وزارة التعليـم العالـي والبحث العلمـي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE
Abdelhamid Ibn Badis
MOSTAGANEM

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق و العلوم السياسية

قسم القانون العام

المرجع: 06

مذكرة نهاية الدراسة لنيل شهادة الماستر

جريمة النصب باستعمال الوسائل المعلوماتية

ميدان الحقوق و العلوم السياسية

الشعبة: حقوق **التخصص: قانون الجنائي والعلوم الجنائية**

من إعداد الطالب: **تحت إشراف الأستاذ الدكتور:**

حبيب بوسماط **عبد القادر فنينخ**

أعضاء لجنة المناقشة

الأستاذ:	الجيلالي بوسحبة	رئيسا
الأستاذ:	عبد القادر فنينخ	مشرفا مقررا
الأستاذ:	خالد زواتين	مناقشا و ممتحنا

نوقشت يوم 2019/06/23 **السنة الجامعية: 2019/2018**

إهداء

إلى الذي رحل بدون وداع , و ترك حسرة تعبر عنها دمعة الاشتياق و الحنين و الشوق

الذي كنت أرى القوة و الحب و العطف في عينيه أبي نور العين أه يا روحي كم أتمنى أن تكون فخورا بابنك و لو انك بقبرك الذي أتمنى من الله أن يكون روضة من رياض الجنة .

إلي من لا حلاوة و لا معنى للدنيا بدونها, إلى من جعلت الدنيا طريقا سهلا لي من خلال تضحياتها و سندها إلي الرائعة و الغالية و الحبيبة أمي و يا ليتني أكون وفقت في نيل رضاها .

إلى روح أخواي إبراهيم و أحمد و إلى إخوتي الشارف و الطاهر و بدر الدين و الحنونة أختي مختارية .

إلى العائلة الكريمة عائلة بوسماط و عائلة غزالي و خاصة الأجداد رحمة الله عليهم جميعا .

الى عائلة : ساحي , بوزيان, نوار, ساهل, بن شرطان , أوغاري

إلى كل الأحبة و الأصدقاء و الجيران بدون استثناء.

الى أصدقائي الدين أعتبرهم أخوة : طيب زيزي عدنان , قاسم بن عمارة

وإلى كل الزملاء في الكلية و التخصص .

إلى كل العاملين في الكلية بدون استثناء في المكتبة و الأقسام و العمادة و الأمن الداخلي و عاملات النظافة .

شكر و عرفان

أولا و قبل كل شيئ الحمد لله الذي باسمه تتم الصالحات , فالحمد لله حمدا كثيرا مباركا فيه أشكرك يا الله على نعمك و فضلك علي أنا العبد الضعيف فيارب لا رجاء لي سوى رضاك.

إلى ذلك الشخص الذي جعل كل شيء ممكن , إلى الذي أخذ بيدي, إلى من أراه قدوتي بعد الرسول عليه أفضل الصلاة و أزكى التسليم , بفضله بعد فضل الله علي تم الانتهاء من كتابة المذكرة التي لم أكن أحلم يوما انني سأصل إليها و أكتبها بأناملي إلى الأستاذ و الدكتور و الأخ و الناصح و المعين إلى الدكتور فنينخ عبد القادر أستاذ القانون بكلية الحقوق و العلوم السياسية بمستغانم.

إلى أساتذتي كلهم بدون استثناء فكلية الحقوق و العلوم السياسة بمستغانم التي تشكل وحدة عائلية لا غنى لأي واحد منها.

إلى العميد الأستاذ الدكتور عباسة الطاهر.

إلى عمال مكتبة كلية الحقوق و خاصة الصديق العزيز بـ-جمال.

إلى كل من أحبني و دعمني و لو بكلمة طيبة.

إلى كل الناس الذين عرفتهم بصفة عامة .

مقدمة:

لم تكن جريمة النصب معروفة في التشريعات القديمة ولقد كانت في القانون الروماني صورة من صور جريمة سلب مال الغير من بينها السرقة وخيانة الأمانة.

كما لم تبرز جريمة النصب بذاتها إلا بعد قيام الثورة الفرنسية فكانت قبل ذلك تكيف تارة على أنها سرقة وتارة أخرى تزوير.فكان يعاقب على استعمال أسماء أو صفات كاذبة على أساس جريمة التزوير بعدها أصبحت جريمة مستقلة بذاتها عن غيرها من الجرائم الشبيهة بها ووضع لها نص خاص في تشريع سنة 1791 التي أتت به الثورة الفرنسية بعدها نصت على جريمة النصب بموجب تشريع 1810 واعتبرت جريمة النصب جريمة قائمة بذاتها لها خصائص ومميزات تميزها عن جريمة السرقة والتزوير وخيانة الأمانة.

واستعمل لأول مرة مصطلح النصب في نص المادة 405 من قانون العقوبات الفرنسي تحت لفظ الطرق الاحتيالية بدلا من لفظ التدليس وحدد ماهية الأفعال المكونة للنصب والمتمثلة في استعمال أسماء أو صفات كاذبة أو وسائل التدليس والاحتيال. بتاريخ 08 أوت 1935 أضيفت فقرة إضافية لتلك المادة بموجب مرسوم تشريعي نص فيها على الظروف المشددة لجريمة النصب والمتمثلة في ارتكاب النصب في مواجهة الجمهور وأضاف إلى جانب ذلك العقوبات التكميلية والمتمثلة في الحرمان من الحقوق الوطنية كلها أو بعضها والمنع من الإقامة وهي عقوبات جوازيه.

يحمي القانون الجنائي حق الملكية سواء كان محله عقارا أو منقولا، وان كانت ملكية المنقولات تحظى بالنصيب الأوفر من رعاية التشريع الجنائي. والجرائم التي تقع اعتداء على ملكية المنقول تنقسم إلى طائفتين رئيسيتين أحدهما تضم جرائم تكون الغاية منها الاستيلاء على مال الغير والأخرى تشمل جرائم تكون غايتها إتلاف مال الغير، ويدخل ضمن الطائفة الأولى جرائم السرقة والنصب وخيانة الأمانة.

