في حقيقتها هي سلاح ذو حدين، وبمعنى آخر فكما كان عالم الكمبيوتر وسيلة للتقدم العلمي بمجالاته الواسعة، كان أيضا ملاذا لاحتراف المجرمين للجريمة، بكل أنواعها، ومنها من تمس الحياة الخاصة للناس كالتهديد والإبتزاز وفضح الأسرار، ومنها ما تمس المال كالسرقة والنصب والتزوير خاصة مع ظهور التجارة الإلكترونية والتعاملات البنكية والمالية عن طريق بطاقات الإئتمان.

كان هذا المجال الجديد فرصة لظهور المجرم الالكتروني الذي يبحث عن الثراء والمال بالطرق السهلة وهكذا ظهرت مفاهيم جديدة للجريمة وظهر ما يسمى بالجرائم الإلكترونية التي تتضمن كل فعل مجرم يرتكب باستعمال تكنولوجيات الاعلام والاتصال.

هناك عدة أنواع من الجرائم الإلكترونية والتي إخترنا منها جريمة النصب الإلكتروني لتكون موضوع دراسة، هذه الأخيرة أي الجريمة إتخذت عدة أساليب وعدة طرق يستطيع من خلالها المجرمون أن يحتالو على ضحاياهم دون أن يتركوا أثر للجريمة في أغلب الأحيان، مما جعل التشريعات تتجه نحو تعديل منضوماتها القانونية لتتلائم مع هذا الالسلوب الجديد من الاجرام وتستطيع حماية ضحايا النصب مهما كانوا، سواءا أشخاص طبيعيون أو معنويون.

يحضى هذا الموضوع بالكثير من الاهمية، شأنه شأن المواضيع المستحدثة التي طفت على الساحة العالمية في جميع المجالات، سواء في القانون أو الإقتصاد أو السياسية إلى غيرها، ونحن كقانونيون نهتم كثيرا بالمستجدات التي تتعلق بالتشريعات، والإشكالات في تطبيق النصوص القانونية، ومن بين هذه المستجدات جريمة النصب الإلكتروني التي يعتبر البحث فيها موضوعا ذو أهمية سواء من الناحية العلمية أو الناحية العملية.

أما من الناحية العملية فنجد أن هذا النوع من الدراسات القانونية التي توضح خطورة النصب الإلكتروني لاسيما مع الإنتشار الواسع للأنترنت وهوس الناس على إقتناء الحواسب والهواتف الذكية التي تسهل وصول النصاب الإلكتروني إليهم بسهولة والإحتيال عليهم بشتى الطرق والحيل.

أما من الناحية العلمية، فتكمن الأهمية في تسليط الضوء على النواحي القانونية لجريمة النصب الإلكتروني خاصة معرفة الجوانب الإجرائية والموضوعية والعقوبات المقررة لها في التشريع الجزائري.

تتنوع أسباب إختيار الموضوع بين أسباب ذاتية تتمثل في الرغبة في التعرف على جريمة من الجرائم الإلكترونية ألا وهي جريمة النصب الإلكتروني، معرفة قانونية وعلمية بما أننا طلبة قانون من جهة، ومن

جهة أخرى، لما يتطلبه العصر الذي شهد تطورا تكنولوجيا كبيرا سريعا، يدعوا إلى زيادة المعرفة لتفادي أخطاره، وأسباب موضوعية تتمثل في كون الموضوع يدور حول جريمة من الجرائم المستحدثة التي تحتاج إلى دراسات مكثفة لإتسقصاء محاورها والتطرق إلى المعالم الظاهرة وخفية فيها.

كما أن هذه الدراسة القانونية تهدف إلى التعرف على جريمة النصب الإلكتروني من الناحية الموضوعية والناحية الإجرائية، من خلال التطرق إلى : أساليب إرتكابها وأركانها، وإجراءات التحقيق ضدها والعقوبات المقررة لها في التشريع الجزائري.

ومن هنا ظهرت الحاجة إلى المزيد من الإهتمام بهذه الجريمة من قبل التشريعات سواءا الوطنية أو الدولية، ومن هنا نصل إلى إشكال التالي: كيف عالج المشرع الجزائري جريمة النصب الإلكتروني في ظل غياب نص قانوني خاص بها كجريمة قائمة بحد ذاتها؟

مستعملين في ذلك المنهج الوصفي من أجل وصف الجريمة والتطرق إلى خصائصها ومميزاتها، والمنهج التحليلي من أجل تحليل أساسيات الموضوع وعناصره، وتحليل أيضا النصوص القانونية ذات الصلة.

ومن الصعوبات التي واجهناها في هذه الدراسة هي كون جريمة النصب الإلكتروني هي جريمة إلكترونية وهي جريمة مستحدثة فرضها عصر التكنولوجيا والأنترنت، فالتصدي لها بالتشريعات القانونية مستحدث أيضا، والدراسات القانونية التي أجريت حولها لم تشمل بعد كل الجوانب لهذه الجرائم بالدقة والوضوح والشمول اللازم بالإضافة إلى أن موضوع النصب الإلكتروني هو موضوع متشعب واسع خاصتا أن هذه الجريمة لم تحضى بنص قانوني خاص بها وإنما سنسقط عليها مواد النصب المقررة في قانون العقوبات، ونظرا لضيق الوقت الممنوح لنا فإنه لايكفي للإلمام بكل جوانبه، لذلك إجتهدنا على قدر المستطاع لإعطاء دراسة شاملة لأهم مايجب معرفته حول جريمة النصب الإلكتروني.

وسيتم من خلال الدراسة الإجابة عن الإشكال المطروح من خلال تقسيم البحث إلى فصلين، حيث نخصص الفصل الأول لدراسة مفهوم جريمة النصب الإكتروني، وفي الفصل الثاني نتطرق إلى الجوانب الإجرائية والموضوعية لجريمة النصب الإلكتروني.

الفصل الأول: مفهوم جريمة النصب الإلكتروني

مقدمة الفصل:

إن التطور السريع الذي شهده العالم في جميع المجالات لاسيما مجال الكمبيوتر والمعلوماتية، جعل من جريمة النصب تتطور وتتحور فسرعان ما أصبحت جريمة تكنولوجية، ودخلت عالم الحواسيب وفضاءات الانترنت لتظهر في نمط جديد وتصبح جريمة من الجرائم المعلوماتية وهكذا ظهر النصب الالكتروني.

الذي سوف نتطرق إلى مفهومه في هذا الفصل عن طريق تقسيمه إلى مبحثين، يضم المبحث الأول ماهية جريمة النصب الإلكتروني وكمطلب أول تطرقنا إلى تعريف النصب الإلكتروني بثلاثة فروع، الفرع الأول يتكلم عن التعريف اللغوي والفقهي والقانوني، والفرع الثاني يتناول خصائص هذه الجريمة، وفي الفرع الثالث التميزبينها وبين ما يشابهها من جرائم، ثم ننتقل إلى المطلب الثاني الذي بينا فيه، أساليب جريمة النصب الإلكتروني في ثلاثة فروع، وكمبحث ثاني درسنا أركان جريمة النصب الإلكتروني في مطلبين، الركن المادي والركن المعنوي.

المبحث الأول: ماهية جريمة النصب الإلكتروني

لكي نتمكن من فهم جريمة النصب الالكتروني فهما قانونيا لابد أن نتعرف على مفهومه بكل ما يضمه من تعريف وخصائص وتميز جريمة النصب الإلكتروني عما يشابهها ويكون ذلك كالتالي:

المطلب الأول: تعريف جريمة النصب الإلكتروني

تعددت تعاريف النصب الالكتروني بين التعريف اللغوي والتعريف القانوني والفقهي، ومن خلال هذا التعريف يتضح لنا تعريف النصب الإلكتروني بصورة واضحة وشاملة.

الفرع الأول: التعريف اللغوي والفقهي والقانوني لجريمة النصب الإلكتروني

إن معرفة معاني الكلمات لغويا يسهل لنا فهم المقصود والدلالة إلا أن المعنى لا يكتمل إلا بالتعريف الفقهي والقانوني وهذا ما سوف نعرفه في هذا الفرع.

أولا: التعريف اللغوي لجريمة النصب الإلكتروني

أصل النصب في اللغة من "نَصَبَ" والنَصْبُ، النصب بضمتين: الداء والبلاء، وناصب الشرّ أظهره له، وقيل النصبُ: مصدر نصب الشيء أي أقمته، ونَصَبَهُ لفلان نصبًا إذ عاديته، ناصبته الحرب مناصبة[1].

وهناك معنى آخر لكلمة النَصب على أنها حجارة حول الكعبة كَانَ أَهْلُ الجاهلية يَذْبَحُونَ عليها لغير الله ويظهر ذلك في قوله تعالي: {إلاَّ مَاذكَيْتُمْ وَمَا ذُبِحَ عَلَى اَلْنُصْبَ}[2].

ثانيا: التعريف الفقهي والقانوني لجريمة النصب الإلكتروني

سوف نجمع بين التعريف القانوني للنصب والتعريف الفقهي للإلكتروني لنستطيع أن نتوصل إلى تعريف شامل لجريمة النصب الإلكتروني في ظل غياب نص قانوني خاص به.

يعرف النصب على أنه : هو الإستلاء على مال الغير عن طريق إستعمال وسائل إحتيالية حددها القانون على سبيل الحصر بنية تملك هذا المال والتي يقع المجني عليه نتيجتها في الغلط الدافع للتسليم، وهذا ما تطرقت إليه المادة 372 من قانون العقوبات الجزائري[3].

أما الإلكتروني فنقصد بها أن الجريمة تقع بإستعمال وسائل إلكترونية والتي هي عبارة عن أجهزة ومعدات حديثة تمتاز بالدقة والسهولة في التركيب والصيانة، تستخدم في أداء وظائف معينة يستعمل فيها الإنسان كل مهاراته في التقنيات والتكنولوجيات الحديثة.

1-اسامة حمدان الرقب، **جرائم النصب والاحتيال الاساليب –المظاهر-العلاج**، الطبعة الاولى، دار يافا العلمية للنشر والتوزيع، الاردن، 2012، ص20.

2-سورة الماءدة اية 3.

3-اسامة حمدان الرقب، مرجع سابق، ص21.

ومن هنا نجد أن النصب الإلكتروني يختلف نوعا ما عن النصب التقليدي، حيث يعتبر النصب الإلكتروني من أخطر الجرائم الإلكترونية الواقعة على الأموال خاصة مع تطور الانترنت والحواسب فأصبح المجرم الإلكتروني يبحث عن كل الطرق للحصول على المال الإلكتروني في محاولة منه للوصول إليه مستعملا طرقا غير شرعية، ونقصد بالمال هنا هو كل مال إلكتروني قابل للنقل والتملك.

كما عرفه الفقه " بأنه المال الموجود في الحاسوب سواء بصورة معلومات وبيانات إلكترونية في أي صورة كان عليها سواء كان مخزن على أقراص صلبة أو دعامات تخزين خارجية، فهو بذلك كل المدخلات الإلكترونية التي لها من القيمة المادية مما يجعلها قابلة للتملك وتكتسي الحماية القانونية[1]".

ونظرا لطبيعة الجريمة الإلكترونية التي هي دائما في تطور سريع ومواكب للتكنلوجيا، فلا يستطيع القانون إعطاء تعريف دقيق محدد على سبيل الحصر لجريمة النصب الإلكتروني وترك ذلك للفقه ومن بين هذه التعريفات تعريف الأستاذ الامريكي " سكويرز" جريمة النصب الإلكتروني على أنها " إساءة إستخدام نظام الحاسوب بحيث ينطوي على سلوك وعلى حيلة أو خدعة مظللة[2]".

كما عرفته المادة الرابعة من القانون العربي النموذجي الموحد أنه: "الإستلاء على البرامج والبيانات المخزنة على الحاسب الالي أو الوسائط الإلكترونية بطريق الإحتيال[3].

الفرع الثاني: خصائص جريمة النصب الإلكتروني

تعد جريمة النصب الإلكتروني من الجرائم المعلوماتية والتي تشترك في خصائصها، وعليه فأهم الخصائص المميزة لهذه الجريمة عن الجرائم التقليدية هي:

أولا: الجريمة الالكترونية متعدية الحدود أو جريمة عابرة للحدود.

المجتمع المعلوماتي لايعترف بالحدود الجغرافية، فهو مجتمع متفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع لحرس الحدود .

فنجد مع ظهور شبكات المعلومات لم يعد هناك حدود مرئية ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالمقدرة التي تتمتع بها الحواسيب وشبكاتها في نقل كميات كبيرة من المعلومات وتبادلها بين الانظمة يفصل بينها ألاف الاميال قد أدت إلى نتيجة مؤداتها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية في آن واحد، فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل بالإمكان إرتكاب جريمة عن طريق حاسوب موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دولة أخرى.

---

[1]-ناير نبيل عمر، **الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية**، دار الجامعة الجديدة، مصر، 2012، ص 32.
[2]-ربيعي حسين، **اليات البحث والتحري عن الجرائم المعلوماتية**، مذكرة دكتوراه، تخصص قانون العقوبات، كلية الحقوق والعلوم السياسية، جامعة باتنة، الجزائر، 2015-2016، ص28.
[3]-عبد الفتاح، بيومي حجازي، **مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي (دراسة معمقة في مكافحة جرائم التقنية الحديثة)**، دار النهضة العربية، الطبعة الأولى، مصر، 2009، ص460.

هذه الطبيعة التي تتميز بها الجريمة المعلوماتية كونها جريمة عابرة للحدود خلقت العديد من المشاكل حول تحديد صاحبة الإختصاص القضائي لهذه الجريمة وكذلك حول تحدي القانون الواجب تطبيقه،[1]

بالإضافة إلى إشكالية بالإجراءات ملاحقة القضائية، وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام.

ونتيجة لهذه الطبيعة الخاصة للجريمة النصب المعلوماتية ونظرا للخطورة التي تشكلها على المستوى الدولي، والخسائر التي قد تتسبب بها، تعالت الأصوات الداعية إلى التعاون الدولية المكثف من أجل التصدي لهاته الجرائم والتعاون الدولي يتمثل في المعاهدات الإتفاقيات الدولية التي تعمل على توفير جو من التنسيق بين الأعضاء، الأمر الذي يكفل الإقاع بمجرمي المعلوماتية وتقديمهم للقضاء العادل.

وبالتالي من أجل التصدي للإجرام المعلوماتي لابد من أن تعمل الدول في إتجاهين واحد داخلي والأخر دولي، وأما الداخلي يكون من خلال أن تقوم الدولة في سن القوانين الملائمة في مكافحة هذه الجرائم، وأما الدولي يكمن في عقد الإتفاقيات الدولة، حتى لايستفيد مجرموا المعلوماتية من عجز التشريعات الداخلية من ناحية وغياب الإتفاقيات الدولية التي تتصدى لحماية المجتمع الدولي من نتائج وآثار هذه الجرائم.

ثانيا: صعوبة إكتشاف الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بصعوبة إكتتشافها وإذا أكتشفت قد يكون ذلك بمحض الصدفة عادة.

حيث يعد ومن الواضح أن عدد الحالات التي تم فيها إكتشاف هذه الجرائم قليلة إن قورنت بما يتم إكتشافه من الجرائم التقليدية، حيث يمكن رد الأسباب التي تقف وراء الصعوبة في إكتشاف الجريمة المعلوماتية إلى عدم ترك هذه الجريمة لأي أثر خارجي بصورة مريبة، كما أن الجاني يمكنه إرتكاب هذه الجريمة في دول قارات أخرى، إذ أن الجريمة المعلوماتية، كما سبق وأشرنا –جريمة عابرة للدول (الدولية) وكذلك فإن قدرة الجاني عن تدمير دليل الإدانة في اقل من الثانية الواحدة بشكل كاملا إضافيا في صعوبة إكتشاف هذا النوع من الجرائم.

فالجرائم المعلوماتية في أكثر صورها خفية لا يلحضها المجني عليه أولا يدري حتى لوقعها والإمعان في حجب السلوك المكون لها وإخفاقه عن طريق التلاعب الغير المرئي في النبضات أو الذبذابات الإلكترونية التي تسجل البيانات عن طريق أمرا عسيرا في الكثير من الاحوال بحكم توافر المعرفة والخبرة في مجال الحسابات غالبا لدى مرتكبيها.

كما أن المجني عليه يلعب دورا رئيسيا في صعوبة إكتشاف وقوع الجريمة المعلوماتية حيث تحرص أكثر الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك أو تمني بخسارة فادحة من جراء ذلك على عدم الكشف

[1]-نهلا عبد القادر المومني، **الجرائم المعلوناتية**، دار الثقافة للنشر والتوزيع، الطبعة الثانية، الأردن، 2010، ص ص50-51.

حتى بين موظفيها كما تعرضت له وتكتفي عادة بإتخاذ إجراءات إدارية داخلية دون الابلاغ عنها لسلطات المختصة تجنبا لاضرارسمعتها ومكانتها وهز الثقة في كفاءتها".

ويرى البعض أن للمجني عليه دورا مثيرا للريبة في بعض الأحيان فقد يشارك بطريق غير مباشرة في إرتكاب الفعل وذلك بسبب وجوده في ظروف تجعل تعرضه للجريمة المعلوماتية أمرا مرتفعا بشكل كبير، ويرجع ذلك بشكل أساسي إلى القصور الامني الذي يعتري الأنظمة المعلوماتية التي قد يساعد على إرتكاب الفعل الإجرامي، ويترتب على ذلك نتيجة أخرى تميز الجريمة المعلوماتية من أن هناك إمكانية للحيلولة دون وقوع هذه الجريمة مقارنة بغيرها من الجرائم، إذ يعتمد ذلك أساسا على تطوير نظم الامن الخاصة بانظمة الحسابات وشبكاتها[1].

وفي الواقع فإن احجام المجني عليه عن الإبلاغ عن وقوع الجرائم المعلوماتية يبدوا أكثر وضوحا في المؤسسات المالية، مثل البنوك والمؤسسات الإدخارية ومؤسسات الإقتراض والسمسرة، حيث تخشى مجالس إدارتها من ان تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم أو إتخاذ الإجراءات القضائية حيالها إلى تضاؤل الثقة فيها من جانب المتعاملين معها، حيث أن الجانب الأكبر من الجرائم المعلوماتية لا يتم الكشف أو التبليغ عنه فإن ذلك يؤثر سلبا في السياسة التي يمكن أن توقع لمكافحتها، وقد تم طرح عدة إقتراحات تكفل تعاون المجني عليه في كشف هذه الجرائم وبالتالي لإنقاص حجم الإجرام المعلوماتي الخفي.