كما لحق بجريمة النصب تطور كبير وهائل مع تطور العصر ولم تعد ترتكز على إتباع الوسائل التقليدية لارتكابها ،وتطورت مع مرور الزمن واتخذت عدة صور وتنوعت أساليب النصابين ووسائلهم الاحتيالية وتطورت مع التطور التكنولوجي وخاصة مع ظهور الإعلام الآلي والشبكات الإعلامية والإنترنت التي عصرنه الوسائل التدليسيه المستعملة حيث أصبح من الصعب على الأشخاص العاديين اكتشافها بسهولة وتفادي الوقوع فيها خاصة في عمليات البنوك والبيع والشراء عن طريق الإنترنيت واشتهرت في الآونة الأخيرة هذه الظاهرة وتفشت في الدول الغربية حيث سهلت الوسائل الحديثة على المحتالين ارتكاب جرائهم بسهولة ودون ترك أي أثر أو دليل وهذا ما يصعب من العمل القضائي لأنه من الصعب العثور على هوية الجناة.

فقد أخدت جرائم النصب والاحتيال موقعاً متقدما في مصاف الجرائم الخطيرة، والتي يعاني منها المجتمع الآمن على نفسه، وماله، ومقدراته ،و قد تنوعت وسائل هذا النوع من الجرائم ولكنها مع اختلافها ،إلا إنها تتفق وغيرها في التمويه ،والخداع ،والتغرير الأمر الذي جعل هذا الجرم ينخر في المجتمع في نواحيهالاقتصادية، و التنظيمية،والاجتماعية،ويطال الفرد والمؤسسة ،والمجتمع بكليته.

كما تعتبر جريمة النصب من ضمن أكثر الجرائم تطورا و استخداما للذكاء و الدهاء و خاصة الحيلة كما إن البعض من هؤلاء المجرمين يعمل جاهدا من أجل الإيقاع بضحاياه دون حتى أن يكشف عن اسمه ، ويسعى في خلق حيل وطرق تتناسب مع التطورات والاحتياطات المبذولة، لأجل تمرير أعمالهم الإجرامية تحت غطاء يوهمون به الآخرين أن أعمالهم مشروعة.

في الوقت الراهن، الكثير منهم يستخدم الإقناع الوهمي عبر شبكات التواصل الاجتماعي و المواقع الإلكترونية ؛ للاستيلاء على أموال الناس.

ولا شك أن الازدياد المطرد ،والملحوظ في أعمال جريمة النصب ،والاحتيال يسببه استمرار الضحايا الكثيرين بالتحلي بالبساطة ،والسذاجة المترتبة على الخلل الكبير في القيم الثقافية، والتربوية، يسنده وجود نفوس شريرة لا يهنأ لها مقام، وهي ترى المال بأيدي هؤلاء البسطاء ،ولو كان من عرق جبينهم ، وكدح أيديهم.

تعتبر شبكة الانترنت اكبر وسيلة اتصال تسهل نقل المعلومات والملفات بين الأشخاص بطريقة سهلة وسلسلة وبدون آي معاناة بأي وقت وبأقل التكاليف وبالصورة والطريقة التي تحب والتي تختارها أنت, حتى أصبح العالم اليوم عبارة عن قرية صغيرة والخبر لا يبقى على إخفاءه ساعة بسبب ظهور مواقع التواصل الاجتماعي هذه الشبكات جعلت العالم أكثر سهولة في التعاملات ونقل الأخبار وعلى التعارف وبناء المصالح المشتركة بين الأفراد بأقل التكاليف وأسهل الطرق حيث أن الأفراد من خلال هذه الشبكات صاروا قادرين على إبداء آراءهم وأفكارهم وتصوراتهم وكذلك كسب ثقافات مختلفة من خلال الاطلاع على الثقافات الأخرى وبناء جسور التواصل معها حتى بات العالم مهووس بهذه البرامج ولاستطيع مفارقة أجهزة الحاسوب والهواتف.

على الرغم من هذه المميزات العديدة التي قدمها "الإنترنت" للعالم، ولكن هناك من استخدم هذه الخدمة بالصور الخاطئة ولا يخفى أيضا عن المناكفات والمؤامرات التي تحدث خلف هذه الشاشة والتي أدت إلى انتشار الكثير من الجرائم والظواهر الغريبة بين متسللي الشبكات والأنظمة المعلوماتية وبين رواد مواقع التواصل الاجتماعي ومن بين الجرائم الأكثر خطورة وانتشارا جرائم النصب والاحتيال الالكتروني والتي أصبحت أخطر من جرائم الإرهاب و غيرها , وبطرق وأشكال متنوعة ومدروسة للنصب والاستيلاء على أموال الآخرين ولعل أبرزها ما تم عن طريق مواقع التواصل الاجتماعي خاصة "فيس بوك" و"توتير"، كونه أداة سهلة للتلاعب بالآخرين لسرقة أموالهم وهذا ما أدى إلى وقوع الكثير من مستخدمين هذه المواقع فريسة الاحتيال والنصب عليهم.

تعتبر جريمة النصب عبر المواقع الالكترونية من أكثر الجرائم تطوراً حيث إن البعض من هؤلاء المجرمين يعمل بذكاء حاد ويسعى في خلق حيل وطرق تتناسب مع التطورات والاحتياطات المبذولة حتى ظهرت طرق متعددة ومتنوعة للاحتيال عبر وسائل التواصل، لأجل تمرير أعمالهم الإجرامية تحت غطاء يوهمون به الآخرين أن أعمالهم مشروعة.

إن التسويق عبر مواقع التواصل الاجتماعي من أهم الظواهر التي انتشرت مؤخرا بسبب سهولة الوصول إليها , عبر الانترنت والى المواد المطلوب شراءها إضافة إلى انخفاض الأسعار ووصول البضاعة إلى غاية بيتك كونه لا يحظى بتنظيم قانوني سوى أنه يعتبر سوق سوداء معلوماتية الرابح فيها من يكون له القدرة على التلاعب بالمعطيات المعلوماتية و نفس الأمر مع الشركات الوهمية التي تبيع الأحلام مثل الشركات التي تعرض هامش ربح محدد مسبقا من أجل الربح السريع أو الحصول على تأشيرات الدخول لدول معينة مقابل مبالغ مالية معينة و غيرها من الأساليب الاحتيالية لأخرى التي تستعمل من أجل النصب على الضحايا.

وهذه الظاهرة الخطيرة المتمثلة في جريمة النصب باستعمال التكنولوجيات و الوسائل المعلوماتية تدفع بنا إلى طرح الإشكال القانوني الأتي: هل تحظي جريمة النصب المعلوماتية بتأطير قانوني مثلها مثل جريمة النصب التقليدية ؟

و منه نطرح بعض الأسئلة الفرعية الناتجة عن الإشكال .

ماهية الجريمة المعلوماتية و جريمة النصب المعلوماتية و بم يتميز المجرم ألمعلوماتي عن غيره من المجرمين و ما هو الإطار القانوني لهذه الجريمة المستحدثة وهل هناك سبل لمكافحتها ؟

وسنحاول الإجابة على هذه الإشكاليات اعتمادا على أسلوب منطقي متسلسل من اجل إثراء الدراسة و تبسيطها من اجل تسليط الضوء عليها .

أهمية الموضوع:

من منطلق الدراسة الأكاديمية التي نسعى من خلالها إلى تسليط الضوء على المواقف القانونية الغامضة و التي هي بحاجة إلى استقصاء و تفسير حتى نقوم بالتنبيه عليها , و منه ظهرت أهمية دراسة أحد صور الإجرام ألمعلوماتي و هو النصب باستعمال الوسائل المعلوماتية أو النصب ألمعلوماتي و تتجلى أساسا في:

– تسليط الضوء على هده الجريمة المستحدثة في ضل التشريع ؛ و معرفة مدي احتواء النصوص القانونية المتعلقة بالنصب لجريمة النصب المعلوماتية ؛ كما نسعى من خلال هده الدراسة إلى إثراء الرصيد المعرفي حول هده الجرائم المستحدثة.

أسباب اختيار الموضوع:

الأسباب الذاتية:

– الرغبة في دراسة الجرائم المستحدثة

– تكوين معرفة قانونية ومعلوماتية حول الإجرام ألمعلوماتي بصفة عامة والنصب ألمعلوماتي بصفة خاصة.

الأسباب الموضوعية:

– موضوع جديد عمليا و يحتاج إلى الدراسة و الاستقصاء.

– التطرق لخبايا و الثغرات التي تتسم بها هذه الجريمة المستحدثة.

– معرفة خصوصيات هده المواضيع.

منهج الدراسة :

المنهج الوصفي: من أجل وصف الجريمة و التطرق لخصائصها و مميزاتها.

المنهج التحليلي: من أجل تحليل أساسيات الموضوع و عناصره.

الفصل الأول الإطار المفاهيمي للجريمة المعلوماتية و جريمة النصب باستعمال الوسائل المعلوماتية:

بدأت الثورة المعلوماتية نتيجة اقتران تقنيتي الاتصالات من جهة، والمعلومات وما وصلت إليه من جهة أخرى، فالثورة المعلوماتية هي الطفرة العلمية والتكنولوجية التي نشهدها اليوم، حتى بات يطلق على هذا العصر: عصر المعلومات. وتعد المعلومة أهم ممتلكات الإنسان، اهتم بها، على مر العصور، فجمعها ودونها وسجلها على وسائط متدرجة التطور بدأت بجدران المعابد والمقابر، وانتهت باختراع الورق الذي تعددت أشكاله، حتى وصل بها المطاف إلى الأقراص الإلكترونية الممغنطة.

ولد علم جديد هو علم تقنية المعلوماتيةTélématique ، وهو مصطلح يعبر عن اقتران التقنيتين، ويتكون من الجزء الأول من كلمتيTélécommunication ، وهو الاتصال عن بعد والجزء الثاني من كلمةInformation ، وتعني المعلومات، وهو علم اتصال المعلومات عن بعد[1].

هكذا جاء التقدم الفني مصحوبًا بصور مستحدثة لارتكاب الجرائم، التي تستعير من هذه التقنية أساليبها المتطورة, فأصبحنا أمام ظاهرة جديدة هي ظاهرة الجريمة المعلوماتية.

لقد تباينت الصور الإجرامية لظاهرة الجريمة المعلوماتية، وتشعبت أنواعها، فلم تعد تهدد العديد من المصالح التقليدية التي تحميها القوانين والتشريعات منذ عصور قديمة، بل أصبحت تهدد العديد من المصالح والمراكز القانونية التي استحدثتها التقنية المعلوماتية، بعد اقترانها بثورتي الاتصالات والمعلومات.

فالمصالح التقليدية التي تحميها كل التشريعات والنظم القانونية منذ زمن بعيد بدأت تتعرض إلى أشكال مستحدثة من الاعتداء بواسطة هذه التقنية الحديثة، فبعد أن كان الاعتداء على الأموال يتم بواسطة السرقة التقليدية أو النصب، وكانت الثقة في المحررات الورقية

1 – أحمد خليفة الملط ، الجرائم المعلوماتية ، دار الفكر الجامعي القاهرة ،ط2 سنة 2006 ،ص 60.

يعتدي عليها بواسطة التزوير، أصبحت هذه الأموال يعتدي عليها عن طريق اختراق الشبكات المعلوماتية، وإجراء التحويلات الالكترونية من أقصى مشارق الأرض إلى مغاربها في ثواني معدودة، كما أصبحت تلك الحقوق الثابتة في الأوعية الورقية يتم الاعتداء عليها في أوعيتها الالكترونية المستحدثة عن طريق اختراق الشبكات والأنظمة المعلوماتية، دون الحاجة إلى المساس بأية وثائق أو محررات ورقية[1].

وبعد أن كانت الحياة الخاصة للإنسان تواجه الاعتداء باستراق السمع أو الصورة الفوتوغرافية، أصبحت هذه الخصوصية تنتهك بواسطة اختراق، البريد الالكتروني والحواسب الشخصية، وقواعد البيانات الخاصة بالتأمين الصحي والمستشفيات ومؤسسات الائتمان والتأمين الاجتماعي.

أما المصالح المستحدثة، فتتمثل في استحداث مراكز قانونية أفرزتها الحياة الرقمية الجديدة، مثل حقوق الملكية الفكرية على تصميم البرامج المعلوماتية، بالإضافة إلى حقوق الملكية الصناعية، والاسم التجاري للمواقع الالكترونية المختلفة، والحقوق الناتجة عن تشغيلها والخدمات التي تقدمها للعملاء[2].

فإذا ما تأخرت القوانين والتشريعات اللازمة لمواجهة هذه الظاهرة الإجرامية، الجديدة فسوف نواجه عشوائية كتلك العشوائية العمرانية التي نتجت عن تأخر قوانين التطوير العمراني. وهو ما يقودنا إلى ضرورة التعرض إلى المفهوم القانوني الجريمة المعلوماتية في ظل التشريع الجزائري،ومن جهة أخرى نتطرق إلى جريمة النصب باستعمال الوسائل المعلوماتية و هي محور الدراسة .