ثالثا: جريمة النصب تصنف ضمن جرائم الأموال

فقد جرت غالبية التشريعات على التفرقة بين قسمين من الجرائم وهي الجرائم المضرة بالمصلحة العامة والجرائم المضرة بالافراد وقد درج شراح القانون على تقسيم الجرائم المضرة بالافراد إلى قسمين ايضا وهما: جرائم الاعتداء على الاشخاص وجرائم الاعتداء على الاموال، وهذا النوع الاخير من الجرائم الذي ينقص أو يعدل من العناصر الايجابية للذمة المالية أو تزيد من عناصرها السلبية.

رابعا: جريمة النصب هي جريمة ذهنية

فمن المستلزمات الأساسية لهذه الجريمة أن تكون لدى المحتال مقدرة ذهنية على كشف الثغرات في نظام التعامل كي يستطيع خداع ضحاياه فيستغل الجاني ذكاءه ودهاءه في إرتكاب الجريمة دون إستخدام وسائل السلب والعنف والقسوة وذلك لامتلاكه غالبا للتخصص والدراية الفنية في مجاله خاصة عالم المعلوماتية[2].

ومن هنا فإن جريمة النصب اللإلكتروني هي من الجرائم المعلوماتية الذاتية تبرز كثيرا وضوحها في أسلوب إرتكابها وطريقتها، فإذا كانت الجرائم التقليدية تتطلب نوع من المجهود العضلي "[3] الذي قديكون في

1-نهلا عبد القادر المومني، مرجع سابق، ص 52، 55.
2-اسامة حمدان الرقب، مرجع سابق، ص ص 24-25.
3-نهلا عبد القادر المومني، مرجع سابق، ص57.

صورة ممارسة العنف والإذاء كما هو الحال في جريمة القتل أو الإختطاف أو في صورة الخلع أو الكسر وتقليد المفاتيح كما هو الحال في جريمة السرقة...فإن الجرائم المعلوماتية هي جرائم هادئة بطبيعتها (soft crème) لاتحتاج إلى العنف بل كل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوصف في إرتكاب الأفعال الغير مشروعة.

وتحتاج كذلك إلى وجود شبكة المعلومات الدولية (الأنترنت) مع وجود مجرم يوظف خبرته أو قدرته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس أو إختراق خصوصيات الغير او التغرير بالقاصرين كذلك تحدث دون حاجة لسفك الدماء.

خامسا: الجريمة المعلوماتية تتم عادة بتعاون اكثر من شخص

تتميز الجريمة المعلوماتية بأنها تتم بتعاون أكثر من شخص أي غالبا ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والانترنت يقوم بالجانب الفني من المشروع الإجرامي وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه".

سادسا: خصوصية مجرمي المعلوماتية

"المجرم الذي يقترف الجريمة المعلوماتية الذي يطلق عليه المجرم المعلوماتي يتسم بخصائص معينة تميزه عن المجرم الذي يقترف الجرائم التقليدية (المجرم التقليدي)".

فإن كانت الجريمة التقليدية لا أثر فيها للمستوى العلمي والمعرفي للمجرم في عملية إرتكابها، بإعتبارها قاعدة عامة فإن الأمر يختلف بالنسبة للجرائم المعلوماتية فهي جرائم فنية تقنية في الغالب الأخص، ومن يرتكبها يكون عادة من ذوي الإختصاص في مجال تقنية المعلومات، أو على الأقل شخص لديه أدنى من المعرفة والقدرة على إستعمال جهاز الحاسوب والتعامل مع شبكة الأنترنت.

فعلي سبيل المثال فإن الجرائم المعلوماتية ذات الطابع الإقتصادي مثل التحويل الإلكتروني غير المشروع للأموال يتطلب مهارة وقدرة فنية تقنية عالية جداً من قبل مرتكبيها كذلك فإن البواعث على إرتكاب المجرم التقليدي"[1].

الفرع الثالث: التمييز بين جريمة النصب الإلكتروني وبين ما يشبهه من جرائم

إن مسألة التمييز بين هذه الجريمة وما يشابهها من جرائم سوف ينصب كله في مصب الجريمة الإلكترونية، إلا أنها تختلف في بعض الشيء وتشترك في البعض الآخر وبالتالي تشترك في التنصنيف وتختلف في الوسيلة والعقوبة، وسوف نميز الآن بين النصب الإلكتروني والسرقة المعلوماتية وبين خيانة الامانة المعلوماتية والنصب الإلكتروني وبينه وبين التزوير المعلوماتي.

[1]-نهلا عبد القادر المومني، مرجع سابق، ص58.

أولا: التميز بين النصب الإلكتروني وبين السرقة المعلوماتية

لقد تعرفنا نوعا ما على معنى النصب الإلكتروني من خلال التعريف والخصائص إلا أننا لا نستطيع التمييز بينه وبين السرقة المعلوماتية إلا إذا تعرفنا على هذه الأخيرة، إذ تتفق التشريعات الجنائية على أن السرقة حسب القواعد العامة هي إختلاس مال منقول مملوك للغير بنية تملكه، وبالتالي محل السرقة هو المال.

غير أن المحل في السرقة المعلوماتية هو معلومات ذات كيان معنوي، قد تكون هذه المعلومات عامة وقد تكون خاصة كالتي تتعلق بالابحاث علمية معينة أو ببرمجيات تتحتوي على نظم تشغيل تكون محلا للتعامل عليها من قبل أصحابها مع الغير، وقد تكون هذه المعلومات ذات قيمة إقتصادية هدفها تحقيق الربح كما هو الحال في التجارة الإلكترونية والتسويق الالكتروني، وقد تكون ذات قيمة معنوية كسرقة المعلومات من أجل إفشاء أسرار شخصية بقصد الإضرار بالغير، ومنها إذا اردنا التمييز بين النصب الإلكتروني والسرقة الالكتروني فعلينا أن نبين الفرق بينهما فيما يلي[1]:

أ. المحل في النصب هو المال، أما المحل في السرقة هو المعلومات.

ب. الإستلاء على حيازنة الشيئ يكون في السرقة بالاختلاس بدون رضا صاحبه، أما النصب فيعتمد على خداع المجني عليه وتضليله بوسائل الإحتيال على نحو يخلق لديه إعتقاد مخالف للواقع يدفعه إلى تسليم ماله إلى الجاني برضاه.

ت. إرادة الضحية في السرقة تكون معدومة، أما إرادة الضحية في النصب تكون سليمة يشوبها عيب الغش والتدليس.

ثانيا: التمييز بين النصب الإلكتروني وبين خيانة الأمانة المعلوماتية

عرفت المادة 376[2] قانون العقوبات خيانة الأمانة على أنها " كل من إختلس او بدد بسوء نية أوراقا تجارية أو نقودا او بضائع أو أوراقا مالية أو مخالصات أو أي محررات لأخرى تتضمن أو تثبت إلتزاما او إبراء لم تكن قد سلمت إليه إلا على سبيل الإجازة أو الوديعة أو الوكالة أو الرهن أو عارية الإستعمال او لأداء عمل بأجر أو بغير أجر بشرط ردها أو تقديمها أو لاستعمالها أو لاستخدامها في عمل معين وذلك إضرارا بمالكيها او واضعي اليد عليها أو حائزيها يعد مرتكبا لجريمة خيانة الأمانة..." .

أما جرمية خيانة الأمانة في صورتها المعلوماتية قد عرفتها المادة 5 من القانون العربي النموذجي الموحد على أنها " كل من استخدم أي وسيط الكتروني وبدون وجه حق في الحصول على الخدمات التي يقدمها، يعاقب بالحبس الذي لا تقل مدتها) تترك لكل دولة تحديد المدة....

---

[1]-عصام عبد الفتاح مطر، **التجارة الألكترونية في التشريعات العربية والاجنبية**، دار الجامعة الجديدة، مصر، 2015، ص ص 314-315.

[2]-المادة 376 قانون العقوبات

حيث يرى الفقه ان التسليم هو العنصر المميز لخيانة الأمانة إذا إقترن مع قصد ونية نقل الحيازة الناقصة او المؤقتة بحيث يكون المستلم ملتزم برد أو تقديم الأشياء التي تسلمها إلى صاحبها[1]، وهذا واضح من طبيعة العقود التي وردت في المادة 376 قانون العقوبات مثل الإجازة أو الوديعة أو الوكالة...

ويتضح مما سبق أن خيانة الأمانة يكون محلها مال منقول وحتى تنطبق هذه القواعد على خيانة الأمانة المعلوماتية فيتوجب إعتبار المعلومات والبيانات المبرمجة في الحواسيب مال معلوماتي يمكن أن يكون محل لخيانة الأمانة المعلوماتية، متى كان هذا المال المعلوماتي مخزن على الوسائط الإلكترونية قد سلم إلى الجاني بناء على عقد من عقود الأمانة المنصوص عليها في نص المادة أعلاه فقام بالاستعماله لنفسه وظهر على المال بمظهر المالك[2].

ثالثا: تمييز النصب الإلكتروني عن التزوير المعلوماتي:

تعد جريمة التزوير من جرائم الغش في مجال المعلوماتية خاصة بعد أن أصبح النظام المعلوماتي في هذا العصر يحل محل الأوراق كالمحررات والصكوك في كافة مجالات الحياة وإن ما يقع على هذه الانظمة المعلوماتية من اعتداءات بالعبث بالبيانات والمعلومات المخزنة[3] من شأنه إحداث ضرر ماديا أو معنويا للغير، كالذي يحدثه التزوير الذي يعرف التزوير بأنه تغيير الحقيقة في المحرر بإحدى الطرق التي حددها القانون، تغير من شأنه أن يرتب ضررا للغير وذلك بنية إستعمال هذا المحرر فيما أعدّله، أما التزوير المعلوماتي فهو التزوير الذي يتم بوسيلة معلوماتية في محرر معلوماتي أو بوسيلة إلكترونية في محرر إلكتروني، وتكون هذه المحررات معالجة عن طريق الحاسب الآلي، فتصبح كيانا ماديا ملموسا يقابل أصل المحرر المكتوب وحسب هذا التعريف فلابد أن يرد التزوير المعلوماتي على البيانات أو المعلومات معالجة عن طريق الحاسب الآلي ومن ناحية أخرى فإنه يجب أن تدون هذه البيانات والمعلومات على كتاب مادي ملموس قد يكون ورقة مطبوعة من طابع الحاسب اللآلي أو نسخ على شريط ممغنط أو قرص مدمج وفي هذه الحالة فقط يمكن القول بوقوع التزوير المعلوماتي[4].

الضرر في التزوير المعلوماتي نجد أن المحرر الإلكتروني سواء كان رسميا أو عرفيا فهو معدّ لإثبات واقعة معينة فإن ترتب على هذا التزوير إهدار لحجتيه في الاثبات أو القيمة الثبوتية فهناك قد وقع الضرر يقوم التزوير[5].

1-أحمد خليفة الملط، **الجرائم المعلوماتية**، دار الفكر الجامعي، مصر، 2005، ص448.
2-عبد الفتاح، بيومي حجازي، مرجع سابق، ص494.
3-أحمد خليفة الملط، مرجع سابق، ص525.
4-عبد الفتاح بيومي حجازي، **الجريمة في عصر العولمة دراسة ظاهرة الاجرامية المعلوماتية**، دار الفكر الجامعي، مصر، 2008، ص ص 99، 101.
5-عبد الفتاح بيومي حجازي، مرجع سابق، ص 119.

أما التميز بينه وبين النصب الإلكتروني فيتلخص في النقاط التالية:

أ. النصب الإلكتروني يقع بالاستلاء فمحله مال الغير أما التزوير فمحله المحررات سواء كانت رسمية أو عرفية.

ب. النصب الإلكتروني يعتمد على الطرق الإحتيالية أما التزوير فيقوم على تغير حقيقة المحرر.

ت. الكذب في النصب الإلكتروني يمكن أن يكون شفويا أما الكذب في التزوير لابد أن يكون كتابيا.

المطلب الثاني: أساليب جريمة النصب الإلكتروني

لكل جريمة أساليبها الخاصة بها التي تقوم بفضلها، ولجريمة النصب الإلكتروني أساليب خاصة بها أيضا، وهي كالاتي:

الفرع الأول: إستعمال طرق إحتيالية

لا يتم النصب إلا إذا إستعملت طريقة من طرق الإحتيال التي وردت في نص المادة على سبيل الحصر 372 من قانون العقوبات، والتي تتمثل في إستعمال أسماء أو صفات كاذبة من خلال إنتحال شخصية الغير أو اسم الغير أو علامته التجارية، بحيث تنخدع الضحية فيكون للادعاء أثر في نفسها يدعوها للتصديق، كما يتم النصب بإستخدام سلطة خيالية أو إعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيء في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها تطبيقا لنص المادة 372 من الأمر 66-156 سالف الذكر.

كما قد تاخذ جريمة النصب والإحتيال الواقعة على المستهلك الإلكتروني صورا أخرى لا يمكن عدها ولا حصرها خلافا لما جاءت به المادة 372 من قانون العقوبات، ومن صور الإحتيال الأكثر شيوعا ما يلي[1]:

أولا: عدم تسليم السلعة المتعاقد عليها بالرغم من سداد ثمنها:

من اهم الإلتزامات التي تقع على عاتق المستهلك هو دفع الثمن وهذا ما نصت عليه المادة 16 من قانون 18-05، حيث يقع على عاتق المستهلك دفع الثمن بطريقة رقمية بإستخدام الكمبيوتر، إلا أنه كثير من الأحيان يكون عرضة للنصب والإحتيال، حيث لا يتمكن من الحصول على ما تعاقد من أجله رغم دفع الثمن المتفق عليه.

ثانيا: الترويج لسلعة مقلدة شبيهة بمنتج أصلي غالي الثمن والجودة: تقليد بعض العلامات التجارية أصبح ظاهرة عالمية تتخذ مظاهر متعددة، إذ يقوم المورد الإلكتروني المحتال بعرض منتجات مقلدة تشبه الأصلية إلى حد كبير مع إيهام المستهلك بانها ذات السلعة بثمن أقل كعرض خاص وحصري من الموقع.

---

[1]-العايب سامية،عرابة منال، **"الحماية الجزائرية للمستهلك من جريمة النصب الإكتروني"**، مجلة هيرودوت للعلوم الإنسانية والإجتماعية، المجلد 05، العدد 03، 2021، ص ص 229، 243.

ثالثا: الترويج لسلع غير معروفة بإستخدام الإعلان المضلل:

أدت الزيادة النهائية في الإنتاج والمنافسة على التسويق عبر الأنترنت إلى إستخدام الطرق الإحتيالية والتظليل في الإعلان، حيث يقوم مورد سلعة غير مشهورة بالإشهار عنها بإعلان كاذب ومظلل من شأنه التعزيز بالمستهلك وخداعه بسهولة، إذ كثيرا ما يشكل الإشهار التجاري المظلل وسيلة إبتزاز ونصب للأموال، فميزة الكذب التي نص عليها المشرع في المادة 372 من قانون العقوبات عند تعداده لصور الإحتيال في جريمة النصب في عبارة "بإستعمال اسماء أو صفات كاذبة" تتحق عن طريق الإشهارات والإعلانات المظللة.

رابعا: سلب مال الغير:

تتم جريمة النصب بتحقيق نتيجتها وهي إستلاء الجاني على المال الذي تسلمه من المجني عليه بعد قيام الجاني بخداع المجني عليه بطرق الإحتيال التي سبق ذكرها، وقد عرفت المادة 372 محل الجرمية، ويتعلق الأمر بالأموال والمنقولات والسندات والتصرفات والاوراق المالية والوعود والمخالصات والإبراء من الإلتزامات.

فلا يكفي لقيام جريمة النصب مجرد إستعمال الوسائل والطرق الإحتيالية، بل يجب أن يتحصل الفاعل جراء إستعمال هذه المناورات الإحتيالية على القيم وأموال غير شرعية إضرار بالغير[1].

الفرع الثاني: إتخاذ الإسم الكاذب أو إنتحال الصفة غير الصحيحة

أساس النصب هو الكذب والإيهام، شرط أن يستعين بمظاهر خارجية تجعل المجني عليه يصدق الجاني إلى درجة تسليم ماله برضاه، غير أن هذا الاسلوب اختلف في شكله وفي وسائله التي عرفها النصب التقليدي الذي كان يكفي فيه ان يتخذ النصاب اسما كاذبا لشخص حقيقي او خيالي كإسم فنان مشهور أو ينتحل صفة كاذبة كأن يدعي انه ضابط شرطة أو طبيب او محامي وهكذا...، أما شكل اتخاذ الاسم وانتحال الصفة الكاذبة في النصب الالكتروني فيكون باستعمال الكمبيوتر وتكنولوجيا الاعلام والاتصال، سواء عبر مواقع التواصل الاجتماعي أو من خلال التلاعب بالبيانات والمعطيات داخل النظام الالي للحواسيب مثل شركات الوهمية، مسابقات لا أساس لها من الصحة، الأمل الكاذب.

الفرع الثالث: التصرف في مال الغير، ثابت او منقول

دخلت هذه الوسيلة في وسائل النصب وأصبحت أسلوب من اساليب النصب بعدما أصبح النصابون يلجأون إلى التصرف في أملاك الآخرين المجني عليهم حسني النية بعد الاستلاء على أموالهم وليتحقق هذا الاسلوب يجب توافر شرطان اساسيان هما[2]:

---

[1]-العايب سامية،عرابة منال، مرجع سابق، ص ص 229، 243.

[2]-عبد الحكيم فودة، **جرائم الاحتيال النصب وخيانة الامانة والشيك والعاب القمار في ضوء الفقه وقضاء النقض**، دار المطبوعات الجامعية، مصر، 2006، ص12.

- أن يقع التصرف في ملك الغير.
- عدم ملكية الجاني للشيء وعدم أحقيته في التصرف فيه.

أولا: الشرط الأول: التصرف في ملك الغير: وهو تصرف الصادر من الجاني وقد يكون هذا التصرف ناقلا للملكية كالبيع أو المقايضة أو الهبة، وقد يكون مرتبا لحق عيني كالرهن وتقرير حق الإنتقال وإرتفاق على العين

ولا يشترط في التصرف أن يكون مكتوبا، بل يجوز أن يكون شفويا وعندئذ يجوز اثباته بكافة الطرق لتعلق الأمر أولا بجريمة وثانيا بواقعة مادية يجوز إثباتها بالبينة والقرائن.

ومحل التصرف قد يكون عقارا وقد يكون منقولا، ولا يشترط لتحقيق هذه الوسيلة من وسائل النصب أن يتم تسليم المنقول أو العقار، أو تسجيله بل يكفي مجرد التصرف.

ثانيا: الشرط الثاني: انعدام الأحقية في الملكية أو التصرف: يشترط لتحقيق هذه الوسيلة ألا يكون الجاني مالكا للعقار أو المنقول وليس ذلك فقط بل أيضا لا يحق له التصرف فيه قانونا فإذا لم يكن مالكا ولكن له حق التصرف فيه بسبب صفته النيابية فلا تقوم الجريمة[1].

[1]-عبد الحكيم فودة، مرجع سابق، ص13.

المبحث الثاني: أركان جريمة النصب الإلكتروني

كل مرة ندرس فيها أركان الجرائم إلا ووجدنا ثلاثة أركان وهي الركن الشرعي والمادي والمعنوي، إلا أن الجرائم المعلوماتية تمتاز بركن رابع يجب أن يتوفر لقيام أي جريمة منها وهو:

الركن الإفتراضي: الذي يفترض ويستلزم وجود نظام المعالجة الآلية للمعطيات هذا الأخير عرفه الفقه بأنه "عبارة عن آلية وإجراءات منظمة تسمح بتجميع وتصنيف وفرز البيانات ومعالجتها ومن ثم تحويلها إلى معلومات يسترجعها الإنسان عند الحاجة للتمكن من إنجاز عمل أو إتخاذ قرار أو القيام بأي وظيفة عن طريق المعرفة التي تحصل عليها من المعلومات المسترجعة من هذا النظام"[1].

ومن هنا يمكن متابعة دراسة باقي الأركان على النحو التالي:

المطلب الأول: الركن المادي لجريمة النصب الإلكتروني

لقد إعتبر الفقهاء الركن المادي هو الركن الأساسي لتكون هذه الجريمة كاملة ووفق نص المادة 372 من قانون العقوبات الجزائري فإن الركن المادي يتألف من ثلاثة عناصر وهي النشاط الإجرامي والنتيجة الإجرامية والعلاقة السببية، فإذا توفرت هذه العناصر فهي جريمة كاملة تتمثل في سلوك يؤدي للنتيجة.

الفرع الأول: السلوك الإجرامي

حتى تكون هناك مسؤولية في جريمة النصب لا بد للجاني باستعمال وسيلة من وسائل التدليس لنصب أو سلب مال الغير، حسب ما نص في المادة 372 من قانون العقوبات الجزائري على سبيل الحصر ولن يكون هناك تدليس ما لم يقوم على الكذب والإحتيال، حيث أنه من المسلم به فقها وقضاء ان الكذب المجرد لا يكفي لتوفير الطريقة الإحتيالية، مهما تنوعت صيغته[2].

والنشاط الإجرامي هو ممارسة المحتال أساليب لابد أن تكون محددة، لمزاولة عملية النصب والإحتيال طبقا لقانون (لاعقوبة ولاجريمة إلا بنص قانوني وكنا قد تطرقنا لهذه الاساليب بالتفصيل فالمطلب لبثني الخاص بأساليب جريمة النصب الإلكتروني)[3].

بمعنى أن الكذب لا يكون كفيل لوحده لقيام النشاط الإجرامي لابد ان تكون هناك أفعال وأعمال مادية تجعل المجني عليه يقع في دوامته ليعتقد بأنه صحيح، وذلك عن طريق إنتحال صفات الكذب أو إسم كاذب مثلا إلهام شخص ويجعله يتأمل بالفوز بشيء، أو مبلغ مالي أو غيرها من الطرق الإحتيالية على سبيل المثال: قد يلجئ المحتال لتأييد فكرته الإحتيالية والكاذبة بإتخاذ وسيلة خارجية كالنشر عبر الصحف والمجالات أو فتح صفحة عبر مواقع التواصل الإجتماعي، عبر نشر معلوماته الشخصية الإنتحالية وعن مشروعه أو شركته

---

[1]-بن دراح علي ابراهيم، **محاضراة في الجرائم المعلوماتية معهد الحقوق والعلوم السياسية**، قسم الحقوق المركز الجامعي افلو، الجزائر، 2020-2021، ص9.

[2]-رحال بومدين، سعداني نورة، **الحماية الجنائية الواقعة على أموال التجارة الإلكترونية (جريمة السرقة والنصب)**، مجلة الواحات للبحوث والدراسات، المجلد 09، العدد 02، 2016، ص ص 100-101.

[3]العودة الى الصفحة 14 .15 .16 للتعرف على الاساليب بالتفصيل.

وفتح حساب في البنك، فكل ذلك يعد من المظاهر الخارجية التي تؤثر في عقلية الشخص، وتكون الغاية من ذلك إكتساب فعل غير مشروع.

الفرع الثاني: النتيجة الإجرامية

يعد هذا العنصر أحد عناصر الركن المادي في الجريمة إلى جوار السلوك الإجرامي وعلاقته السببية، وتثير مسألة النتيجة الإجرامية في جرائم الانترنت مشاكل عدة اهمها، تحديد هل الجريمة المرتكبة سلوك ونتيجة في العالم الافتراضي أم أن هناك امتداد للنتيجة ليتحقق منتهاها في العالم المادي؟[1].

ومما سبق فإن الجاني يستولي على مال الغير بدون وجه حق، نتيجة الوسائل الإحتيالية المستعملة، أما الحاسب الالي، ذلك أن هذا الأخير يعد أداة إيجابية في جريمة النصب المعلوماتي متى تم التدخل مباشرة في المعطيات بإدخال معلومات وهمية أو بتعديل البرامج أو خلق برامج صورية وليس هناك صعوبة في اكتشاف الطرق الاحتيالية في هذه الحالات.

الفرع الثالث: العلاقة السببية

تكون جريمة كاملة على الجاني ان يرتكب إحدى وسائل الإحتيال المنصوص عليها في المادة 372 من قانون العقوبات الجزائري تم إستلائه على مال منقول مملوك للغير "وإنما يجب تقوم العلاقة السببية بين وسائل الإحتيال التي يستعملها الجاني وتسلم المجني عليه المالي، يعني يجب أن يكون تسليم المال ضمن وسائل الإحتيال التي لجأ لها الجاني.

أما إذا تسلم شخصا من صديق له مال على سبيل الأمانة ثم إرتكب إحتيال وضم تلك الأمانة لممتلكاته، فإنه لا يعاقب على جريمة النصب وإنما على خيانة الأمانة والسرقة، هنا يجب أن تكون وسيلة من وسائل الإحتيال التي قام بها الجاني من شأنها أن تؤدي إلى تسليمه مال منقول دون تأثير بهذه الوسيلة وكان التسليم لسبب آخر لادخل للجاني فيه فلا وجود لجريمة النصب لانقطاع العلاقة السببية[2].

لا نصب إلا إذا كان الإستلاء على المال قد وقع سابقا على قيام جانب بالطرق الإحتيالية، إذ تنعدم رابطة العلاقة السببية.

فنقول إن العلاقة السببية أنها تلك الصلة او الرابطة المادية بين السلوك الإجرامي للجاني وبين النتيجة، وحتى يتحقق الركن المادي لابد من وجود علاقة سببية بين فعل الخداع الجاني وتسليم المجني المال.

فإذا لم يرجع تسليم المجني عليه مال الجاني إلى الطرق الإحتيالية التي مارسها الغير، رغم وقوع هذه الطرق الإحتيالية، ورغم أن قصد الجاني منها كان سلب المال.

---

[1]-زيان سعيد، سالمي هاشم، **جريمة النصب الالكتروني**، مذكرة ماستر، تخصص قانون جنائي،كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف –المسيلة، 2021-2022، ص20.

[2]-رحال بومدين، سعداني نورة، مرجع سابق، ص 105.

فنرى بأن الركن المادي يجب ألا ينقص عنصر من عناصره ليصبح الركن المادي متكامل، يعني إذا بطلت العلاقة السببية بطل الركن المادي ترتكز العلاقة على مال منقول مملوك للغير.

وتقوم هذه العلاقة بين الفعل والنتيجة، الغلط الذي يقع عليه المجني عليه بناء على ما إستعمل من مناورات إحتيالية مما أدى إلى التأثير على إرادته وتوجيهها نحو تسليم المالي للجاني، وعليه فإن الرابطة السببية في جريمة تقتضي على قيام مزدوجة بإسناد الفعل المادي إلى الجاني ثم إستناد النتيجة الجريمة إلى هذا الفعل.

المطلب الثاني: الركن المعنوي لجريمة النصب الإلكتروني

إن جريمة النصب الإلكتروني عمدية تتطلب توفر الركن المعنوي فإن لم تثبت قيام الركن المادي فلا تتحق جريمة النصب حتى لو تبين أن الجاني قد إستعمل وسيلة من وسائل الإحتيال ويشترط فيها القصد العام والقصد الجنائي الخاص، فيكون الجاني بكامل قواه العقلية لتخطيط وبداية للمخادعة والإستلاء على مال الغير

ويتعلق الركن المعنوي بشخصية الجاني وبمسلكه الذهني والنفسي كما لهذا الركن ايضا ثلاث صور في الجرائم المتعلقة بالأنترنت وهذه الصور هي[1]:

الفرع الأول: القصد الجنائي العام

يتطلب القصد العام علم الجاني بالعناصر المتمثلة في ماديات الجريمة، وإنصراف إرادته إلى تحقيق هذه العناصر، يقوم القصد العام على العلم بالاحتيال بأن يعلم الجاني بأنه يرتكب فعل تدليس من شأنه إيقاع المجني عليه في غلط يدفعه إلى تسليم أمواله، فقد يقوم شخص بالتلاعب في البيانات والمعلومات المتواجدة بالحاسب الآلي أو يستخدم إسما وصفة كاذبة للحصول على أموال الغير، ومن ثم فيجب أن يعلم الجاني بأن فعله غير مشروع وأنه يستغل صفة كاذبة[2]، بمعنى آخر يقوم القصد الجنائي العام إلى إتجاه الإرادة لتحقيق العناصر التي تشكل جريمة النصب[3]، فيجب أن يتوفر لديه العلم على محاولته التدليسية[4].

يتحقق القصد العام إذا علم المجرم أنه يرتكب أو يتوصل للاستلاء على مال الغير كله أو بعضه متى وقع على فواتير الشراء بإسم كاذب أو استغل صفة كاذبة لتحويل أموال الغير من حساب إلى آخر عن طريق التلاعب بالمعطيات أو البيانات الإلكترونية ويجب عمله بهذه الوقائع، ومع ذلك تتصرف إراداته إليها رغم عمله بأن فعله من الأفعال التدليسية[5].

1-عبد الفتاح بيومي حجازي، **النظام القانوني لحماية التجارة الإلكترونية**، دار الفكر الجامعي، الكتاب الثاني، مصر، ص 171.
2-مطر عصام عبد الفتاح، **التجارة الإلكترونية في التشريعات العربية والجنبية**، دار الجامعة الجديدة، مصر، 2015، ص321.
3-العايب سامية، عرابة منال، مرجع سابق، ص229-243.
4-مطر عصام عبد الفتاح، مرجع سابق، ص321.
5-عبد الفتاح بيومي حجازي، مرجع سابق، ص 171.

الفرع الثاني: القصد الجنائي الخاص

يقوم القصد الجنائي الخاص إذ إتجهت إرادة الجاني إلى نية الإستلاء وسلب ثروة الغير كلها أو بعضها، بمعنى آخر هي نية التملك، أما إن كان الغرض من وراء الإحتيال هو مجرد الدعابة والمزاح فلا تقوم الجريمة عندئذ[1].

والقصد الخاص هو نية التملك، فيقوم متى كان هدف الجاني من هذا الإحتيال الإستلاء على مال مملوك لغيره، علما بأنه لا عبرة بالبواعث في إرتكاب جريمة النصب سواء كان الباعث نبيلا أم خسيسا، كما يتوافر القصد الخاص في النصب المعلوماتي، متى قام الجاني مثلا بإستخدام البطاقة وهوعالم أن رصيده فارغ أو أن بطاقته موقوفة ويستخدمها[2].

أ. **العمد:** ينبغي لارتكاب الجريمة الإلكترونية أن يكون مرتكبها نابغة في إستعمال الحاسوب، أي أنه يجب أن يكون مكتسبا للمعرفة والتعليم التخصصي ليتمكن من ممارسة هذا النوع من الجرائم وفي هذه الحالة يكون وقوعها في صورة واحدة وهي صورة العمد حيث أن المجرم الإلكتروني يكون قد خطط ودبر لارتكاب هذه الجريمة سواء من أجل الحصول على معلومة أو لإختراق شبكة حاسوب آخر كجريمة النصب تتطلب من الفاعل إرادة إرتكاب السلوك تحقيق نتيجة، وقد يكون القصد عاما أو خاصا.

[1]-العايب سامية، عرابة منال، مرجع سابق، ص229-243..
[2]-عبد الفتاح بيومي حجازي، مرجع سابق، ص 171.

الخلاصة:

من خلال ما درسناه في الفصل الأول من موضوع جريمة النصب الإلكتروني إستطعنا أن نصل إلى فكرة هي: أنه حتى ولو كانت هذه الجريمة معروفة في المفهوم التقليدي إلا أنها في مفهومها الإلكتروني تختلف كثيرا، خاصة في الوسائل الإحتيالية التي أصبحت إلكترونية غير ملموسة، ذهنية واصبحت أخطر من الأولى سواء من حيث سرعة تنفيذ الجريمة أو طمس معالمها وهذا ما يمنحها ركنا إضافيا إلى جانب الأركان التقليدية للجريمة، المادي والمعنوى، وهو الركن الإفتراضي، إذ من خصائص جريمة النصب الإلكتروني أن تحدث في نطاق إلكتروني أو بوسائل الكترونية.

الفصل الثاني: الجوانب الإجرائية والموضوعية لجريمة النصب الإلكتروني

تمهيد:

ان دراسة الجانب الاجرائي والموضوعي لجريمة النصب الالكتروني، يمكننا من فهم االمفهوم القانوني لهذه الجريمة ويمكننا ايضا، من ادراك صعوبة تحديد هذا المفهوم في الجرائم التي ليس لها نص قانوني خاص بها وانما تقع تحت طائفة الاسقاط الذي يتطلب دراية قانونية، ومن هنا حاولنا أن نوصل الفكرة على قدر المستطاع، سوف نتطرق في هذا الفصل إلى الجانب التطبيقي والإجرائي من الدراسة موضحتين كل ما يتعلق بالاختصاص ونطاقه وتحديد أنواعه ومعاييره، ثم إجراءات المتابعة التقليدية منها والمستحدثة في الكشف عن جريمة النصب كجريمة إلكترونية مع بعض الصعوبات التي تتعلق بالإثبات في مثل هذه الجرائم لنصل في المبحث الثاني إلى تفصيل العقوبات المقررة سواء على الأشخاص الطبيعة أو المعنوية.

المبحث الاول: نطاق الإختصاص في جريمة النصب الالكتروني وإجراءات التحقيق فيها

تعتبر المتابعة الجزائية من أهم الخطوات لكشف معالم الجريمة الإلكترونية، ولقد أولى لها المشرع الجزائري جملة من الإجراءات التي من شأنها مساعدة جهات التحقيق في إيجاد الدليل وإظهار الحقيقة وتتنوع هذه الإجراءات بين التقليدية وبين المستحدثة التي راع فيها خصوصية الجريمة الإلكترونية لجريمة النصب الإلكتروني وهذه الطبيعة الخاصة للجرائم المستحدثة تجعل من معايير الاختصاص التقليدية لا تتلائم مع تحديد محل وقوع الجرم في العالم الافتراضي ولا تتلائم مع المبادئ الأساسية التي تحكم مسألة الاختصاص ومن ثم فإن هذه الطبيعة المتعدية للحدود الجغرافية تنعكس على إمكانية ضبطها والتصدي لها ومن هنا توجب دراسة معايير الاختصاص ونطاق تطبيق الإجراءات الجزائية كما يلي[1]:

المطلب الأول: معايير تحديد الإختصاص والإختلاف الفقهي حول تمديد الإختصاص

لكل مبنى ركيزة وركيزة تطبيق القانون هو الإختصاص فلا يمكن أن يأخذ القانون مجراه دون تحديد الإختصاص سواء النوعي من حيث الموضوع أو الإقليمي من حيث المكان والزمان، ومن هنا سنوضح معايير تحديد هذا الإختصاص، التباين بين مختلف الاراء في هذا المجال لنصل الى موقف المشرع الجزائري في مسالة الإختصاص.

الفرع الأول: الموقف الفقهي والقضائي والتشريعي من مسألة الإختصاص في جريمة النصب الإلكتروني

إن من الحقوق التي كفلها الدستور للمواطنين هو حق اللجوء إلى القضاء وضمانا لحسن سير العدالة ولتقريب العدالة من المواطنين أقر المشرع عدة مبادئ منها التقاضي على درجات (إختصاص نوعي) وهذا يؤدي إلى تحديد درجة المحكمة المختصة (محكمة إبتدائية، مجلس قضائي، الأقطاب الجزائية، محكمة عليا)

وأقر تعدد المحاكم ذات الدرجة الواحدة مما يؤدي إلى وضع قواعد تبين إختصاص المحكمة التي تنظر في الدعوى ذات الدرجة الواحدة وهذا يؤدي إلى نتيجة حتمية وهي وجوب إيجاد قواعد تبين نصيب كل محكمة من النزاعات المعروضة وهو ما يعرف بالاختصاص.

وهو ما نص عليه المشرع في قانون الإجراءات الجزائية، فالاختصاص هو السلطة التي يقررها القانون لجهة قضائية معينة للنظر في دعاوي من نوع معين والإختصاص الجزائي هو السلطة التي خولها القانون إلى الجهات القضائية الجزائية للنظر في الدعاوي العمومية باختلافها، ويعرف بأنه صلاحية مباشرة الجهة القضائية لإجراءات المتابعة والتحقيق والحكم بمقتضى القانون في الدعوى، ويقصد بالمحكمة المختصة التي يمنحها القانون سلطة الفصل في هذه الأخيرة.

وعليه سنبين الموقف الفقهي والقضائي والتشريعي من مسألة الإختصاص.

[1]-حبيب بوسماط، **جريمة النصب باستعمال الوسائل المعلوماتية**، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، الجزائر، 2018-2019، ص77.

أولا: موقف الفقه من مسألة الإختصاص

إن عالمية شبكة الأنترنت وسهولة الحصول على خدماتها كما أن سهولة حركة المعلومات عبر الأنظمة التقنية عبر الشبكة المعلوماتية جعل بالإمكان إرتكاب الجرائم عن طريق الحاسوب ليس ممكنا فقط بل يسيرا، وهو بالفعل موجود في معظم الدول، وقد يكون الفعل الإجرامي في دولة والنتيجة الإجرامية في دولة أخرى، هذه الطبيعة التي تميز بها الجريمة الإلكترونية كونها جريمة عابرة الحدود خلقت العديد من المشاكل حول تحديد الدولة صاحبة الإختصاص القضائي، وكذلك حول تحديد قانون الواجب التطبيق في هذه الحالة.