وعليه فإن إعطاء صورة عامة عن الجريمة المعلوماتية، وما تثيره من إشكالات في القانون الجنائي يقتضي ضرورة التعرض للمشكلات الموضوعية والإجرائية التي يثيرها هذا

1- أمير فرج يوسف،الجرائم المعلوماتية على شبكة الإنترنت،دار المطبوعات الجامعية مصر،ب ط ،سنة 2008 ،ص 35.

2- خالد مصطفى ،فهمي النظام القانوني للتوقيع الإلكتروني في ضوء التشريعات العربية و الاتفاقيات الدولية ، دار الجامعة الجديدة ،مصر، ب .ط. س2008 ،ص 120.

النوع المستحدث من الجرائم، وعليه فسنتعرض إلى مفهوم الجريمة المعلوماتية في المبحث الأول و جريمة النصب بصفة عامة في المبحث الثاني .

المبحث الأول: الجريمة المعلوماتية و المجرم المعلوماتي:

تعد الجريمة المعلوماتية ، من أكبر التحديات التي نواجهها في عالمنا المعاصر، إن لم تكن أكبرها على الإطلاق، والحديث عن هذه التحديات يتطلب أولا إعطاء صورة عامة عن تحديد ماهيتها، قبل التعرض إلى بحث مشكلة المسؤولية الجنائية الناتجة عنها، وهو ما يدعونا إلى التعرض إلى ماهية الجريمة المعلوماتية بتعريفها و تصنيفها في مبحث أول قبل التعرض إلى مفهوم المجرم ألمعلوماتي و تصنيفاته في مبحث ثان .

المطلب الأول الجريمة المعلوماتية

يصعب الاتفاق على تعريف موحد للجريمة المعلوماتية، حيث اختلفت الاجتهادات في ذلك اختلافا كبيرا، يرجع إلى سرعة وتيرة تطور التقنية المعلوماتية من جهة، وتباين الدور الذي تلعبه هذه التقنية في الجريمة من جهة أخرى، فالنظام ألمعلوماتي لهذه التقنية يكون محلا للجريمة تارة، ويكون وسيلة لارتكابها تارة أخرى، فكلما كان البحث منصبا على الجرائم التي ترتكب ضد النظام ألمعلوماتي، انطلق التعريف من زاوية محل الجريمة بأنها الجريمة المرتكبة بالاعتداء على النظام ألمعلوماتي، أما إذا كان البحث منصبا على دراسة الجرائم التي ترتكب باستخدام التقنية المعلوماتية ارتكز التعريف على الوسيلة، وكان" كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب الآلي".

تجدر الإشارة أيضا إلى أن أهم عوامل صعوبة الاتفاق على تعريف هو أن التقنية المعلوماتية أصبحت تحل محل العديد من التقنيات السابقة كالهاتف والفاكس والتلفزيون فالمسألة لم تقتصر على معالجة البيانات فحسب، بل تعدتها إلى وظائف عديدة، مثل وظيفة النشر والنسخ، وهو ما يحتم ضرورة التفرقة بين جرائم الإنترنت وشبكات المعلومات بالمعنى الفني عن بقية الجرائم الأخرى التي يستخدم فيها الإنترنت أو الحاسب الآلي كأداة لارتكابها.

فيقصد بجرائم الإنترنت وشبكات المعلومات الدخول غير المشروع إلى الشبكات الخاصة، كالشركات والبنوك وغيرها، وكذلك الأفراد، والعبث بالبيانات الرقمية التي تحتويها شبكة المعلومات، مثل تزييف البيانات أو إتلافها ومحوها، وامتلاك أدوات أو كلمات سرية لتسهيل ارتكاب، مثل هذه الجرائم التي تلحق ضررا بالبيانات والمعلومات ذاتها، وكذلك بالنسبة للبرامج والأجهزة التي تحتويها، وهي الجرائم التي تلعب فيها التقنية المعلوماتية دورا رئيسًا في مادياتها أو السلوك الإجرامي فيها. وكذلك جرائم التجارة الإلكترونية، جرائم السب والقذف، هي جرائم تستخدم التقنية المعلوماتية، كأداة في ارتكابها، دون أن تكون جرائم معلوماتية بالمعنى الفني، وإن كان يطلق عليها الجرائم الإلكترونية[1].

نصل إلى أن الجرائم المعلوماتية لها أنواع وأصناف عديدة، وكما أسلفنا القول فإن الجريمة المعلوماتية تتميز بأنها تضم نوعين من الجرائم المستحدثة، الأول أنواعا مستحدثة من الاعتداء على مصالح محمية جنائيا بالنصوص القانونية التقليدية، أي أنه في هذه الحالات، فإن طرق الاعتداء فقط هي المستحدثة؛ لأنها تتم عن طريق التقنية المعلوماتية، بعد أن كانت ترتكب بالسلوك المادي الملموس، أما محل الاعتداء فهي المصالح المحمية أصلا حماية جنائية على مر الأزمان، والعصور كالأموال والشرف والاعتبار،

أما النوع الثاني فيضم أنواعا أخرى من الاعتداءات بالطرق المستحدثة على مصالح مستحدثة لم تعرفها القواعد التقليدية كالشبكات المعلوماتية التي تتعرض للاختراق أو التعطل أو الإغراق [2].

1- عبد الحميد بسيوني و عبد الكريم بسيوني، التجارة الإلكترونية دار الكتاب للنشر و التوزيع، مصر، ب ط سنة 2003 ص15 .

2-عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر و الإنترنت في القانون العربي النموذجي ،مصر ،ط1 ،سنة 2006 .
- الأمر 09/ 04 مؤرخ في 14 شعبان عام 1430 الموافق ل5 غشت سنة 2009 ، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته ومكافحتها.

يشهد العالم منذ منتصف القرن العشرين ثورة جديدة، أصطلح على تسميتها بالثورة المعلوماتية، وذلك إشارة إلى الدور البارز الذي أصبحت تلعبه المعلومات في الوقت الراهن . فقد أمست قوة لا يستهان بها في أيدي الدولو الأفراد.

وتعتبر المعلومات في الوقت الراهن سلعة أو خدمة تباع وتشتري، ومصدر قوة اقتصادية وسياسية وعسكرية، وذلك لارتباطها بمختلف مجالات النشاط الإنساني وتداخلها في كافة جوانب الحياة العصرية، وبات الوعي بأهميتها مظهرا لتقدم الأمم والشعوب إلا أن الجانب الإيجابي لعصر المعلوماتية لا ينفي الانعكاسات السلبية التي أفرزتها هذه الثورة، وهذه التقنية العالية، والمتمثلة في إساءة استخدام الأنظمة المعلوماتية، واستغلالها على نحو غير مشروع وبصورة تضر بمصالح الأفراد والجماعات، وبالتالي بمصلحة المجتمع كله .