كما أن مسألة الإختصاص القضائي في الجرائم الإلكترونية لا تخلو من الصعوبات فتارة تؤدي إلى إثارة التنازع الإيجابي في الإختصاص بين أكثر من تشريع دولي وتارة أخرى يقوم التنازع السلبي في الإختصاص أي تمتنع اي دولة من الدول المعنية بملاحقة الجاني وهذا النوع الأخير من التنازع نادر الوقوع.

وفي حالة قيام التنازع الإيجابي في الإختصاص بين أكثر من دولة لملاحقة نفس النشاط الإجرامي، أو في حالة الجرائم التي يتوزع فيها السلوك المادي للجريمة في إقليم أكثر من دولة تتطلب بطبيعة الحال حلول مستحدثة وإبتكارا لمفاهيم قانونية جديدة دون الإخلال بالمبادئ الشرعية الجزائية التي ترتكز عليها معظم النظم الجنائية وهي مبدأ الإقليمية.

ففكرة السيادة كل دولة على إقليمها وهذا ما يحدث في الجرائم الإلكترونية عندما يرتكب شخص جريمة في إحدى الدول وتجري محاكمته في دولة أخرى.

وبالتالي فإذا كان الأصل أن عناصر الركن المادي للجريمة تكتملان في مكان واحد أو بالأحرى في نطاق إقليم واحد إستثناءا في الجرائم الإلكترونية والتي تسمى بالجرائم العابرة للحدود الإقليمية للدول والقارات.

يمكن أن يتوزع فيها السلوك المادي للجريمة في إقليم أكثر من دولة، فيقودنا التساؤل عن مكان وقوع الجريمة في هذه الحالة، فهل مكان وقوع السلوك الإجرامي ام المكان الذي تحققت فيه النتيجة.

وإذا كنا بصدد جريمة معلوماتية أو أمام جريمة نصب معلوماتية عبر الأنترنت عن طريق الإعلانات الكاذبة مثلا فهناك صعوبة قانونية كبيرة في تحديد المحكمة المختصة للنظر في القضية بسبب طابع شبكة الأنترنت العابرة للحدود، فقد يبث المتهم الإعلان الكاذب من بلد معين لإيهام الشخص المجني عليه من بلد أخر، فيقوم هذا الأخير بتسليم ماله إلى المتهم كما أنه قد يستخدم تقنيات التمويه مثل تقنية VPN التي تسمح بتمويل الدولة التي إرتكبت فيها الجريمة وبل حتى تغير هذه الأخيرة ال adresse ip الخاص بالحاسوب الذي إرتكبت منه الجريمة هو الأخر بالتالي يصبح الأمر أكثرا تعقيدا[1].

كما هو الحال في جرائم الصحافة المرتكبة في البيئة الرقمية، وهو محل تمركز الموقع الذي نشرت فيه الأقوال أو المعلومات بواسطته، وأيضا بالنسبة لبعض الجرائم الماسة بحقوق الملكية الفكرية كجرائم التقليدية والأنترنت، حيث يرجع الإختصاص إما لمحكمة المكان الذي أرتكبت فيه التقليد وإما لمكان نشره بالإضافة

[1]-حبيب بوسماط، مرجع سابق، ص77.

إلى هذه المعايير تم الإيجاد معايير أخرى مرتبطة أيضا بجرائم المرتكبة ضد الأحداث حيث ينعقد الإختصاص في النوع من الجرائم لمكان إرتكاب الجريمة، وقد يكون المكان الذي شوهد فيه الموقع غير مشروع.

الملاحظة من خلال مختلف هذه المعايير المستحدثة أنها تجاوزت المعايير التقليدية لانعقاد الإختصاص وجاءة بمفهوم جديد لمكان إرتكاب الجريمة الإلكترونية يتماشى وينسجم مع طبيعة هذه الجرائم، مما يستدعي البحث وإيجاد معايير تتماشى مع مختلف الجرائم إلكترونية الأخرى، فعلى سبيل المثال بالنسبة لمسألة تفتيش المعلومات والبيانات المعالجة إلكترونيا خارج إقليم الدولة أثار جدل بشأنها.

أ. فالرأي الأول: يرى أن من غير المشرع أن تقوم السلطات دولة ما بالتدخل وتفتيش النظم الإلكترونية الموجودة في لإقليم دولة أخرى، بهدف كشف وضبط أدلة للإثبات جريمة كانت قد وقعت على أراضيها وذلك إستنادا إلى مبدأ الإقليمية.

ب. أما الرأي الثاني: فيرى بأنه يمكن السماح بتنفيذ هذه الإجراءات حال توفر ظروف معينة يتم تحديدها كإشعار الدولة المراد تفتيش البيانات والمعلومات المخزنة بنظمها المعلوماتية وبالرجوع لمبدأ الإقليمية والمبادئ الأخرى المعمول بها لتحديد الإختصاص القضائي للجرائم التي ترتكب بواسطة شبكة المعلومات الدولية للأنترنت، نجد ان معظم التشريعات قامت بتطبيقها في مسألة الإختصاص الجزائي الدولي، إلا ان طريق تبني هذا الحل إختلفت من دولة إلى أخرى، فهناك من ساير موقف الفقه وهناك من ساير موقف القضاء، وهناك آخر اتبع الإتفاقيات الدولية.

ثانيا: موقف القضاء من مسألة الإختصاص: يقصد بمبدأ إقليمية القانون الجزائي لدولة ما يطبق على كل جريمة ترتكب على إقليم هذه الدولة سواء كان الجاني يحمل جنسية هذه الدولة أم يحمل جنسية دولة أجنبية وسواء كان المجني عليه مواطنا ام اجنبيا.

ويجب التذكير بأن المحكمة المختصة وكذا سلطة التحقيق المختصة وفقا لمبدأ الإقليمية الذي يسود معظم التشريعات المقارنة وهي محكمة المكان الذي وقعت فيه الجريمة أو جزء منها أي وقع فيه الركن المادي أو جزء منه وإذا طبقنا ذلك على جريمة النصب الإلكترونية نتذكر أن جريمة النصب من الجرائم المركبة، حيث يتشكل فيها الركن المادي من أولا: ممارسة أحد الطرق الإحتيالية، ثانيا: الإستلاء على مال الغير وثالثا: علاقة السببية، التي تتمثل في إقناع المتهم المجني عليه بتسليم ماله وحدوث هذا التسليم بناء على ذلك وبالتالي فعلى المحكمة المختصة بمحاكمة المتهم في جريمة النصب الإلكترونية هي تلك المحكمة التي تمارس في دائرتها المتهم نشاطه الإحتيالي وكذلك محكمة المكان الذي تم فيه تسليم المال وفي هذا الصدد إنقسم رأي الفقهاء إلى ثلاث إتجاهات لتحديد مكان وقوع الجريمة مذهب السلوك أو النشاط الإجرامي بوصفه معيار لتحديد مكان وقوع الجريمة[1].

[1]-حبيب بوسماط، مرجع سابق، ص77.

وفقا لهذا المعيار ينعقد الإختصاص القضائي للمحكمة التي يقع في نطاقها النشاط الإجرامي وليس مكان تحقق النتيجة أو الآثار المترتبة عليه، لأن هذا المعيار يسهل عملية الآثبات وجمع ادلة الجرمية وأن المحكمة التي لها ولاية النظر في القضية تكون قريبة من مسرح الجريمة: كما لأن تطبيق قانون الدولة التي تحقق فيها الضرر لا يتفق وإعتبارات العدالة لأن الجاني لا يكون على دراية بقانون تلك الدولة الذي يتم إعماله بحقه إلا أن هذا الرأي تعرض للنقد بصفة معيار مرن مذهب النتيجة الجرمية كمعيار لتحديد مكان وقوع الجريمة[1]:

على الرغم من الحجج التي جاء بها الإتجاه الأول إلا أنه تعرض لجملة من الإنتقادات من جانب أخر من الفقه وهي أن الإتجاه الأول لم يبدى إهتمام للمكان الذي تحقق فيه الضرر أو النتيجة الإجرامية، كما أن تمام الجريمة لا يكون إلا في المكان الذي ظهرت فيه آثارها الضارة التي كان الجاني يقصدها أو يرغب في تحقيق آثارها، بالإضافة إلى أن تقادم الجريمة يبدأ إحتسابه من الوقت الذي تحققت فيه نتيجة الجريمة، كما يؤخذ في الحسبان جسامة الضرر كأساس لتقدير التعويض وأن الضرر شرط أساسي لقيام المسؤولية المدنية فهذا الإتجاه يأخذ بمبدأ وحدة الجريمة بعد الفصل بين عناصرها، وكذلك يمتاز في نظر المدافعين عنه بأنه أكثر واقعية على إعتبار أن الضرر له مظهر خارجي ملموس على خلاف السلوك الإجرامي الذي قد لا يكون له كذلك، والذي قد يتخذ فعل إيجابي كما قد يكون عبارة عن إمتناع أي فعل سلبي، وقد تبنيه في بعض التشريعات المقارنة منها القانون الألماني.

ثالثا: المذهب المختلط: أمام الإنتقادات التي تعرض لها كلا الإتجاهين السابقين برز إتجاه الثالث يرى أن الجريمة تعد واقعة في مكان حصول النشاط الإجرامي (العمل التنفيذي) وكذلك المكان الذي تحققت فيه النتيجة الإجرامية او الذي من المتوقع أو من المنتظر تحقيقها فيه وهذا الإتجاه حضي بموافقة أغلب الفقه، ويعد مبرره في أن الركن المادي لجريمة يقوم على ثلاثة عناصر، وهي الفعل أي نشاط الإجرامي والنتيجة والعلاقة السببية، وما يعنب أن الجريمة وقعت في كل مكان تحقق فيه عنصر من عناصر الركن المادي للجريمة وهذا الإتجاه أخذت به بعض التشريعات المقارنة منها قانون العقوبات النرويجي وكذلك الدنماركي والصيني والإيطالي كما تبنته محاكم الدول، منها فرنسا في عدد من الأحكام إذا ذهبت إلى أن إختصاصاها يمتد ليشمل كل الأمكنة التي كانت مسرحا للجريمة وقت وقوعها.

وتجدر الإشارة إلى أنه بالرجوع إلى مبررات التي إستند إليها كل إتجاه فإن الإتجاه الثالث هو الأرجح لأنه تجاوز ما أخذ به كل من الإتجاهين الآخرين، كما انه وسع في نطاق الحماية الجزائية وفي تمديد الإختصاص القضائي وبالتالي يمكن إعتباره إتجاه شامل وجامع.

إلا ان مفهوم الإقليمية شهد تطورا ملحوظا فيما يتعلق بتحديد مكان وقوع الجريمة فلم يعد يلازم وقوع الفعل مادي أو حتى أحد العناصر المكونة لهذا الفعل، بل بلغ الأمر حد نزع الصفة المادية كلية عن هذا الفعل.

[1]-حبيب بوسماط، مرجع سابق، ص ص78-79.

وهكذا تعتبر مجرد مكالمة هاتفية مع شخص في دولة اخرى مبررا لاعتبار الجريمة وقعت فوق إقليم الدولة وبالتالي يجب صياغة معيار الإختصاص الإقليمي للجريمة الإلكترونية وفالمثل هذه المعطيات الجديدة: تطبيق المبادئ الأخرى على جريمة الإحتيال الإلكترونية[1]:

تجدر الإشارة إلى أن التقدم العلمي الرّاهن وتطور وسائل الإتصال الحديثة كالأنترنت وسائر صور الإتصلات الإلكترونية عبر الأقمار الصناعية، أتاح فرصا هائلة لخروج على مبدأ الإقليمية وتبني معايير جديدة، لفض مسألة تنازع الإختصاص القضائي لأن معيار الاقليمية لم يعد هو المعيار الوحيد ولا ربما الأكثر قبولا في بعض الجرائم، بل ازدادت أهمية معايير أخرى كانت فيما مضى تعد احتياطية كمعيار العينية ومعيار الشخصية ومعيار العالمية.

رابعا: مبدا العينية: يقصد بمبدأ الذاتية أو العينية بتطبيق القانون الجزائي على الجرائم التي تمس المصالح الأساسية للدولة، والمرتكبة خارج إقليمها أي كانت جنسية مرتكبها، وهذا المبدأ يرفضه حرص الدولة على حماية مصالحها الأساسية مثل إرتكاب جناية أو جنحة مخلة بأمن الدولة أو تقليد خاتم الدولة والجرائم التي تمس بالمصالح الأساسية للدولة.

خامسا: مبدأ الشخصية: يقصد بمبدأ الشخصية كملاحقة القانون الوطني للأشخاص الذي يحملون جنسية الدولة، أينما وجدوا ليحاكموعلى افعالهم الإجرامية المرتكبة في الخارج ويطبق مبدأ الشخصية بطريقتين إيجابية وسلبية ويقصد بالطريقة الإيجابية تطبيق القانون الجزائري على مرتكب الجريمة الذي يحمل جنسية الدولة ولو إرتكبت الجريمة خارج إقليمها، وهذا لتجنب فرار المجرم الذي يسيء لسمعة دولته، أما الطريقة السلبية فيقصد بها تطبيق القانون الجنائي على كل جريمة يكون مجني عليه حاملا لجنسية الدولة، ولو ارتكبت الجريمة خارج إقليمها وأيا كانت جنسية الجاني وهذا لضمان حماية رعايا الدولة من الإعتداءات الجرمية عليهم.

الفرع الثاني: موقف المشرع الجزائري من مسألة الإختصاص القضائي المحلي

حدد المشرع الجزائري معايير الإختصاص المحلي للجرائم الإلكترونية في قانون الإجراءات الجزائية في المواد37، 40، 329 ونجد أن المشرع الجزائري تخطى مشكلة إمتداد التفتيش خارج الإقليم الوطني بموجب ما رسمه القانون.

لكن مشكلة الإختصاص القضائي وملائمة القانون الواجب التطبيق تظل قائمة في مجال الجرائم الإلكترونية لأنه وإن بادر المشرع الجزائري بتعديل قانون الإجراءات الجزائية بموجب القانون 04-14 المؤرخ في 10-11-2004[2]، حيث عدل المادة 329 [3]من قانون الإجراءات الجزائية وذلك لجواز تمديد

1-حبيب بوسماط، مرجع سابق، ص ص 78-80.

2-القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004 المعدل للأمر 66-156 المتضمن قانون الاجراءات الجزائية، الجريدة الرسمية العدد 71.

3-المادة 329، الفقرة الخامسة.

الإختصاص المحلي للمحكمة، ليشمل إختصاص محاكم أخرى عن طريق تنظيم في الجرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة، وقد جاء عقب ذلك المرسوم التنفيذي رقم 06-348[1] المؤرخ في 5-10-2006 والمتضمن تمديد الإختصاص المحلي ببعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ليجسد فعلا بموجب المادة الأولى منه مجال إختصاص بعض المحاكم في إطار الجرائم الماسة بالأنظمة المعالجة الآلية للمعطيات...لأن مشكلة الإختصاص القضائي المحلي تضل قائمة إذا وقعت النتيجة الإجرامية في إقليم الدولة الأجنبية.

اولا: إختصاص وكيل الجمهورية:

نصت المادة 37 من قانون الإجراءات الجزائية على الإختصاص المحلي لوكيل الجمهورية بمكان وقوع الجريمة أو بمحل إقامة الأشخاص المشتبه في مساهمتهم في إقترافها أو بمحل القبض على احد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب آخر.

ومن المستجدات التي إستحدثها المشرع الجزائري في تعديل قانون الإجراءات الجزائية لسنة 2004-2006 وما يتعلق بتمديد الإختصاص، بحيث نصت المادة 37-2 يجوز تمديد الإختصاص المحلي لوكيل الجمهورية إلى دائرة إختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم المسماة بالمعالجة الآلية للبيانات والمعطيات وجرائم تبيض الأموال والإرهاب والجرائم الخاصة بتشريع الصرف.

ثانيا: إختصاص قاضي التحقيق:

بالنسبة لقاضي التحقيق نصت المادة 40-1 على ان إختصاصه المحلي يتحدد بمكان وقوع الجريمة أو محل إقامة المشتبه في مساهمتهم في إقترافها، او بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان القبض قد حصل لسبب آخر.

أما فيما يخص ضباط الشرطة القضائية طبقا للمادة 16-1 من قانون الإجراءات الجزائية فإنهم يمارسون الإختصاص المحلي في حدود الدائرة التي يباشرون فيها وظائفهم المعتادة وفي حالات الإستعجال لهم مباشرة مهامهم في كافة إختصاص المجلس القضائي الملحقين به، أو كافة الإقليم الوطني بناءا على أمر من القاضي المختص وبعد الإطلاع وكلاء الجمهورية التابعين له.

ثالثا: الإختصاص المحلي لجهات الحكم:

عدل المشرع الجزائري الإختصاص المحلي بالنسبة لجهات الحكم حيث نصت المادة 329 من قانون الإجراءات الجزائية المعدلة بموجب القانون رقم 04-14 السالفة الذكر، تختص محليا بالنظر في الجنحة[2]

---

[1]-المرسوم التنفيذي رقم 06-348 المؤرخ في 5-11-2006، الجريدة الرسمية رقم 63 المؤرخ في 8-11-2006.

[2]-حبيب السعيد، مرجع سابق، ص85.

محكمة محل إرتكاب الجريمة أو محل إقامة أحد المتهمين أو شركائهم، أو محل القبض عليهم ولو كان هذا القبض قد وقع لسبب آخر [1].

إن القواعد العامة تقتضي الإختصاص الإقليمي حسب ما حددته المادة 37 مكرر قانون الإجراءات الجزائية السالفة الذكر، ونظرا لخصوصية جريمة النصب الإلكتروني خرج المشرع بتمديد الإختصاص فيها على إعتبارها من الجرائم الإلكترونية إذ يصبح إختصاص وطني حسب المادة 16 الفقرة السابعة قانون الإجراءات الجزائية، ونظرا لكونها تحتاج إلى قضاة متخصصين ولهم دراية بالمعلوماتية، وبغية الوصل إلى الحقيقة وتحقيق العدالة، قام المشرع بإنشاء القطب الجزائي بموجب الأمر 21-11[2]، طبقا لنصوص المواد من 211 مكرر 22 إلى 211 مكرر 29 قانون الإجراءات الجزائية.

لكن الإختصاص لا يثير أي إشكال عندما يتعلق بالجرائم الإلكترونية المرتكبة داخل الإقليم الجزائري، وإنما الأشكال يمكن في الجريمة الإلكترونية التي تمتد مجريات التحقيق والتحري فيها خارج الإقليم الجزائري، إذ ان الوضع كهذا بصدد عولمة الجريمة.

وقد حاول المشرع الجزائري إيجاد حل لهذه النقطة، إذ نص في المادة 15 من قانون 09-04[3]على انه: وفضلا عن الإختصاص المنصوص عليه في قانون إجراءات الجزائية، تخص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها اجانب وتستهدف مؤسسات الدولة الإستراتيجية الإقتصاد الوطني أو الدفاع الوطني أو المصالح العامة للدولة.

المطلب الثاني: الإجراءات التقليدية والإجراءات المستحدثة في متابعة جريمة النصب الإلكتروني

طلب التحقيق في الجرائم اتباع إجراءات معينة للكشف عن الحقيقة، وجريمة النصب الالكتروني هي جريمة ذكية تتطلب إجراءات تقليدية وإجراءات مستحدثة تفرضها المستجدات المرتبطة بالتكنولوجيا والتطور العلمي

الفرع الأول: الإجراءات التقليدية للمتابعة في جريمة النصب الإلكتروني

تتمثل هذه الإجراءات في المعاينة والتنفتيش والضبط والشهادة، الخبرة، إستجواب المتهم، إلا اننا سنتطرق لشرح المعاينة والتفتيش والضبط كمثال.

أولا: المعاينة : هي رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة.

وتعتبر المعاينة إجراء من إجراءات التحقيق التي تقوم بها سلطة التحقيق بنفسها أو تندب ضباط الشرطة للقيام بها، كما يمكن للمحكمة ان تقوم بإجراءات معاينة إذا رأت ذلك يستدعي لكشف الحقيقة سواء كان ذلك من تلقاء نفسها أو بناءا على طلب من الشخص المعني بعد موافقة القاضي المختص بناءا على طلب عريضة.

---

[1]-حدي نسيمة، مرجع سابق، ص45.

[2]-الأمر 21-11 المؤرخ في 25 أوت 2021 يتمم الأمر رقم 66-155 المؤرخ في 8 يونيو 1966 والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية العدد 65.

[3]-القانون رقم 09-04 المؤرخ في 5-8-2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والإتصال، الجريدة الرسمية رقم 47 المؤرخة في 16-8-2009.

أ. كيفية إجراء المعاينة التقنية لمسرح الجريمة الإلكترونية

عند العلم بوقوع الجريمة فإن أول خطوة يقوم بها مأمور الضبط القضائي هو الإنتقال إلى مسرح الجريمة، لأن هذا الأخير حجز الزاوية في التحقيق الجنائي وممكن الآثار والأدلة المادية، وينبغي التعامل في الإطار مع مسرح الجريمة المعلوماتية على أنه مسرحان هما [1]:

1. المسرح التقليدي:

يقع خارج البيئة الإلكترونية لأنه يتكون من المكونات المادية للمكان الذي وقعت فيه الجريمة، وهو أقرب إلى مسرح الجريمة التقليدية ويترك فيها الجاني عدة آثار كالبصمات وبعض متعلقاته الشخصية أو وسائط تخزين رقمية.

2. المسرح إفتراضي:

يقع داخل البيئة الإلكترونية، لانه يتكون من البيانات الرقمية التي تتواجد داخل الحاسوب وشبكة الأنترنت في ذاكرة الأقراص الصلبة الموجودة بداخله.

ونظرا لاختلاف مسرح الجريمة عن غيره من الجرائم الأخرى فينبغي التعامل الخاص مع هذه الجريمة وذلك بإتباع قواعد فنية قبل الإنتقال إلى مسرح الجريمة الإلكترونية والمتمثل في:

- ضرورة وجود معلومات مسبقة عن مكان الجريمة من حيث عدد الأجهزة المطلوب معاينتها وشبكاتها
- وجود خريطة توضح الموقع الذي سيتم معاينته وتفاصيل المبنى أو الطابق موضوع البلاغ، وعدد الأجهزة والخزائن والملفات ويحدد ذلك من خلال مصادر سرية لجهات الأمن.
- تحديد الأجهزة المحتمل تورطها في الجريمة الإلكترونية حتى يتم تحديد كيفية التعاون معها فنيا قبل المعاينة.
- تأمين الأجهزة والمعدات التي سيتم الإستعانة بها في عملية المعاينة سواء كانت أجهزة أو برامج.
- إعداد الفريق المتخصص الذي يتولى المعاينة من الخبراء ورجال الضبط والأمن.
- تحديد البيانات والمهام والإختصاصات المطلوبة من كل عضو في فريق المعاينة على حده، وذلك حتى لا تتداخل الإختصاصات.
- إعداد خطة المعاينة موضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها على الوجه الأكمل.
- أن تتم هذه المعاينة وفق مبدأ المشروعية وفي إطار ما تنص عليه القوانين الجنائية.
- تأمين عدم إنقطاع التيار الكهربائي لان معاينة الأجهزة وما بها من برامج وشبكات وأنظمة تشغيل لا جدولا منها في ظل عدم وجود التيار الكهربائي.

---

[1]-عائشة بن قارة مصطفلى، **حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائن الجزائري والمقارن**، دار الجامعة الجديدة، كلية الحقوق جامعة الإسكندرية، ص ص 84، 86.

ولمعاينة مسرح الجرائم الإلكترونية، يجب التفرقة بين حالتين[1]:

ب. معاينة الجرائم الواقعة على المكونات المادية للحاسوب (Hardware):

كشاشة العرض ومفاتيح التشغيل والأقراص وغيرها من مكونات الحاسوب ذات الطابع المادي المحسوس، فهي لا تثير أية مشكلة بحيث يمكن لضابط الشرطة القضائية معاينتها والتحفظ على الأشياءالتي تعد ادلة مادية للكشف عن الجريمة.

ت.معاينة الجرائم الواقعة على المكونات غير المادية أو بواسطتها (Software):

كتلك الواقعة على برامج الحاسوب وبياناته، هذه المكونات تثير صعوبات عديدة تحول دون فاعلية المعاينة أو فائدته، وهذه الصعوبات، تتخلص فيما يلي:

ـقلة الآثار المادية المترتبة عن الجرائم التي تقع على المكونات غير المادية للحاسوب.

ـالأعداد الكبيرة من الأشخاص الذين يترددون على مسرح الجريمة خلال المدة الزمنية التي غالبا ما تكون طويلة، وذلك بين إقتراف الجريمة والكشف عنها، الأمر الذي يمنح فرصة لإحداث تغييرات او العبث بالآثار المادية أو زوال بعضها، مما يؤدي إلى غموض الدليل المشتق من المعاينة.

ولنجاح المعاينة في الجرائم الإلكترونية يوصي الخبراء بوجوب إتباع ومراعاة قواعد وإرشادات فنية أبرزها ما يلي:

1. القيام بتصوير الحاسوب وما قد يتصل به من أجهزة ظرفية ومحتوياته، وأوضاع المكان الذي يوجد به بصفة عامة مع التركيز على تصوير أجزائه الخلفية وملحقاته، ومراعاة تسجيل الزمان والتاريخ والمكان الذي إلتقطت فيه كل صورة.

2. يجب ملاحظة وإثبات الحالة التي تكون عليها توصيلات الكابلات (الخيوط الكهربائية للحاسوب)، والتي تكون متصلة بمكونات النظام، حتى يسهل القيام بعملية مقارنة وتحليل لها عند عرض الموضوع على المحكمة.

3. عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة، وذلك قبل إجراء الإختبارات الازمة للتأكد من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي حتى لا يحدث أي إتلاف للبيانات المخزنة ومحو للبيانات المسجلة.

4. وضع مخطط تفصيلي للمنشآة الواقعة بها الجريمة مع كشف تفصيلي بالمسؤولين بها ودور كل واحد منهم.

5. ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يتمكن من إجراء عملية المقارنة والتحليل عند عرض الأمر فيما يعد على القضاء.

---

[1]-حشمان عمار، **الجريمة المعلوماتية في التشريع الجزائري**، مذكرة ماستر، تخصص إدارة التحقيقات الاقتصادية والمالية، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة قاصدي مرلاح –ورقلة-، 2018-2019، ص47.

6. التحفظ على ما تحتويه سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة، والأشرطة والأقراص الممغنطة غير السليمة أو المحملة وفحصها، ورفع البصمات التي قد تكون لها صلة بمرتكبي الجريمة.

ثانيا: التفتيش

أ. تعريف التفتيش:

إن التفتيش المنصب على منظومة المعلومات يختلف عن التفتيش المتعارف عليه، في القواعد الإجرائية العامة من حيث الشروط الشكلية والوضعية وموضوع التفتيش.

على رغم من أن المشرع الجزائري اعتبر التفتيش إجراء من الإجراءات التحقيق وإحاطته بقواعد صارمة إلا أنه لم يورد تعريفا خاصا ودقيقا وقد إهتم الدستور الجزائري بعدم مساس بحرية الأشخاص وكرامتهم وأكد ذلك في المادة 40 منه بالقول: "فلا تفتيش إلا بمقتضى القانون وفي إطار إحترامه، ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة".

وفي الأخير ان التشريعات العربية تتفق على تعريف التفتيش بانه "إجراء من إجراءات التحقيق غايته ضبط أدلة الجريمة موضوع التحقيق وكل ما يفيد الحقيقة في شأنها"[1].

إن الهدف من التفتيش هو ضبط الأدلة المادية للكشف عن الجريمة، فكل ما يضبطه ضابط الشرطة القضائية بعد عملية التفتيش من أشياء متعلقة بالجريمة هو الأثر المباشر للتفتيش، فالضبط إذن يعد أيضا إجراء من إجراءات التحقيق في الجرائم الإلكترونية، بوضع اليد على الشيء، وحبسه والمحافظة عليه، للحصول على دليل لمصلحة التحقيق عن طريق إثبات واقعة معينة، وهو ماسنبرزه فيما يلي[2]:

ب. تفتيش نظم المعلوماتية:

عملية تفتيش تنصب على المكونات المادية بأوعيتها المختلفة، للبحث في أي شيئ يتصل بجريمة معلوماتية ما للكشف عنها، يدخل في نطاق التفتيش التقليدي وفقا للإجراءات القانونية المعمول بها، إلا أن هناك حالات خاصة للتفتيش في هذه المكونات، هي:

1. الحالة الأولى:

في حالة ما إذا كانت هذه المكونات موجودة في مكان خاص كمسكن المهتم أو أحد ملحقاته، فإنها تأخذ نفس الأحكام المقررة لتفتيش المسكن وبنفس الضمانات المقررة قانونا في مختلف التشريعات.

2. الحالة الثانية:

إذ كانت مكونات الحاسوب المادية منعزلة عن غيرها من اجهزة الكمبيوتر أم أنها متصلة بجهاز أو نهاية طرفية في مكان آخر كمسكن غير مسكن المتهم، بحيث إذا كانت هناك بيانات مخزنة في أوعية هذا النظام

---

[1]-زيبحة زيدان، **الجريمة المعلوماتية في التشريع الجزائري والدولي**، دار الهدى، عين ميلة، الجزائر، 2011، ص ص 130-131.

[2]-عمار حشمان، مرجع سابق، ص49.

الأخر، فإن عملية الكشف تصبح صعبة جدا، وربما مستحيلة، لذلك حتى تتم عملية تفتيش هذه الأجهزة المرتبطة بأجهزة في أماكن أخرى، يتعين مراعاة القيود والضمانات التي يوجبها المشرع لتفتيش هذه الأماكن.

وقد حذا المشرع الجزائري حذو معظم التشريعات المعاصرة، بأن قرر المادة 65[1] مكرر 5 وما يليها من قانون الإجراءات الجزائية التي تسمح إذا إقتضت ضرورة التحري أو التحقيق في الجرائم الماسة بانظمة المعالجة الآلية للمعطيات بإعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور.

3. الحالة الثالثة:

إذا وجدت مكونات الحاسوب المادية (في حالة الحاسوب الآلية المحمولة) في الأمكان العامة بطبيعتها كالمطاعم والسيارات العامة كسيارات الأجرة...إلخ، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص، وبنفس الضمانات والقيود المنصوص عليها في هذه الحلات.

ت. تفتيش نظم الحاسوب المنطقية أو المعنوية:

يعرف الكيان المنطقي للحاسوب بأنه: "مجموعة البرامج والأساليب والقواعد وعند الإقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات"

وقد حذا المشرع الجزائري في المادة 47 الفقرة الرابعة من قانون الإجراءات الجزائية الجزائري حذو التشريعات السابقة بإمكانية التفتيش والضبط على المكونات المعنوية للحاسوب، بنصه على أنه: "إذا تعلق الأمر بجريمة ماسة بأنظمة المعالجة الآلية للمعطيات يمكن لقاضي التحقيق أن يقوم بأية عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على إمتداد التراب الوطني أو يأمر ضباط الشرطة القضائية للقيام بذلك".

ث. القواعد الشكلية لتفتيش نظم المعلوماتية:

تتلخص هذه القواعد كما يلي[2]:

1. إجراء التفتيش بحضور أشخاص معينين بالقانون:

من بين هذه الأشخاص: المتهم والقائم بالتفتيش وشاهدين طبقا للمادة 45 من قانون الإجراءات الجزائية الجزائري، تنص على أن: التفتيش يتم بحضور المتهم أو من يجوز أن يمثله وضابط الشرطة القضائية –القائم بالتفتيش-، وإذا تعذر حضور المتهم أو من يجوز أن يمثله يتم التفتيش بحضور شاهدين من غير الموظفين الخاضعين لسلطته، غير أنه كاستثناء على هذه القواعد نص المشرع الجزائري في الفقرة من المادة 45 من قانون الإجراءات الجزائية الجزائري، على أنه: "لا تطبق هذه الأحكام إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات".

---

[1]-المادة 65 مكرر 5 من قانون الإجراءات الجزائية.

[2]-عمار حشمان، مرجع سابق، ص ص50-51.

2. إعداد محضر خاص بالتفتيش:

ويكون بتكليف القائم بالتفتيش باصطحاب كاتب يحرر محضرا خاصا بالتفتيش والظّبط، تسجل فيه جميع وقائع التحقيق بالتفصيل، وذكر البيانات والأشياء والوثائق التي يتم ضبطها بكل أمانة ودقة وحرص.

3. إجراء تنفيذ تفتيش نظم الحاسوب الآلي ومعداته:

لهذه الإجراءات خصوصية تتميز بها، وذلك لطريقة التعامل مع الأجهزة والبرامج الموجودة عليها، ولكي تتم على أكمل وجه، يجب تحديد نوع النظام المراد تفتيشه، وبالتالي يجب أن يكون القائم بالتفتيش على علم بقدر كبير بعلوم الإعلام الآلي حتى يتسنى له معرفة نظم الحاسوب المراد تفتيشها، والإستعانة بخبراء النظام للإستعانة بهم في عملية إجراء التفتيش، ومعرفة إمكانية الحصول على كلمة السر والدخول للنظام المراد تفتيشه، ومعرفة مكان القيام بتحليل نظم الحاسوب الآلي.

بالإضافة إلى تحديد هوية أعضاء فريق التفتيش يجب على القائم بالتفتيش إتخاذ الخطوات التالية عند تنفيذ إذن التفتيش والتي تتلخص في ما يلي[1]:

- تأمين حماية مسرح الجريمة، بضمان فصل القوة الكهربائية عن موقع المعاينة وأجهزة خادمة شبكة الأنترنت، لشل فاعلية الجاني في القيام بأي فعل من شأنه التأثير على لآثار الجريمة.
- إبعاد المتهم عن مكان النظام إن كان قريبا منه.
- أخذ الحيطة لمنع تمكن المتهم من الدخول عن بعد للنظام المعلوماتي.
- الدخول إلى الموقع ببطء، لكي لا يتم تشويه أو إتلاف الدليل.
- عدم لمس لوحة المفاتيح، لأن ذلك قد يستلزم إستخدام برامج اخرى إحتيالية أو صعبة.
- يجب العناية بالملاحظات وكلمات السر ورموز الشفرة إلى غيرها من العمليات والإجراءات الفنية التي تساعد على الكشف عن الجريمة المراد إثباتها.

وفي نطاق تفتيش نظم الحاسوب، نجد ان المشرع الجزائري لم تحدد مدته لتنفيذ إجراء التفتيش، غير أن الرأي الغالب في مجال تفتيش النظم المعلوماتية هو عدم تقييد المحقق بمدة زمنية معينة، بل يجب تركها للسلطة التقديرية له، لأن الوقت الذي تكثر فيه الجرائم الإلكترونية هو ليلا، لسهولة الإتصال ومجانيته في ذلك الوقت في بعض الحالات، وأيضا لسهولة الدخول إلى المواقع المستهدفة بالفعل الإجرامي لقلة المستخدمين في هذا الوقت، كما نص عليها في الفقرة الثالثة من المادة 47 من قانون الإجراءات الجزائية الجزائري.

ثالثا: الضبط

يختلف الضبط في الجريمة الإلكترونية عن الضبط في غير ذلك من الجرائم من حيث المحل، وذلك بسبب أن الأول يرد على أشياء ذات طبيعة معنوية وهي البيانات، المراسلات والاتصالات الإلكترونية، أما الثاني فيرد على أشياء مادية منقولة كانت أم عقارات، وقد أثارت هذه الطبيعة المعنوية للبيانات جدلا فقهيا

[1]-عمار حشمان، مرجع سابق، ص ص 51، 53.

وإختلافا تشريعيا حول مدى إمكانية ضبطها خاصة إذا كانت مجردة من الدعامة المادية المثبتة عليها، ويرجع السبب في ذلك أن الضبط –حسب الأصل- لايرد إلاّ على الاشياء المادية[1].

إلا أن المضبوطات في الجرائم الإلكترونية ومنها النصب الإلكتروني قد تأخذ الصورة المادية في تلك الحالة التي يتعلق الأمر بعناصر مادية ومن قبل ذلك جهاز الحاسب الآلي وملحقاته، أو الأقراص الصلبة أو الأشرطة الممغنطة، أو الطابعة أو بطاقات الإئتمان أو المعدات المستعملة في شبكة الأنترنيت مثل: المودم، كما قد تأخذ المضبوطات الصورة غير المادية أي المعنوية مثل البرامج والبيانات المعالجة آليا، والمراسلات الإلكترونية، والدليل الموجود على مستوى الدليل الإلكتروني وبذلك إذ أسفر التحقيق على وجود دليل رقمي ثم ضبطه فإن الإجراءات المتخذ بعدها، هو الحجز كما عبر عنه المشرع الجزائري بموجب المادة 06 من قانون المتعلق بالقواعد الخاصة للرقابة من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتهارقم 09-04 المؤرخ في 9 اوت 2009 والتي تنص على أنه" تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية"[2].