حيث أدى هذا التطور الهائل إلى ظهور أنماط مستحدثة من الجرائم أصطلح على تسميتها **بالجريمة المعلوماتية**.

لقد تغيرت أنماط الجريمة، فلم تعد الاعتداءات تستهدف النفس والمال فقط، بل طالت المعلومات، وهو ما أصبح يعرف على الساحة الدولية بإجرام ذوي الياقات البيضاء. حيث يستطيع المجرمون العصريون ارتكاب أبشع الجرائم، ليس فقط دون إراقة دماء، ولكن أيضا بدون الانتقال من أماكنهم، فهذا النوع من الجرائم ليس مقصورا على منطقة، أو دولة معينة، لكنها مشكلة عالمية.

إن هذا النوع من الجرائم لا يحتاج لجهد كبير، بل ترتكب الجريمة في أمن وهدوء وهو ما جعل البعض يصفها بالجرائم الناع(Crime Soft) ، فبمجرد لمس لوحة المفاتيح يحدث دمارا وخرابا في اقتصاديات كبرى الشركات. وتتشابه الجريمة الإلكترونية مع الجريمة التقليدية في أطراف الجريمة من مجرم ذي دافع لارتكاب الجريمة وضحية، والذي قد يكون شخص طبيعي أو شخص اعتباري.

أما الاختلاف الحقيقي بين نوعي الجريمة فيكمن في أداة الجريمة ومكانها. ففي الجريمة الإلكترونية الأداة ذات تقنية عالية، وأيضا مكان الجريمة الذي لا يتطلب انتقال الجاني إليه انتقالا فيزيقيا وإنما هي جرائم تتم عن بعد، أي بدون وجود الجاني والمجني عليه في نفس المكان.

نص المشرع الجزائري على هذه الجرائم في قانون 09-04 و اصطلح على تسميته: " الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال " و عرفها بأنها : " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أية جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية" فلا يوجد اتفاق على مصطلح معين للدلالة على هذه الظاهرة المستحدثة، فهناك من يطلق عليها ظاهرة الغش ألمعلوماتي، أو الاختلاس ألمعلوماتي، أو الجريمة المعلوماتية . أو الجرائم باستعمال الوسائل المعلوماتية.

في إطار تعريف الفقه للجريمة المعلوماتية نجد أن الاتجاهات تتباين في هذا السياق بين موسع لمفهوم الجريمة المعلوماتية وبين مضيق لمفهومها.

فمن التعريفات المضيقة لمفهوم الجريمة المعلوماتية تعريفها على أنها " كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية لملاحقته وتحقيقه من ناحية أخرى".

وحسب هذا التعريف يجب أن تتوافر معرفة كبيرة بتقنيات الحاسوب ليس فقط لارتكاب الجريمة بل كذلك لملاحقتها والتحقيق فيها.

كذلك عرفها الأستاذ **'Rosemblat'** على أنها "نشاط غير مشروع موجه لنسخ أو الوصول الى المعلومات المخزنة داخل الحاسوب.أو تغييرها أوحذفها".

وفي المقابل فإن هناك تعريفات حاولت التوسع في مفهوم الجريمة المعلوماتية عرفها البعض بأنها "كل سلوك سلبي أم إيجابي تم بموجبه الاعتداء على البرامج أو المعلومات للاستفادة منها بأي صورة كانت ".

وفي تقرير الجرائم المتعلقة بالحاسوب أقر المجلس الأوروبي بقيام المخالفة (الجريمة)في كل حالة يتم فيها " تغيير معطيات أو بيانات أو برامج أو محوها أو كتابتها أو أي تدخل آخر في مجال إنجاز البيانات أو معالجتها، وتبعا لذلك تسببت في ضرر اقتصادي أو فقد حيازة ملكية شخص آخر أو بقصد الحصول على كسب اقتصادي غير مشروع له أو لشخص آخر[1]".

ودائما حسب أصحاب الاتجاه الموسع تعرف الجريمة المعلوماتية "بأنها كل سلوك إجرامي يتم بمساعدة الكمبيوتر" أو هي "كل جريمة تتم في محيط أجهزة الكمبيوتر" أو هي "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها".

بالإضافة لما سبق فقد تنوعت تعاريف مفهوم جرائم المعلوماتية أهمها: **يعرفها الفقيه الألماني كلاوس تادماين** بأنها: "كافة أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب الآلي".

ويعرفها الفقه البلجيكي بأنها: "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية، يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية، ويعد استخدام مصطلح الجريمة المعلوماتية للدلالة على الجرائم الناشئة عن استخدام الانترنت".

وقد عرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها:"الجرائم التي تلعب فيها البيانات الكمبيوترية، والبرامج المعلوماتية دورا رئيسيا".

1 – مندر الشاوي, فلسفة القانون ، مطبوعات المجمع العلمي العراقي، بغداد 1994، ص8.

وعرفت جريمة الحاسب الآلي كذلك بأنها:"جريمة تقنية تنشأ في الخفاء يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، وتوجه للنيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات" وفي محاولة تحديدها لطبيعة الجرائم المعلوماتية، ترى الباحثة هدى قشقوش أنه: "يجب أن نعترف بأننا بصدد ظاهرة إجرامية ذات طبيعة خاصة تتعلق بالقانون الجنائي المعلوماتي، ففي معظم حالات ارتكاب الجريمة ندخل في مجال المعالجة الالكترونية للبيانات" **أما مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين،** فقد تبنى التعريف الآتي للجريمة المعلوماتية: "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية" أما عن أسباب انتشار الإجرام المعلوماتي، تعد الدوافع الشخصية الخاصة بالمجرمين هي إحدى أسباب انتشار الإجرام المعلوماتي. إلى جانب الانبهار بالتقنية المعلوماتية، وانتشارها في المجتمعات الحديثة، وقد تكون الرغبة في تحقيق انتصارات تقنية هي الهاجس الأول عند استخدام الحاسبات الآلية إلى درجة تحقيق ما يسمى ""Fantasme électronique"" وبصورة أخرى هي المتعة والرغبة في قهر النظام المعلوماتي وإثبات الذات وليس بالضرورة النوايا السيئة[1].