الفرع الثاني: الإجراءات المستحدثة في جريمة النصب الإكتروني

سنتطرق في هذه المجموعة إلى الإجراءات المستحدثة في كشف أساليب النصب الإلكتروني كجريمة من الجرائم الإلكترونية ويوجد هناك الكثير من أنواع هذه الإجراءات مثل ترصد الإلكتروني، إعتراض المراسلات، تسجيل الأصوات والتسرب، والتي تعتبر من الحقوق التي كفلها الدستور الجزائري وتعتبر إجراءات خطيرة تمس بالحياة الخاصة للأفراد لذلك كانت منظمة تنظيما قانونيا ومتاحا في جرائم محددة على سبيل الحصر منها: الجرائم المرتكبة على الأموال ونذكر من بين هذه الإجراءات على سبيل المثال:

التسرب: جاءت المادة 65 مكرر 12 قانون الإجراءات الجزائية تعرف التسرب بأنه "يقصد بالتسرب ضابط أعوان الشرطة القضائية المكلف بتنسيق العلمية، بمراقبة الأشخاص المشتبه في إرتكابهم جناية أو جنحة بإهتمام أنه فاعل معهم أو شريك لهم خاف.

يسمح لضابط الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة وإن يرتكب عند الضرورة الأفعال المذكورة في المادة 65 مكرر 14 أدناه ولا يجوز تحت طائلة البطلان أن تشكل هذه الأفعال تحريض على إرتكاب الجرائم.

أما بالنسبة لمواصفات الاذن بالتسرب وطبيعته حددتها المادة 65 مكرر 15 من قانون الإجراءات الجزائية وهي[3]:

---

[1]-عائشة بن قارة مصطفلى، مرجع سابق، ص114.

[2]-مجدوب نوال، **الاليات الإجرائية للكشف عن الجريمة المعلوماتية**، مجلة البحوث القانونية والإقتصادية، المجلد 06، العدد 03، المركز الجامعي مغنية، الجزائر، 2023، ص198.

[3]-بن زرت اسيا، **إثبات الجريمة المعلوماتية في التشريع الجزائري**، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، الجزائر، 2018-2019، ص 25.

1. أن يسلم فقط لضرورة التحري أو التحقيق القضائي.

2. أن يكون مكتوبا.

3. أن يكون مسببا.

4. أن يذكر في الإذن طبيعة الجريمة التي ينص عليها الإذن.

5. يذكر فيه هوية ضابط الشرطة القضائية المعني أو الذي تتم العملية تحت مسؤوليته.

6. يحدد فيه المدة المقرر للعملية والمحددة بأربعة (4 اشهر) وهي قابلة للتجديد لمدة 4 أشهر أخرى كل ما دعت الضرورة لذلك.

7. أن تودع الرخصة أي الإذن في ملف الإجراءات بعد الإنتهاء من عملية التسرب.

وملاحظة على ذلك أنه إذا أغفل شرط من هذه الشروط يؤدي إلى بطلان الإذن .

خرج المشرع الجزائري عن الأصل العام في التحقيق القائم بالفصل بين سلطتي الإتهام والتحقيق وأوكل لوكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية مهمة إصدار الإذن بالتسرب[1].

الفرع الثالث: صعوبات الإثبات في جريمة النصب الإلكتروني

إذا كان الإثبات هو إقامة الدليل على وقوع الجريمة ونسبتها إلى فاعلها وفق طرق مشروعة ومحددة قانونا، فإن هذه الطرق التي عرفتها الجرائم التقليدية لن تكون مجدية على الوجه التام في الجرائم الإلكترونية وذلك للصعوبات العديدة التي تفرضها الخصوصيات المتعلقة بطبيعة الجريمة الالكترونية باعتبارها غير ملموسة وسهل محو آثارها ويصعب الوصول إلى فاعلها، الذي يتحلى بالذكاء والدراية الفنية الفائقة بعالم الكمبيوتر، بالإضافة إلى التعقيدات الموجودة في أجهزة الحواسيب والهواتف الذكية، ومنها تثار إشكالية الإثبات في الجرائم الالكترونية بوجه عام، ومنها جريمة النصب الإلكتروني التي نحن بصدد دراستها، حيث نذكربعض الصعوبات كالآتي:

أولا: الصعوبات المتعلقة بالدليل الرقمي

أ. تعريف الدليل الرقمي على أنه:

يعرف الدليل الرقمي على أنه: " الدليل الذي يجد أساسا له في العالم الافتراضي ويقود إلى الجريمة فهو كل بيانات يمكن إعدادها أو تخزينها بشكل رقمي بحت تمكن الحاسوب من إنجاز مهمة ما " وعرف أنه ذلك الدليل المشتق من أو بواسطة النظم البرامجية المعلوماتية الحاسوبية، وأجهزة ومعدات وأدوات الحاسب الألي أو شبكات الإتصال من خلال إجراءات قانونية وفنية، لتقديمها للقضاء بعد تحليلها علميا أو تفسيرها في شكل نصوص مكتوبة او رسومات أو صور واشكال واصوات لإثبات وقوع الجريمة لتقرير البراءة أو الإدانة فيها[2].

---

[1]-بن زرت اسيا، مرجع سابق، ص26.

[2]-عائشة بن قارة مصطفلى، مرجع نفسه، ص ص53-54.

ب.خصائص الدليل الرقمي

يمتاز الدليل الرقمي عن غيره من الأدلة الجنائية بعدد من الخصائص[1]:

1. تتكون الأدلة الرقمية من بيانات ومعلومات إلكترونية غير مرئية وغير ملموسة، بحيث يتطلب لإدراكها استخدام أجهزة ومعدات الحاسب الآلي Hardware واستعمال نظم برمجيات الحاسوب Software.

2. يعد الدليل الرقمي علمي، بحيث يتطلب منه توافر مجال تقني للتعامل معه، لذلك فكل ما ينطبق على الدليل العلمي ينطبق على الدليل الرقمي، بالتالي فالدليل العلمي يخضع لقاعدة ضرورة تعبيره عن الحقيقة، وهذا ما تضمنته قاعدة في القضاء المقارن التي تنص على ما يلي: "إن القانون مسعاه العدالة أم العلم فمسعاه الحقيقة".

3. يعد الدليل الرقمي من طبيعة تقنية وهذا ما يميزه عن الدليل التقليدي، من حيث أن التقنية لا تنتج سكينا يتم من خلاله معرفة القاتل أو اعترافا مكتوبا أو مالا قدم كرشوة أو بصمة بل تنتج التقنية نبضات رقمية تكمن قيمتها في إمكانية التعامل مع القطع الصلبة التي يتكون منها الحاسب الآلي مهما كان نوعه، وهذا ما حذا به المشرع البلجيكي بمقتضى القانون الصادر في 28 نوفمبر 2000 م، بتعديل قانون التحقيق الجنائي من خلال إضافة المادة (39) التي أجازت ضبط الأدلة الرقمية مثل: نسخ المواد المخزنة في نظم المعالجة الآلية للبيانات بقصد عرضها على الجهات القضائية، وعليه ما يميز الدليل الرقمي على أنواع الأدلة الأخرى أنه يمكن أن يستخرج نسخ من الدليل الرقمي مماثلة ومطابقة الأصل ولها نفس القيمة العلمية والثبوتية، وهذا ما يكفل وجود ضمانة قوية وفعّالة للحفاظ على الدليل ضد الفقدان والتلف ولتغيير من خلال وضع نسخ طبق الأصل من الدليل.

4. صعوبة التخلص من الدليل الرقمي، وتعتبر هذه الخاصية من أهم مميزات الدليل الرقمي باعتبارها ميزة يتمتع بها الدليل الرقمي عن غيره من الأدلة، وهذا ما يستوجب مقارنة الأدلة الرقمية بالأدلة التقليدية، حيث أن هذه الأخيرة تستمد قوتها في حالة التسريع بالحصول عليها فتكون قابلة للشك، كما أن في الشهادة يجب التعرف على مدى قدرة الشهاد على التذكر حيث أن قبول شهادة تعتمد على مستوى الرجل العادي في التذكر الذي يعترف به القانون وهذا من ناحية، أما من ناحية أخرى فالأدلة المادية يمكن التخلص منها عن طريق مسح بصمة الأصبع من مكانها، كما أن في بعض الدول يتم التخلص من الشهود عن طريق القتل أو التهديد به، وكذلك يمكن التخلص من الأوراق والأشرطة المسجلة إذا كانت تحتوي على ارتكاب أشخاص لجرائم، وذلك عن طريق حرقها أو تمزيقها، وعليه فإن عملية التخلص من هذه الأدلة سهل جدا ومن مستحيل استرجاع الدليل المستمد إذا ما تم تدميره كلية، أما الحال بالنسبة للأدلة الرقمية فهو ليس كذلك لأن موضوع التخلص من الدليل الرقمي باستعمال أو الاستعانة بخصائص التخلص من المستندات في الحاسب الآلي والشبكة الإلكترونية لا تعتبر من العوائق التي تحيل دون استرداد الملفات، حيث أنه تتوافر برمجيات من

[1]-حبيب بوسماط، مرجع سابق، ص ص 85-86. ص131-132

ذات الطبيعة الرقمية يمكن من خلالها استرجاع كامل الملفات التي تم من قبل إلغاؤها أو محوها من الحاسب الآلي أو إظهارها، وهذا ما يعني صعوبة إخفاء الجاني لجريمته.

5. إمكانية توظيف نشاط الجاني لمحو أو إزالة الدليل من الحاسب الآلي كدليل إدانة ضده، لأن فعل الجاني بمحو الدليل يتم تسجيله في الحاسوب، والذي يمكن الحصول عليه لاحقا كدليل للإدانة.

6. تمتاز بعض الأدلة الرقمية بسعة تخزينية عالية، بحيث يمكن لقرص صغيرة تخزين مكتبة كاملة كما يمكن لآلة فيديو رقمية تخزين مئات الصور.

7. يمكن الدليل الرقمي من تسجيل المعلومات عن الجاني ورصدها وتحليلها في الوقت نفسه، لأن الدليل الرقمي يمكن أن يقوم بتسجيل تحركات الأفراد وسلوكاتهم وعاداتهم وبعض الأمور الخاصة بهم لذلك فالبحث الجنائي عن الدليل الرقمي يكون بسهولة مقارنة مع الدليل المادي[1].

8. الدليل الرقمي هو مفهوم يحتوي التطور والتنوع، ذلك لأن هذا المصطلح يتضمن كافة أشكال وأنواع البيانات الرقمية التي يمكن تداولها رقميا، بحيث يكون بين هذه البيانات والجريمة رابطة أو علاقة من نوع ما تلك التي تتصل بالضحية أو المجني عليه على النحو الذي يحقق هذه الرابطة[2].

ثانيا: صعوبات التحري في كشف غموض الجريمة

إن التحري في كشف غموض الجريمة الإلكترونية تعترضه عدة عقبات، وتتمثل في ما يلي[3]:

أ. الكم الهائل للبيانات:

يشكل الكم الهائل للبيانات التي يتم تداولها من خلال الأنظمة المعلوماتية أحد مصادر الصعوبات التي تعوق تحقيق الجرائم التي تقع عليها أو بواسطتها والدليل على ذلك أن طباعة كل ما يوجد على الدعامات الممغنطة لمركز حاسب متوسط الأهمية يتطلب مئات الآلاف من الصفحات والتي قد لا تثبت كلها تقريبا شيئا على الإطلاق.

ب.مميزات الجرائم الإلكترونية:

ان الجرائم الإلكترونية تتميز بحداثة أساليب إرتكابها وسرعة تنفيذها وسهولة إخفائها ودقة وسرعة محو آثارها وهي تعتمد في الأساس على الخداع في إرتكابها ولتضليل في التعرف على مرتكبيها، وتحتاج لخبرة فنية يصعب على الخبير التقليدي التعامل معها.

ومن تم يقتضي أن تكون جهات التحري والتحقيق بل والمحاكمة على درجة كبيرة من المعرفة بأنظمة الحاسبة الإلكترونية وطريقة تشغيلها وأساليب إرتكاب الجرائم عليها أو بواسطتها مع القدرة على كشف غموض هذه الجرائم وسرعة التصرف بشأنها من حيث كشفها وضبط الأدوات التي استخدمت في ارتكابها،

---

[1]-زيان سعيد، سالمي هيشام، مرجع سابق، ص87.

[2]-حبيب بوسماط، مرجع سابق، ص134.87.

[3]-الطيبي البركه، حاج سودي محمد، **إشكالية الإثبات في الجرائم الإلكترونية**، مجلة آفاق علمية، المجلد 11، العدد 01، جامعة أدرار، 2019، ص276.

لذلك فقد وجدت صعوبات جمة في كشف غموضها وإجراء التفتيش والضبط اللازمين أو التحقيق فيها على نحو استدعى إعداد برامج تدريب وتأهيل لهذه الموارد من الناحية الفنية على نحو تمكينها من تحقيق المهمة المطلوبة وبكفاءة عالية.

ففي الفترة الأولى لظهور هذا النوع من الجرائم وقعت الشرطة في أخطاء جسيمة أدت إلى الضرار بالأجهزة أو الملفات أو الأدلة الرقمية الخاصة بإثبات الجريمة، ونعطي مثالا لهذا الخطأ من عمل الشرطة بالولايات المتحدة الأمريكية فقد حدث أن طلبت إحدى دوائر الشرطة بالولايات المتحدة الأمريكية من شركة تعرضت للقرصنة أن تتوقف عن تشغيل جهازها الآلي للتمكن من وضعه تحت المراقبة بهدف كشف مرتكب الجريمة وقد حدث نتيجة ذلك أن تسببت دائرة الشرطة بدون قصد في إتلاف ما كان قد سلم من الملفات والبرامج.

ت. أساليب التحري التقليدية

أن أساليب التحري أو التحقيق التقليدية لا تصلح لكشف غموض هذه الجرائم وضبط مرتكبيها والتحفظ على أدلتها، لذلك عمدت العديد من التشريعات إلى وضع أساليب أخرى للتحري عن هذه الجرائم، ومن بينها المشرع الجزائري الذي قام بوضع أساليب تتوافق مع الطبيعة التقنية للتحري عن هذه الجرائم بموجب القانون 09-04 المؤرخ في 2009/08/05، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وأهمها المراقبة الإلكترونية والتي تحوي أسلوبي الوقاية والمكافحة وإجراءات التفتيش في النظم المعلوماتية وحجز الأدلة الرقمية (حجز المعطيات) وحفظ معطيات السير من طرف مقدمي الخدمات.

ويبدو أن المشرع الجزائري وبغية تسهيل عمل المحققين في وضع الترتيبات التقنية المشار لها تجاوز كل الحدود ولم يراع حرمة الحياة الخاصة، وقد يكون الدافع إلى ذلك هو طابع الخطورة التي تكتسيه الجريمة إذ أنه ومع سرية المراسلات مضمونة دستوريا وفي المواثيق الدولية كما ورد في المادة 12 من الإعلان العالمي لحقوق الإنسان28، وهذه الضمانة الدستورية نص عليها المشرع الجزائري في الفقرة الأولى من[1] المادة 46 من الدستور الحالي، المعدل بموجب القانون رقم 16-01 مؤرخ في 26 جمادى الأولى عام 1437 الموافق 6 مارس 2016، المتضمن التعديل الدستوري.

كما يمكن للمجني عليه في هذه الجرائم أن يقدم خدمات كبيرة لرجال الشرطة أو لسلطة التحقيق بتقديمه معلومات تحقق فائدة كبيرة في معرفة طبيعة الجريمة التي وقعت وأساليب ارتكابها والأدوات المستخدمة في ارتكابها والأشخاص المشتبه فيهم وبواعث الجريمة وما إذا كان هناك شهود أم لا.

إضافة إلى أن إثبات الجرائم التي تقع على العمليات الإلكترونية باستخدام الوسائل الإلكترونية سيتأثر بطبيعة هذه الجرائم و بالوسائل العلمية التي قد ترتكب بها، مما قد يؤدي إلى عدم إكتشاف العديد من الجرائم

[1]-الطيبي البركه، حاج سودي محمد، مرجع سابق، ص ص 276-277.

في زمن إرتكابها، أو عدم الوصول إلى الجناة الذين يرتكبون هذه الجرائم، أو تعذر إقامة الدليل اللازم لإثباتها مما يترتب عليه إلحاق الضرربالأفراد وبالمجتمع.

وعليه يمكن القول أن التحري في كشف غموض الجريمة من طرف سلطات التحقيق يتطلب تدريبهم وتأهيلهم والمامهم بالتقنيات الأساسية لتكنولوجيات الإعلام والاتصال ومواكبتهم للتطور السريع الحاصل في هذا المجال اولإستعانة بالخبراء في الأمور التقنية المعقدة على نحو يمكنهم من استخلاص الأدلة الإلكترونية من بيئة افتراضية والتحقق من سلامتها وتقديمها كأدلة موثوقة للقضاء.

ث.ضعف التعاون الدولي في مكافحة الجرائم الإلكترونية

إن التعاون والتنسيق بين الأفراد والشركات يلعب دورا رئيسيا في إثبات الجريمة الإلكترونية، وعلى العكس من ذلك فإن غياب سياسة التعاون الدولي والتنسيق بين الدول في مقاومة الجريمة الإلكترونية يقابله في ذات الوقت تعاون واضح بين محترفي الإجرام المعلوماتي فضلا عن البرامج إلي يستعين بها القراصنة في أنشطتهم الإجرامية فإنهم يتعاونوا فيما بينهم ويتبادلون النصائح والخبرات فيما يتعلق بأنشطتهم، مما يزيد فاعلية وخطورة هجومهم وخصوصا في ظل قصور وعدم فاعلية سياسة الدفاع الخاصة والمنصوص ضد هذه الجريمة.

لذلك تنشأ ضرورة وجود توافق دولي محكم في مجال الحق في المعلومات على وجه الخصوص من سهولة حركة المعلومات في أنظمة تقنية المعلومات حيث يرجع لهذه السهولة في حركة المعلومات بأنه بالإمكان إرتكاب جريمة عن طريق حاسب آلي موجود في دولة معينة بينما يتحقق نجاح هذا النشاط الإجرامي في دولة أخرى.

كما أنه ورغم المناداة بضرورة التعاون الدولي في مكافحة هذه الجريمة إلا أن هناك عوائق تحول دون ذاك وتجعل هذا التعاون صعبا، وأهمها[1]:

أ. عدم وجود نموذج موحد للنشاط الاجرامي: فالأنظمة القانونية القائمة في الكثير من الدول لمواجهة الجرائم المعلوماتية لا يوجد فيها اتفاق عام مشترك حول نماذج إساءة إستخدام نظم المعلومات وشبكة الأنترنت الواجب تجريمها، فما يكون مباحا في بعض الأنظمة يكون محرما في أنظمة أخرى، ويرجع ذلك إلى عدة عوامل كإختلاف العادات والتقاليد والديانات والثقافات من مجتمع لآخر.