و قد تكون هناك أسباب و دوافع مختلفة تؤدي لارتكاب الجريمة المعلوماتية منها:

– الوصول إلى المعلومات بطريقة غير شرعية، كسرقة بعض المعلومات أو الاطلاع عليها أو القيام بعملية حذفها أو تعديلها بشكل يحقق هدف المجرم.

– محاولة الوصول عن طريق الإنترنت إلى الأجهزة التي تقوم بتوفير المعلومات وتعطيلها.

– الوصول للمعلومات السرية لبعض الجهات المستخدمة للتكنولوجيا، مثل الجهات الحكومية والبنوك والمؤسسات وبعض الأفراد ومن ثم ابتزازهم بواسطتها.

1 – مندر الشاوي ،نفس المرجع، ص 10–11– 12.

– استغلال المعرفة بالتكنولوجيا و المعلوماتية في التلاعب بالمعطيات و محاولة التغلب عليها و كسر التشفير الخاص بها .

– محاولة قرصنة المواقع المعادية أو التى لا يرغب المجرم بها المعلوماتي أو تلك التي تستفزه بطريقة أو بأخرى.

– الدخول و سرقة مختلف البيانات و المعلومات و الأرصدة و غيرها من الأمور التي يسعى لتحقيقها.

–التحايل على الضحايا من خلال إيقاعهم بأساليب تدليسية مختلفة.

– كما أنها قد تكون هجمة منظمة من دولة أو منظمة ضد دولة أو منظمة أخرى لدوافع مختلفة.

الفرع الأول : خصائص الجريمة المعلوماتية:

تتميز الجريمة المعلوماتية بعدة خصائص نوجزها فيما يلي:

– إن مسرح الجريمة المعلوماتية أو الإلكترونية لا يظهر في الواقع، بل هو الفضاء الإلكتروني بأسره.

– إن الجاني والمجني عليه لا يشترط أن يكونا في مكان واحد أو دولة واحدة، عكس الجرائم العادية مثل المخدرات أو القتل يكون لها مسرح جريمة ثابت للمعاينة. فهي جرائم ترتكب عن بعد.

– مبدأ إقليمية النص الجنائي، وما يعنيه ذلك بالنسبة لجرائم الانترنت، ومدى إمكانية تطبيق القوانين الوطنية على الجرائم الواقعة بالانترنت.

– إن الجرائم المعلوماتية أو الإلكترونية قابلة للتوسع والابتكار، فهي مرتبطة في الأساس بالتقدم التقني والمعلوماتي، فكلما ظهرت تقنية جديدة ظهرت معها جرائم جديدة.

– إن جرائم الانترنت لا تعترف بالحدود الجغرافية للدول، إذ يمكن أن توصف هذه الجرائم في

هذه البيئة بأنها جرائم عابرة للدول، ذلك لأن الطابع العالمي لشبكة الانترنت، وما يرتبه من جعل معظم دول العالم في حالة اتصال دائم على الخط "On line".

إذا كانت الجريمة بصورتها التقليدية تحتاج في الأغلب إلى جهد عضلي من نوع خاص كجرائم القتل، السرقة، الاغتصاب، فإن الجرائم التي ترتكب على شبكة الانترنت لا تحتاج إلى أدنى مجهود عضلي، بل تعتمد على الدراسة الذهنية والتفكير العلمي المدروس القائم على المعرفة الجيدة بتقنيات الحاسب الآلي.

– تتسم الجرائم المتعلقة بشبكة الانترنت بالخطورة البالغة، فهي ترتكب من طرف فئات متعددة مما يصعب معرفة من هو مرتكب الجريمة، هذا ما جعل مكتب التحقيقات الفيدرالي الأمريكي يطلق عليها وصف الوباء Épidémie".

– صعوبة اكتشاف الجريمة المعلوماتية، وإذا اكتشفت فإن ذلك يكون بمحض الصدفة وغالبا لا يتم الإبلاغ عن هذه الجرائم إما لعدم اكتشاف الضحية لها، وإما خشية من عواقب محتملة عادة مثل التشهير و الابتزاز، أضف إلى ذلك أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي تم اكتشافها.

– هذه الجرائم تهدف إلى الاعتداء على الأموال المادية والمعنوية، حيث يقابل مصطلح cyber crime مصطلح cyber tribunal للدلالة على المحاكمات عبر الإنترنت.. .الخ

– الجرائم المعلوماتية تتصف بالخفاء، أي عدم وجود آثار مادية يمكن متابعتها، فهي صعبة الاكتشاف، وكذا صعوبة الاحتفاظ الفني بدليل الجريمة المعلوماتية، إذ يستطيع المجرم في زمن محدود. فضلا عن سهولة تهربه من مسؤولية هذا العمل بإرجاعها مثلا إلى خطأ في نظام الحاسب.

– يعتمد هذا النوع من الجرائم على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها والاعتماد على التمويه.

– الجرائم المعلوماتية لا تتسم كلها بالمتابعات القضائية كون ان بعض الهاكر مثلا يساعد دولته في الهجوم أو التصدي لدولة أخرى أو مجموعة تخريبية مثل ما يعرف بمجموعة " أنونيموس ".

– عدم وجود مفهوم مشترك لماهية الجريمة المعلوماتية، وعدم وجود تعريف قانوني موحد لها، ولعل السبب في ذلك يرجع إلى عدم وجود تنسيق دولي في مجال الجريمة المعلوماتية، وهذا لغياب معاهدات دولية ثنائية أو جماعية لمواجهة الجريمة المعلوماتية، أو لاختلاف مفهوم الجريمة تبعا لاختلاف النظم القانونية[1].

الفرع الثاني : أنواع الجرائم المعلوماتية :

هناك أنواع كثيرة للجرائم الالكترونية حيث لم يوضع لها معايير محددة من أجل تصنيفها و هذا راجع إلى التطور المستمر للشبكة و الخدمات التي تقدمها.

وقد تضاربت الآراء لتحديد أنواع جرائم الانترنت وتعددت التصنيفات، فهناك من عددها بحسب موضوع الجريمة ، وأخر قسمها بحسب طريقة ارتكابها.

و قد صنفها معهد العدالة القومي بالولايات المتحدة الأمريكية عام 1985 بحسب علاقتها بالجرائم التقليدية.

– **الصنف الأول** :يتمثل في الجرائم المنصوص عليها في قانون العقوبات متى ارتكبت باستعمال الشبكة .