ب. اختلاف النظم القانونية الاجرائية: بسبب تنوع وإختلاف النظم القانونية الإجرامية نجد أن طرق التحري والتحقيق والمحاكمة التي تثبت فائدتها وفاعليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى.

ت. عدم وجود معاهدات ثنائية أو جماعية بين الدول: وحتى في حالة وجودها فإنها تكون قاصرة عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم وبرامج الحاسب وشبكة الانترنت.

[1]-الطيبي البركه، حاج سودي محمد، مرجع سابق، ص ص 277-278.

ث. مشكلة الاختصاص في جرائم الأنترنت: وتثار هذه المشكلة بالنسبة للاختصاص على المستوى الدولي وذلك لاختلاف التشريعات والنظم القانونية من دولة لأخرى حيث ينجم عنها تنازع الاختصاص بين هذه الدول بالنسبة للجرائم المتعلقة بالأنترنت التي تتميز بكونها عابرة للحدود، فيحدث أن ترتكب داخل إقليم دولة معينة إلا أنها تمتد إلى خارج إقليم دول أخرى مما يعني خضوعها لأكثر من قانون جنائي.

ج. عدم وجود قنوات اتصال: أن من أهم الأهداف المرجوة من التعاون الدولي في مجال الجريمة والمجرمين هي الحصول على المعلومات والبيانات المتعلقة بهم ولتحقيق هذا الهدف كان لازما أن يكون هناك نظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أمنية لجمع أدلة معينة أو معلومات مهمة، فعدم وجود مثل هذا النظام يعني عدم القدرة على جمع الأدلة والمعلومات العلمية التي غالبا ما تكون مفيدة في التحري لجرائم معينة ولمجرمين معينين وبالتالي تنعدم الفائدة من هذا التعاون.

لذاك أصبح أمر التعاون الدولي ومكافحة الجرائم الإلكترونية أمرا حتميا يستلزم ضرورة إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة هذه الجرائم، والعمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم، ويجب أن يشمل هذا التعاون تبادل المعلومات، تسليم المجرمين، سبل المكافحة، وضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دول أخرى، وتعد الوسيلة المثلى للتعاون الدولي في هذا الخصوص هو إبرام الإتفاقيات الدولية.

في مجال الاجراءات فإن التوافق بين مختلف سلطات التدخل الوطنية سيكون هاما من أجل التسيير دون عقبة لطلب المساعدة القانونية الوطنية، ويسهل من عملية القبض على مرتكبي هذه الجرائم، وذلك دون مساس هذه الإجراءات بسيادة الدول الأخرى وأمنها ونظامها العام أو أي مصلحة أخرى من مصالحها الأساسية.

كما تجدر الإشارة إلى أن المشرع الجزائري نص في الفصل السادس من القانون 09-04 المؤرخ في 2009/08/05، السالف الذكر، على قواعد تتعلق بالإختصاص القضائي والمساعدة القضائية الدولية المتبادلة وتبادل المعلومات واتخاذلاجراءات التحفظية ووضع قيود على طلبات المساعدة القضائية الدولية التي من شأنها المساس بالسيادة الوطنية أو النظام العام[1].

[1] الطيبي البركه، حاج سودي محمد، مرجع سابق، ص ص 279-280.

المبحث الثاني: العقوبات المقررة على الجريمة لنصب الإلكتروني

خطى المشرع الجزائري خطوات كبيرة في مجال مكافحة الجريمة الإلكترونية، وذلك بعد أن أقر بتجريم صور الإعتداء على شبكة الأنترنت والمساس بالبيانات المعالجة آليا، في إطار أحكام التعديل الذي شمل قانون العقوبات لسنة 2004 بموجب القانون رقم 04-15 المؤرخ في 2004/11/10 [1].

وبالرجوع إلى تعرف المشرع الجزائري لجريمة النصب من خلال ماتضمنته تعديل المادة 372 قانون العقوبات فنجد عرفها على صيغة العموم، ولم يحدد جريمة النصب الإلكتروني في حد ذاتها حيث عرف جريمة النصب على أنها " كل من توصل إلى إستلام أو تلقى أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالفات أو إجراء من إلتزامات أو إلى الحصول على أي منها أو شرع في ذلك وكان ذلك بالإحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما بإستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو إعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيئ أو في وقوع حادث او أية واقعة أخرى وهمية أو الخشية من وقوع شيئ منها.

وعليه فإن كان المشرع لم يربط جريمة النصب بالجريمة الإلكترونية ولم يحدد وسيلة بعينها، ولكن يمكن إسقاطها إذا ماتوفرت شروطها والمتمثلة في ما يلي:

أ. تحديد هوية مرتكب جريمة النصب الإلكتروني.

ب. أن نكون أمام تعامل قانوني للمال المعلوماتي وهي:

إستلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إجراء من إلتزامات أو الحصول على أي منها كما لم يفرق المشرع من الحصول على هذه المعلومات وبين الشروع فيها زرع الخوف في وقوع حادث أو واقعة أخرى وهمية أو الخشية في وقوع شيئ منها.

ومن أبرز الامثلة الخاصة بالنصب الإلكتروني نجد القضية التي حكم عليها محكمة النقض الفرنسية حول شخص داخل ساحة إنتظار السيارات، ولكنه عوض وضع النقود الأصلية في الآلة الإلكترونية وضع قطعة نقدية عديمة القيمة ترتب عن ذلك تشغيل الآلة وتحرك العقارب، بحيث إعتبرتها جريمة نصب إلكتروني وحتى وإن كان المعني لم يحصل على أي شيئ مادي .

المطلب الأول: العقوبات المقررة على الشخص الطبيعي

وهي الجزء الأساسي للجريمة ويكون في غالب الأحيان كافيا دون الإستعانة بعقوبات أخرى، وخصوصا أنها تنطبق على الفعل الإجرامي بحسب ما يستحق الحكم [2]، وهذا ما اقرته المادة 372 قانون العقوبات الجزائري "يعاقب بالحبس من سنة إلى 5 سنوات وبغرامة من 100.000 دج إلى 500.000 دج،

---

[1]-القانون رقم 04-15 المؤرخ في 2004/11/10 المتضمن قانون العقوبات، الجريدة الرسمية، عدد77، الصادر في 2004/11/10، ص8.

[2]-احمد نوري، **استرداد عائدات الفساد ودوره في الحد من جرائم الفساد**، مجلة العلوم الانسانية الجامعة، المجلد1 ، العدد1، ام البواقي، 2021، ص154.

وإذا وقعت الجنحة على مجموعة تزيد عن ثلاثة أشخاص فيجوز ان تصل مدة الحبس إلى 10 سنوات والغرامة إلى 1.000.000 دج"

الفرع الأول: العقوبات الأصلية

بالاضافة إلى العقوبات التي قررتها المادة 372 والتى تطرقنا إليها سابقا، ومن خلال النصوص الخاصة بالجرائم الماسة بالانظمة الإلكترونية يتبين لنا وجود تدرج داخل النظام العقابي، هذا التدرج في العقوبات يحدد الخطورة الإجرامية التي قدرها المشرع لهذه التصرفات إذ نجد سلم خطورة يتضمن ثلاث درجات، جريمة الدخول او البقاء بالغش في الدرجة الأولى وبعدها في الدرجة الثانية جريمة الدخول والبقاء المشددة، أما الدرجة الثالثة فتحتلها الجريمة الخاصة بالمساس العمدي بالمنظومة الإلكترونية.

أولا: عقوبة الدخول أو البقاء غير المشروعان للنظام

في حالة الدخول غير المشروع من طرف المجرم الإلكتروني للنظام كله أو جزء منه أو متى كان مسموح له بالدخول إلى جزء معين النظام وتجاوزه، ومتى كان الدخول أو التواجد داخل النظام مخالف لإرادة صاحب النظام، تكون العقوبة حسب المادة 394 مكرر (قانون 04-15+قانون 24-06) يعاقب بالحبس من ستة أشهر إلى سنتين وغرامة من 60.000 دج إلى 200.000دج كل من يدخل او يبقى عن طريق الغش في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات او يحاول ذلك، تضاعف العقوبة اذا ترتب على ذلك حذف او تغير معطيات المنظومة.

وإذا ترتب على الافعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة بالحبس من سنة الى ثلاث سنوات والغرامة من 100.000 دج الى 300.000دج.

ثانيا: عقوبة المساس بمنظومة معلوماتية

نص المشرع الجزائري في المادة 394 مكرر 01 من نفس القانون السابق الذكر على يعاقب بالحبس من سنة إلى 03 سنوات وغرامة من 500.000 دج إلى 2.000.000 دج، كل من ادخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها.

ثالثا: عقوبة الإشتراك والشروع في جريمة النصب الإلكتروني

أ. عقوبة الإشتراك:

نصت عليها المادة 394 مكرر 05 من القانون رقم 04-15 بقولها ": كل من شارك في مجموعة أو إتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم، وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها"[1].

[1]-احمد نوري، مرجع سابق، ص154.

ب. عقوبة الشروع:

يعاقب القانون على الشروع كما لو وتمت الجريمة ولا يتحقق الشروع الا ابتداءا من الوقت الذي يظهر فيه المحتال نيته في إستلام المال بعد استعمال وسيلة من وسائل التدليس، وقبل هذه اللحظة لاتعد الأعمال التي يقوم بها المحتال الا مجرد اعمال تحضيرية لتنفيذ الجريمة وهي اعمال غير مجرمة[1].

نصت عليها المادة 394 مكرر 07 من نفس القانون بقولها: "يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها"

إلا أن المشرع الجزائري اعتمد على ضرورة المعاقبة على الشروع في المادة 394 مكرر07 السالفة الذكر فالجرائم الماسة بالانظمة الإلكترونية لان لها وصف جنحي ولاعقاب على الشروع في الجنح إلا بنص نصت عليه المادة 11 من اتفاقية الدولية للاجرام المعلوماتي.

يبدو من خلال هذا النص رغبت المشرع في توسيع نطاق العقوبة لتشمل اكبر قدر من الافعال الماسة بالانظمة الإلكترونية، إذ جعل الشروع في إحدى هذه الجرائم معاقب بنفس عقوبة الجريمة التامة، ومن خلال استقراء نص المادة نستنتج ان الجنحة الواردة بنص المادة 394 مكرر 05 من قانون العقوبات مشمولة بهذا النص، أي أن المشرع الجزائري بهذا المنطق يكون قد تبنى فكرة الشروع في الإتفاق الجنائي[2].

الفرع الثاني: العقوبات التكميلية

بالاضافة الى العقوبات التكميلية التي حددتها المادة 394 مكرر 06 قانون العقوبات والتي سنذكرها بالشرح في العقوبات التكميلية للشخص المعنوي تطبق على جريمة النصب نفس العقوبات التكميلية المقررة لجنحة السرقة وهكذا يجوز الحكم على الجاني بالحرمان من الحقوق الوطنية والمدنية والعائلية المنصوص عليها المادة [3] 9 مكرر 1 لمدة أقصاها عشرة سنوات تسري من يوم انقضاء العقوبة الاصلية أو الافراج عن المحكوم عليه.

وعلاوة على العقوبتين التكميليتين المذكورين أعلاه يجيز قانون العقوبات بوجه عام للجهات القضائية الحكم على الشخص المدان لإرتكاب جنحة بالعقوبات التكميلية الآتية[4]:

أولا: العزل أو الإقصاء من جميع الوظائف والمناصب العمومية التي لها علاقة بالجريمة.

ثانيا: الحرمان من حق الإنتخاب والترشح ومن حمل أي وسام الأهلية لأن يكون مساعدا محلفا، أو خبيرا، أو شاهدا على أي عقد، أو شاهدا أمام المحكمة.

ثالثا: عدم القضاء إلا على سبيل الإستدلال.

---

[1]-حسن بوسقيعة، **الوجيز في القانون الجزائي الخاص**، الجزء الأول، الطبعة العشرون، دار هومة، الجزائر، 2018، ص323.

[2]-طبال احسان، **محاضرات مقياس الجرائم المعلوماتية**، كلية الحقوق والعلوم السياسية، جامعة يحي فارس بالمدية، الجزائر، بدون سنة، ص14.

[3]-المادة 09 مكرر أظيفت بموجب القانون 06-23 المؤرخ 20 ديسمبر 2006.

[4]-حسن بوسقيعة، مرجع سابق، ص323.

رابعا: الحرمان من الحق في حمل الأسلحة، وفي التدريس، وفي إدارة مدرسة أو الخدمة في مؤسسة للتعليم بوصفه أستاذا، أو مدرسا أو مراقبا.

خامسا: عدم الأهلية لأن يكون وصيا أو قيما.

سادسا: سقوط حقوق الولاية كلها أو بعضها.

الفرع الثالث: الظرف المشدد للاشخاص الطبيعية

نص القانون على ظرفين مشددين لجريمة النصب وهما[1]:

أولا: ظرف يتعلق بالجاني: وهو الظرف المنصوص عليه في الفقرة الثانية من المادة 372 التي جاءت على النحو الاتي: "إذ وقعت الجريمة من شخص لجأ الى الجمهور بقصد اصدار اسهم سواء شركات أو مشروعات تجارية أو صناعية، وفي هذه الحالة يجوز رفع العقوبة لتصل مدة الحبس إلى 10 سنوات والغرامة الى 400.000دج.

ثانيا: ظرف يتعلق بالمجني عليه: وهو الظرف المنصوص عليه في الفقرة 2 من المادة 382 مكرر، وهو عندما تكون الضحية الدولة أو احدى مؤسساتها، ففي هذه الحالة تكون العقوبة بالحبس من سنتين الى 10 سنوات حبسا.

وقبل تعديل نص المادة 382 مكرر بموجب القانون المؤرخ في 26-06-2001، كانت العقوبة تصل الاعلام عندما يترتب عن الجريمة اضرار بمصالح الامة.

هذا بالاضافة الى الظرف المشدد الذي ذكرناه في عقوبة الدخول أو البقاء غير المشروعان.

المطلب الثاني: العقوبات المقررة للشخص المعنوي

كباقي الجرائم هناك عقوبات مقررة على جريمة النصب للشخص المعنوي.

الفرع الأول: العقوبة الأصلية

مبدأ مساءلة الشخص المعنوي وارد في المادة 12 من الاتفاقية الدولية للاجرام المعلوماتي، بحيث يسأل الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا اصليا او شريكا او متدخلا كما يسأل عن الجريمة التامة او الشروع فيها، كل ذلك بشرط ان تكون الجريمة قد ارتكبت لحساب الشخص المعنوي بواسطة احد اعضائه او ممثليه.

هذا مع ملاحظة ان المسؤولية الجزائية للشخص المعنوي لا تستبعد المسؤولية الجزائية للاشخاص الطبيعيين بصفتهم فاعلين او شركاء او متدخلين في نفس الجريمة، ولقد نصت المادة 394 مكرر 4 (قانون 04-15) "يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الاقصى للغرامة المقررة للشخص الطبيعي".

[1]-حسن بوسقيعة، مرجع سابق، ص324.

كما تجدر الاشارة إلى أن المشرع الجزائري قد اقر في التعديل الأخير لقانون العقوبات المسؤولة الجزائية للشخص المعنوي وذلك في نص المادة 18 مكرر من القانون 04-15 المتضمن تعديل قانون العقوبات الذي ينص على أن: "العقوبات المطبقة على الشخص المعنوي في مواد الجنايات والجنح هي:

أولا: الغرامة التي تساوي من مرة إلى خمس مرات الحد الأقصى للغرامة المقدرة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.

ثانيا: واحدة او اكثر من العقوبات الآتية [1]:

أ. حل الشخص المعنوي.

ب. غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز 5 سنوات.

ت. الإقصاء من الصفقات العمومية لمدة لا تتجاوز 5 سنوات.

ث. المنع من مزاولة نشاط أو عدة أنشطة مهنية أو إجتماعية بشكل مباشرة أو غير مباشرة نهائيا أو لمدة لا تتجاوز 5 سنوات.

ج. مصادر الشيء الذي إستعمل في إرتكاب الجريمة أو نتج عنها.

ح. نشر او تعليق حكم الادانة.

خ. الوضع تحت الحراسة القضائية لمدة لاتتجاوز 5 سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكب الجريمة بمناسبته.

بالنسبة لعقوبات الغرامة المطبقة على الشخص المعنوي عند إرتكابه أحد الجرائم الماسة بالأنظمة الإلكترونية فهي تعادل طبقا للمادة 394 مكرر 4 قانون العقوبات 5 مرات الحد الاقصى للغرامة المقررة للشخص الطبيعي.

3. الشروع في جريمة النصب : ويتحقق الشروع عادة بإتيان المتهم أي فعل أو أي عمل يمكن اعتباره بدء في التنفيذ لجريمة ثم تخيب ولا تحدث النتيجة لسبب خارج عن إرادة المجرم وقد عرفت المادة 30 من قانون العقوبات عملية الشروع بأنها أنها كل محاولة تبتدئ بالشروع المباشر في التنفيذ أو بأفعال لا لبس فيها تؤدي إلى ارتكابها حتى لو توقفت ولم تخب أثرها إلا نتيجة ظروف مستقلة عن إرادة مرتكبيها.

4. الاشتراك في جريمة النصب: فإن مثله مثل الشروع فيها يخضع إلى القواعد العامة المنصوص عليها المادة 42 من قانون العقوبات التي جاء فيه": انه يعتبر شريكا في الجريمة من لم يساهم فيها إسهاما مباشرا لكنه يكون قد ساعد أو عاون الفاعل بكل الطرق على إنجاز الأفعال التحضيرية أو المسهلة أو المنفذة لها علمه لذلك".

[1]-طبال احسان، مرجع سابق، ص12.

الفرع الثاني: العقوبات التكميلية

نصت المادة 394 مكرر 06 من نفس القانون على مجموعة من العقوبات التكميلية، يحكم بها إلى جانب العقوبات الأصلية مع الاحتفاظ بحقوق غير حسن النية، يحكم:

أولا: المصادرة: وتعني مصادرة الأجهزة والبرامج والوسائل المستخدمة لإرتكاب الجرائم الماسة بالنظام وذلك ببيعها، أو حجزها مع مراعاة حقوق الغير حسن النية.

ثانيا: إغلاق المواقع: إغلاق مواقع الأنترنت أو المواقع الإلكترونية بصفة عامة، والتي كانت وسيلة لإرتكاب هذه الجرائم أو ساهمت في إرتكابها.

ثالثا: إغلاق المحل (المقهى الإلكتروني):

يكون في الحالة التي يكون صاحب المحل مشاركا في الجريمة، وذلك إذا تمت الجريمة وهو عالم بها ولم يتصدى لها بالإخبار عنها، أو بمنع مرتكبيها من ارتياد محله لارتكاب مثل هذه الجرائم.