الصنف الثاني: تضمن دعم الأنشطة الإجرامية ويتعلق الأمر بما تلعبه الشبكة من دور في دعم جرائم غسيل الأموال، المخدرات الاتجار بالأسلحة، و استعمال الشبكة كسوق للترويج غير المشروع في هذه المجالات.

الصنف الثالث : بجرائم الدخول في نظام المعالجة الآلية للمعطيات، وتقع على البيانات والمعلومات المكونة للحاسوب وتغييرها أو تعديلها أو حذفها مما يغير مجرى عمل الحاسوب.

---

1 – نسرين عبد الحميد نبيه،الجريمة المعلوماتية و المجرم المعلوماتي، منشأة المعارف,جلال حزي و شركائه،الإسكندرية 2008، ص88 .

الصنف الرابع: فتضمن جرائم الاتصال وتشمل كل ما يرتبط بشبكات الهاتف ، و ما يمكن أن يقع عليها من انتهاكات باستغلال ثغرات شبكة الإنترنت.

وأخيرا صنف الجرائم المتعلقة بالاعتداء على حقوق الملكية الفكرية ويتمثل في عمليات نسخ البرامج دون وجه حق، وسرقة حقوق الملكية الفكرية المعروضة على الشبكة دون إذن من صاحبها بطبعها وتسويقها واستغلالها بأي صورة طبقا لقانون حماية الملكية الفكرية.

إن تقسيم الجرائم الإلكترونية بما أنها ترتكب باستخدام الحاسوب كأداة أساسية، فدور الحاسوب في تلك الجرائم يكون هدفا للجريمة أو أداة لها[1].

أولا :الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي:

و هنا لا يكون النظام المعلوماتي هو محل الجريمة ، بل يكون الحاسب الآلي هو الوسيلة لتسهيل النتيجة الإجرامية باستخدام النظام المعلوماتي، و يكون الهدف من ورائها الربح بطريق غير مشروع، الاعتداء على أموال الغير ، الإعتداء على الأشخاص و سلامتهم و حياتهم الخاصة ، أو في سمعتهم و شرفهم و الاعتداء على أمن الدولة و أسرارها.

1- الجرائم الواقعة على الأشخاص:

فرغم الإيجابيات و الفوائد التي جاءت بها الشبكة المعلوماتية و التسهيلات المقدمة للفرد، إلا أنها جعلته أكثر عرضة للانتهاك ، و منها

1-1- جريمة التهديد: وهو الوعيد يقصد به زرع الخوف في النفس، بالضغط على إرادة الإنسان ، وتخويفه من أضرار ما ستلحقه أو ستلحق أشخاص له بها صلة، ويجب أن يكون التهديد على قدر من الجسامة المتمثلة بالوعيد بإلحاق الأذى ضد نفس المجني عليه أو ماله أو ضد نفس او مال الغير ، ولا يشترط أن يتم إلحاق الأذى فعلا أي تنفيذ الوعيد ،لأنها تشكل جريمة أخرى قائمة بذاتها ، تخرج من إطار التهديد الى التنفيذ الفعلي ، وقد يكون التهديد

1 – محمد ابو بكر بن يونس،الأحكام الموضوعية و الجوانب الإجرائية.الجرائم الناتجة عن استخدام الإنترنت،دار النهضة العربية، مصر،ب ط ،سنة 2004 ،ص60.

مصحوبا بالأمر أو طلب لقيام بفعل أو الامتناع عن الفعل ، أو لمجرد الانتقام ، و لقد أصبحت الانترنت الوسيلة لارتكاب جرائم التهديد ، والتي في حد ذاتها تحتوي عدة وسائل لإيصال التهديد للمجني عليه لما تتضمنه من نوافذ وجدت للمعرفة كالبريد الإلكتروني أو الويب...

1-2-**انتحال شخصية** : و هو استخدام شخصية فرد للاستفادة من ماله أو سمعته أو مكانته و لقد تميزت بسرعة الانتشار خاصة في الأوساط التجارية. و تتم بجمع قدر كبير من المعلومات الشخصية المراد انتحال شخصيته ، للاستفادة منها لارتكاب جرائمه عن طريق استدراج الشخص ليدلي بمعلوماته الشخصية الكاملة ، كالاسم، العنوان الشخصي،رقم بطاقة الائتمان للتمكن من الوصول لماله أو سمعته... عن طريق الغش.

1-3- **انتحال شخصية أحد المواقع** : و يتم ذلك عن طريق اختراق أحد المواقع للسيطرة عليه، ليقوم بتركيب برنامج خاص به هناك، باسم الموقع المشهور.

1-4- **جرائم السب و القذف:** للمساس بشرف الغير و سمعتهم، و اعتبارهم، و يكون القذف و السب كتابيا،أو عن طريق المطبوعات أو رسوم، عبر البريد الإلكتروني أو الصوتي، صفحات الويب، بعبارات تمس الشرف.

فيقوم المجرم بنشر معلومات تكون مغلوطة عن الضحية، و قد يكون شخصا طبيعيا أو معنويا ،لتصل المعلومات المراد نشرها إلى أعداد كبيرة من مستخدمي شبكة الانترنيت.

1-5- **المواقع الإباحية و الدعارة** : وجود مواقع على شبكة الانترنيت تحرض على ممارسة الجنس للكبار والقصّر،و ذلك بنشر صور جنسية للتحريض على ممارسة المحرمات و الجرائم المخلة بالحياء عن طريق صور ، أفلام ، رسائل... بالإضافة إلى انتشار الصور و مقاطع الفيديو المخلة بالآداب على مواقع الانترنت من قبل الغزو الفكري لكي بتداولها الشباب و إفساد أفكارهم وإضعاف إيمانهم.

و توفر الشبكة تسهيلا للدعارة ، عبر آلاف المواقع الإباحية ،و تسوق الدعارة و تستثمر لها مبالغ ضخمة مع استخدام أحدث التقنيات.

1-6 التشهير وتشويه السمعة: يقوم المجرم بنشر معلومات قد تكون سرية أو مضللة أو مغلوطة عن ضحيته، والذي قد يكون فرداً أو مؤسسة تجارية أو سياسية، تتعدد الوسائل المستخدمة في هذا النوع من الجرائم، لكن في مقدمة هذه الوسائل إنشاء موقع على الشبكة يحوي المعلومات المطلوب نشرها أو إرسال هذه المعلومات عبر القوائم البريدية إلى أعداد كبيرة من المستخدمين، و يُضم لهذه الجرائم كذلك تشويه السمعة،الشائعات و الأخبار الكاذبة لمحاربة الرموز السياسية و الفكرية و حتى الدينية من أجل تشكيك الناس في مصداقية هؤلاء الأفراد،و قد يكون الهدف من ذلك هو الابتزاز[1].