ومنا لملاحظ أن هذه العقوبات جاءت رادعة حيث تضاعف عند الضرورة، كما إشتملت على عقوبات التكميلية، وحتى عقوبات الشخص المعنوي [1].

الفرع الثالث: الظرف المشدد للشخص المعنوي

العقوبات المقررة للشخص المعنوي.

نص المشرع الجزائري في المادة51 [2] مكرر من القانون رقم 04-15 على مسائلة الشخص المعنوي "باستثناء الدولة والجماعات المحلية والاشخاص المعنوية الخاضعة للقانون العام، يكون الشخص المعنوي مسؤولا جزئيا عن الجرائم التي ترتكب لحسابه من طرف أجهزته أو ممثليه القانونيين أو الحائزين على تفويض سلطات، عندما ينص القانون على ذلك، كما نصت المادة 394 مكرر 04 من نفس القانون على " يعاقب الشخص المعنوي الذي يرتكب احدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمسة مرات الحد الاقصى للغرامة المقررة للشخص الطبيعي".

كما تبنى المشرع الجزائري مبدأ معاقبة الإتفاق الجنائي بنص المادة 394 مكرر 05 وفقا للمادة 11 من الاتفاقية الدولية للإجرام المعلوماتي.

---

[1]-نايري عائشة، **الجريمة الإلكترونية في التشريع الجزائري**، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة أحمد درارية –أدرار-، الجزائر، 2016-2017، ص ص38-39.

[2]-المادة 51 مكرر اضيفت بالقانون 04-15 ومعدلة قانون 24-06.

الخلاصة:

إستخلصنا من هذا الفصل أنه كلما تم تحديد معايير الإختصاص تحديدا دقيقا، كلما سهل العمل القضائي في الوصول إلى نتائج إيجابية في مواجهة جريمة النصب الإلكتروني كجريمة من الجرائم الإلكترونية التي تتسم بخصوصية التحقيق فيها والتحري بطرق حديثة متطورة تختلف عن تلك المتبعة في الجرائم التقليدية التي لا تتطلب آليات معقدة في إثباتها كآليات الإثبات الخاصة بالجريمة الإلكترونية خاصة مع ظهور شبكة الانترنت التي فسحت المجال لظهور المجرم الإلكتروني الذي إستطاع أن يعبر الحدود الدولية بجريمته، وبالتالي وضعت على عاتق الدول ومنها الجزائر عبئ اثبات جرائم سريعة الانتشار وسريعة طمس الآثار، ثم وضحنا فيه العقوبات المقررة لجريمة النصب الالكتروني في التشريع الجزائري، كما قمنا بإسقاط المادة 372 قانون العقوبات الجزائية التي تضمنت العقوبات الأصلية واشارت إلى المادة 9 قانون العقوبات للرجوع إلى العقوبات التكميلية سواء على الشخص الطبيعي أو المعنوي، كما أشارت أيضا في فقرتها الثانية إلى الظرف المشدد والعقوبة المقرر له، هذا يالاضافة إلى ما جائت به المواد 394 مكرر 1 إلى 394 مكرر 7 من قانون 04-15 المعدل والمتمم قانون العقوبات.

خاتمة

خاتمة.

من خلال ما سبق تعرفنا على جريمة النصب الإلكتروني من الناحية الموضوعية ومن الناحية الإجرائية، فتطرقنا إلى مفهومها وخصائصها وأركانها، كما ميزنا بينها وبين ما يشابهها من جرائم إلكترونية، ثم إنتقلنا إلى الناحية الإجرائية بدءا بالاختصاص وأعطينا نماذج عن إجراءات التحقيق وصعوبات الإثبات التي تواجهها كما وضحنا العقوبات المقررة لها سواء كان ذلك بالنسبة للشخص الطبيعي أو الشخص المعنوي.

وعالجنا بكل موضوعية هذه الجريمة التي إستفحلت في المجتمعات وأصبحت من أخطر الجرائم على الأشخاص والأموال، خاصة بعد التطور التكنولوجي المذهل والسريع في عالم الحواسيب والعولمة ومن هنا توصلنا الى نتائج أهمها:

– ان التطور التكنولوجي هو العنصر المحوري في تطور جريمة النصب الإلكتروني فكلما علا نمط التكنولوجيا كلما زاد معه المجرم الالكتروني حيلة ودهاء، فاصبح النصاب يختفي وراء الشاشات ويتفننون في إيجاد طرق ووسائل إحتيالية إجرامية في عالم إفتراضي، كم يسهل الهروب منه بكبسة زر.

– إن غياب نص قانوني خاص بجريمة النصب الإلكتروني كجريمة قائمة بحد ذاتها يصعب من مهمة دراستها بشكل دقيق، بل يعتمد الباحث على إسقاط مواد قانونية أخرى عليها.

– إن إجراءات التحقيق التقليدية تحتاج إلى تطوير من اجل التعامل مع هاته الجريمة من حيث الوسائل المستعملة في ذلك.

بالاضافة الى ان اموال الناس أصبحت في خطر دائم ومحتمل للإستلاء عليها برضاهم حتى وإن كان ذلك الرضا مشوبا بعيب الغش هذا من جهة ومن جهة اخرى أثارت الجرائم الإلكترونية تحديات لها وزنها في النظام القانوني وبالأخص قانون العقوبات، الذي أضفى بضلاله على الجرائم التقليدية بالحماية القانونية وعجز عن إحتواء جميع الجرائم الإلكترونية إلا في حيز ضيق، إلا أنه تفطن لإلحاق صفة المال على المعلومات والبيانات وبرامج الحوسبة مما جعل منها محلا للحماية القانونية ومن أجل إكتمال هذه الحماية توجب حل بعض المشكلات القانونية كتحديد القانون الواجب التطبق والمحكمة المختصة في ذلك، كما ان العقاب على جريمة النصب الإلكتروني في ظل نقص النصوص التشريعية غالبا ما يصطدم مع مبدأ الشرعية الذي يقضي بألا جريمة ولا عقوبة إلا بنص، ومن هنا يمكن أن نقدم اقتراحات التالية، على سبيل الإجتهاد.

أ.توحيد النصوص القانونية وضم القواعد الواردة في قانون العقوبات من كل القوانين الأخرى المتعلقة بمكافحة الجرائم الإلكترونية في نص واحد تحت مسمى قانون مكافحة الجرائم الإلكترونية.

ب. كان ينبغي على المشرع الجزائري ان يفرد مادة قانونية خاصة بجريمة النصب الالكتروني كما فعل مع الكثير من الجرائم الإلكترونية او لو انه اضاف فقرة في المادة 372 قانون العقوبات تنص على تشديد العقوبة في حالة ما اذا تم النصب الإلكترونية.

ت. تطوير أنظمة الحماية التقنية في إطار المعالجة الآلية للمعطيات بالإضافة إلى الحماية الجنائية لتقنيات الإتصال الحديثة.

ث. العناية بالعنصر البشري المتخصص عن طريق التدريب الفني الفائق خاصة من قبل المحقيقين في كل ما يخص النظام المعلوماتي.

ج. تبادل الخبرات والكفاءات بين مختلف الدول في مجال مكافحة الجرائم الإلكترونية.

ح. حماية الدليل الرقمي من محو أثاره، وتطوير تقنيات إسترجاعه بعد إتلافه.

خ. الإعتماد على البصمة الإلكترونية للتمكن من الوصول إلى كل مجرم يلج عالم الكمبيوتارات والحواسيب.

د. الإستغناء عن الحصر للوسائل الإحتيالية لقيام جريمة النصب المنصوص عليه في المادة 372 من القانون العقوبات الجزائية وذلك للتطور السريع للتكنولوجيا الذي يساعد على إبتكار وسائل إحتيالية جديدة ليست مذكورة في النصوص القانونية وبالتالي يفلت النصاب الإلكتروني من العقاب بحجة أنه لم يأتي وسيلة مجرمة قانونا ونكون أمام ثغرات قانونية نحن في غنى عنها.

وأخيرا تقبلوا منا المجهود ومن الله التوفيق أن شاء الله.

قائمة المراجع

أولا: القراءان الكريم

ثانيا:النصوص القانونية

1. النصوص التشريعية

أ. القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004 المعدل للأمر 66-156 المتضمن قانون الاجراءات الجزائية، الجريدة الرسمية العدد 71.

ب.القانون رقم 04-15 المؤرخ في 2004/11/10 المتضمن قانون العقوبات، الجريدة الرسمية، عدد77، الصادر في 2004/11/10.

ت.القانون رقم 09-04 المؤرخ في 5-8-2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والإتصال، الجريدة الرسمية رقم 47 المؤرخة في 16-8-2009.

ث.المرسوم التنفيذي رقم 06-348 المؤرخ في 5-11-2006، الجريدة الرسمية رقم 63 المؤرخ في 8-11-2006.

ج. المادة 09 مكرر أظيفت بموجب القانون 06-23 المؤرخ 20 ديسمبر 2006.

ح. المادة 51 مكرر اضيفت بالقانون 04-15 ومعدلة قانون 24-06.

خ. المادة 65 مكرر 5 من قانون الإجراءات الجزائية.

ثالثا: الكتب

1.احمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، مصر، 2005

2. عبد الحكيم فودة، جرائم الاحتيال النصب وخيانة الامانة والشيك والعاب القمار في ضوء الفقه وقضاء النقص، دار المطبوعات الجامعية، مصر، 2006.

3. حسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجرائم ضد الأشخاص والأموال، دار هومه، الجزء الأول، 2008.

4. عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة دراسة ظاهرة الإجرامية المعلوماتية، دار الفكر الجامعي، مصر، 2008.

5. عبد الفتاح، بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي (دراسة معقة في مكافحة جرائم التقنية الحديثة)، دار النهضة العربية، الطبعة الأولى، مصر، 2009.

6. عائشة بن قارة مصطفلى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائن الجزائري والمقارن، دار الجامعة الجديدة، كلية الحقوق جامعة الإسكندرية، مصر، 2010 .

7. نهلا عبد القادر المومني، الجرائم المعلوناتية، دار الثقافة للنشر والتوزيع، الطبعة الثانية، الأردن، 2010.

8. زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين ميلة، الجزائر، 2011.

9. اسامة حمدان الرقب، جرائم النصب والاحتيال الاساليب –المظاهر-العلاج، دار يافا العلمية للنشر والتوزيع، الطبعة الاولى، الاردن، 2012.

10. ناير نبيل عمر، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، مصر، 2012.

11. مطر عصام عبد الفتاح، التجارة الإلكترونية في التشريعات العربية والجنبية، دار الجامعة الجديدة، مصر، 2015.

12. عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، دار الفكر الجامعي، الكتاب الثاني، مصر،

رابعا:مذكرات والرسائل الجامعية

1. ربيعي حسين، أليات البحث والترحي عن الجرائم الإلكترونية، مذكرة دكتوراه، كلية الحقوق والعلوم السياسة، جامعة باتنة، الجزائر، 2016.

2. نايري عائشة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية –أدرار-، الجزائر، 2016-2017.

3. حشمان عمار، الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماستر، تخصص إدارة التحقيقات الاقتصادية والمالية، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة قاصدي مرلاح – ورقلة-، 2018-2019

4. بن زرت اسيا، إثبات الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، الجزائر، 2018-2019.

5. حبيب بوسماط، جريمة النصب باستعمال الوسائل المعلوماتية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، الجزائر، 2018-2019.

6. زيان سعيد، سالمي هشام، جريمة النصب الإلكتروني، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف –المسيلة، الجزائر، 2021-2022.

7. بوعلاق مهدي، جريمة النصب والإحتيال في التشريع الجزائري، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة تبسة، الجزائر، 2022-2023.

خامسا:المجلات والمقالات:

1. رحال بومدين، سعداني نورة، الحماية الجنائية الواقعة على أموال التجارة الإلكترونية (جريمة السرقة والنصب)، مجلة الواحات للبحوث والدراسات، المجلد 09، العدد 02، 2016

2. الطيبي البركه، إشكالية الإثبات في الجرائم الإلكترونية، مجلة آفاق علمية، المجلد 11، العدد 01، جامعة أدرار، 2019.

3. احمد نوري، استرداد عائدات الفساد ودوره في الحد من جرائم الفساد، مجلة العلوم الانسانية الجامعة، المجلد1 ، العدد1، ام البواقي، 2021.

4. العايب سامية، عراب منال، الحماية الجزائية للمستهلك من جريمة النصب الإكتروني، مجلة هيرودوت للعلوم الإنسانية والإجتماعية، المجلد 05، العدد 03، 2021.

5. مجدوب نوال، الاليات الإجرائية للكشف عن الجريمة المعلوماتية، مجلة البحوث القانونية والإقتصادية، المجلد 06، العدد 03، المركز الجامعي مغنية، الجزائر، 2023

سادسا: المحاضرات الجامعية

1. طبال احسان، محاضرات مقياس الجرائم المعلوماتية، كلية الحقوق والعلوم السياسية، جامعة يحي فارس بالمدية، الجزائر، بدون سنة،

فهرس المحتويات

العنوان	الصفحة
شكر وتقدير:	
إهداء:	
مقدمة:	**3-1**
الفصل الأول: مفهوم جريمة النصب الإلكتروني	**19-4**
تمهيد:	**4**
المبحث الأول: ماهية النصب الإلكتروني.	**5**
المطلب الأول:تعريف النصب الإلكتروني.	**5**
الفرع الأول: التعريف اللغوي والفقهي والقانوني لجريمة النصب الإلكتروني.	**5**
الفرع الثاني: خصائص النصب الإلكتروني.	**6**
الفرع الثالث: التمييز بين النصب الإلكتروني وبين ما يشبهه من جرائم.	**9**
المطلب الثاني: أساليب جريمة النصب الإلكتروني.	**12**
الفرع الأول: إستعمال طرق إحتيالية.	**12**
الفرع الثاني إتخاذ الإسم الكاذب أو انتحال الصفة غير الصحيحة.	**13**
الفرع الثالث: التصرف في مال الغير، ثابت او منقول.	**14**
المبحث الثاني: أركان جريمة النصب الإلكتروني.	**15**
المطلب الأول: الركن المادي لجريمة النصب الإلكتروني.	**15**
الفرع الأول: السلوك الإجرامي.	**15**
الفرع الثاني: النتيجة الإجرامية.	**16**
الفرع الثالث: العلاقة السببية.	**16**
المطلب الثاني: الركن المعنوي لجريمة النصب الإلكتروني .	**17**
الفرع الأول: القصد الجنائي العام.	**17**
الفرع الثاني: القصد االجنائي الخاص.	**18**
الخلاصة:	**19**
الفصل الثاني: الجوانب الإجرائية والموضوعية لجريمة النصب الإلكتروني.	**47-21**

فهرس المحتويات

العنوان	الصفحة
تمهيد:	**21**
المبحث الاول: نطاق الإختصاص في جريمة النصب الإلكتروني وإجراءات التحقيق فيها	**22**
المطلب الأول: معايير تحديد الإختصاص والإختلاف الفقهي حول تمديد الإختصاص	**22**
الفرع الأول: الموقف الفقهي والقضائي والتشريعي من مسألة الإختصاص في جريمة النصب الإلكتروني	**22**
الفرع الثاني:موقف المشرع الجزائري من مسألة الإختصاص القضائي المحلي	**26**
المطلب الثاني: الإجراءات التقليدية والإجراءات المستحدثة للمتابعة في جريمة النصب الإلكتروني.	**28**
الفرع الاول: الاجراءات التقليدية للمتابعة في جريمة النصب الإلكتروني.	**28**
الفرع الثاني: الإجراءات المستحدثة في جريمة النصب الإكتروني.	**34**
الفرع الثالث: صعوبات الإثبات في جريمة النصب الإلكتروني.	**35**
المبحث الثاني: العقوبات المقررة لجريمة لنصب الإلكتروني	**41**
المطلب الأول: العقوبات المقررة للشخص الطبيعي	**42**
الفرع الأول: العقوبات الأصلية.	**43**
الفرع الثاني: العقوبات التكميلية.	**46**
الفرع الثالث: الظرف المشدد.	**46**
المطلب الثاني: العقوبات المقررة للشخص المعنوي	**44**
الفرع الأول :العقوبة الأصلية.	**44**
الفرع الثاني: العقوبات التكميلية.	**46**
الفرع الثالث: الظرف المشدد.	**46**
الخلاصة:	**47**
الخاتمة:	**49**
قائمة المراجع:	**52**
الفهرس:	**56**
الملخص	**59**

ملخص

ملخص

تعد جريمة النصب الالكتروني من الجرائم المستحدثة التي تشكل خطوة على الاموال والاشخاص في نطاق واسع لا يعرف الحدودو لقد تمت دراسة هذا الموضوع من خلال التعرف على خصائصها وأركانها، وما يميزها عما يشابهها من جرائم، والتطرق إلى مسألة الإختصاص الذي كثيرا ما يصعب تحديده في مثل هذه الجرائم، لنصل إلى العقوبات المقررة لها في التشريع الجزائري، وإنتهت الدراسة بجملة من النتائج من أهمها ان النصب الإلكتروني يزداد تطورا وذكاء كلما ازداد تطور التكنولوجيا، وهذا ما أرق التشريعات في التصدي لهذه الجريمة.

الكلمات المفتاحية: النصب الإلكتروني، الجريمة الإلكترونية، الدليل الإلكتروني.

Résumé :

Le délit de fraude électronique est l'un des nouveaux délits qui constituent une menace pour l'argent et les personnes à grande échelle et sans frontières, Ce sujet a été étudié en identifiant ses caractéristiques et ses éléments,Ce qui le distingue des crimes similaires, et abordant la question de la compétence, qui est souvent difficile à déterminer dans de tels crimes, Venons-en aux sanctions prévues par la législation algérienne, L'étude conclut par un certain nombre de résultats dont le plus important est que la fraude électronique devient de plus en plus sophistiquée et intelligente à mesure que la technologie se développe, C'est ce qui rend difficile la législation pour lutter contre ce crime.

les mots clés : Fraude électronique, Cybercriminalité, Guide électronique.

Summary :

The crime of electronic fraud is one of the new crimes that constitute a threat to money and people on a wide scale that knows no borders. This topic has been studied by identifying its characteristics and elements. What distinguishes it from similar crimes, and addressing the issue of jurisdiction, which is often difficult to determine in such crimes, Let us arrive at the penalties prescribed for it in Algerian legislation. The study concluded with a number of results, the most important of which is that

ملخص

electronic fraud becomes more sophisticated and intelligent as technology develops. This is what makes legislation difficult to combat this **crime.**

Keywords: electronic fraud, Cybercrime, Electronic guide.