كل هذه الجرائم الماسة بالأشخاص تدخل ضمن الحياة الخاصة للأفراد التي كفلها القانون و في مقدمته **الدستور الجزائري حيث تنص[2] المادة 40** منه: " تضمن الدولة عدم انتهاك حرمة الإنسان .

و عليه يمكن استخدام الشبكة المعلوماتية في الاعتداء على حرمة الفرد و حياته الخاصة و حرمته، و الحريات العامة للأفراد، و هو مخالف للقانون و معاقب عليه.

2- الجرائم الواقعة على الأموال:

أصبحت المعاملات الشراء ، البيع و الإيجار تتم عبر الشبكة المعلوماتية ، و ما انجرّ عليه من وسائل الدفع و الوفاء ، فابتكرت معه طرق و وسائل للسطو على هذا التداول المالي بطريق غير مشروع ، كالتحويل الإلكتروني ، السرقة ، القرصنة و غيرها.

2-1- السرقة الواقعة على البنوك : يتم سرقة المال بالطرق المعلوماتية عن طريق اختلاس البيانات و المعلومات الشخصية للمجني عليهم ، و الاستخدام لشخصية الضحية ليقوم بعملية السرقة المتخفية ، ما يؤدي بالبنك إلى التحويل البنكي للأموال الالكتروني أو المادي إلى الجاني. حيث يستخدم الجاني الحاسب الآلي لدخول شبكة الانترنيت و الوصول إلى المصارف و البنوك ، و تحويل الأموال الخاصة بالعملات إلى حسابات أخرى. و عملية السرقة

---

[1]- محمد أبو بكر بن يونس ، نفس المرجع ،ص63-64.

- قانون رقم 16 - 01 مؤرخ في 26 جمادى الأولى عام 1437 الموافق ل 6 مارس سنة 2016 يتضمن التعديل الدستوري.

الإلكترونية كالاستيلاء على ماكينات الصرف الآلي والبنوك ، يتم فيها نسخ البيانات الإلكترونية لبطاقة الصراف الآلي ومن ثم استخدامها لصرف أموال من حساب الضحية ، أو إنشاء صفحة انترنت مماثلة جدا لموقع احد البنوك الكبرى أو المؤسسات المالية الضخمة لتطلب من العميل إدخال بياناته أو تحديث معلوماته بقصد الحصول على بياناته المصرفية وسرقتها. رسائل البريد الواردة من مصادر مجهولة التي توهم صاحب البريد الإلكتروني بفوزه بإحدى الجوائز أو اليانصيب وتطالبه بموافاة الجهة برقم حسابه المصرفي ، و الأمثلة كثيرة...

2-2- تجارة المخدرات عبر الانترنيت : تتعلق بالترويج للمخدرات و بيعها، و التحريض على استخدامها ، و صناعتها بمختلف أنواعها.

2-3- غسيل الأموال : تمارس عبر الانترنيت ، حيث استفاد الجناة ما وصلت إليه عصر التقنية المعلوماتية لتوسيع نشاطهم الغير مشروع في غسيل أموالهم ، بتوفير السرعة ، و تفادي الحدود الجغرافية، و القوانين المعيقة لغسيل الأموال ، و كذا لتشفير عملياتهم و سهولة نقل الأموال و استثمارها لإعطائها الصبغة الشرعية.

2-4- الاستعمال الغير الشرعي للبطاقات الائتمانية : رافق استخدام البطاقات الائتمانية الاستيلاء عليها باعتبارها نقود الكترونية و دلك إما بسرقة أرقام البطاقات ثم بيع المعلومات للآخرين ، من خلال الحصول على كلمة السر المدرجة في ملفات أنظمة الحاسب الآلي للضحية عن طريق الاحتيال ، و ذلك بإيهامه بحصول ربح ، فيقدم الضحية معلومات تمكن الجاني من التصرف في ماله ، أو إساءة استخدام الغير البطاقات الائتمانية، كأن يقوم السارق استعمال البطاقة للحصول على السلع و الخدمات أو سحب مبالغ مالية بموجبها من أجهزة التوزيع الآلي أو السحب باستخدام بطاقات مزورة.

2-5- الجرائم الواقعة على حقوق الملكية الفكرية و الأدبية : كذلك يكون النظام المعلوماتي وسيلة للاعتداء على حقوق الملكية الفكرية ، و ذلك بالسطو على المعلومات التي يتضمنها

نظام معلوماتي آخر، و تخزين و استخدام هذه المعلومات دون إذن صاحبها، حيث يعدّ اعتداء على الحقوق المعنوية و على قيمتها المادية.

2-**6/ قرصنة البرمجيات:** هي عملية نسخ أو تقليد لبرامج إحدى الشركات العالمية على اسطوانات وبيعها للناس بسعر أقل، و جريمة نسخ المؤلفات العلمية و الأدبية بالطرق الالكترونية المستحدثة. حيث أن المعلومة الأدبية و الفكرية ذات قيمة أدبية و مادية بالإضافة إلى براءات الاختراع التي تخول لمالكها حق معنوي و آخر مالي[1].

نص عليها المشرع في الدستور في المادة 44 :"حقوق المؤلف يحميها القانون ". بالإضافة إلى قوانين المتعلقة بحقوق المؤلف و الحقوق المجاورة ، و براءات الاختراع.

3- الجرائم الواقعة على أمن الدولة:

تقع هذه الجرائم باستعمال النظام المعلوماتي سواء للإفشاء الأسرار التي تخص مصالح الدولة و نظام الدفاع الوطني، أو الإرهاب، التجسس.. **نصت عليها المادة 394 مكر 2:** "تضاعف العقوبة المنصوص عليها في هذا القسم اذا استهدفت الجريمة الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام دون الاخلال بتطبيق عقوبات أشد".

3-1- **الإرهاب :** تستخدم المجموعات الإرهابية حالياً تقنية المعلومات لتسهيل الأشكال النمطية من الأعمال الإجرامية. وهم لا يتوانون عن استخدام الوسائل المتقدمة مثل: الاتصالات والتنسيق، وبث الأخبار المغلوطة، وتوظيف بعض صغار السن، وتحويل بعض الأموال في سبيل تحقيق أهدافهم.

و يقوم الإرهابيون باستخدام الإنترنت لاستغلال المؤيدين لأفكارهم وجمع الأموال لتمويل برامجهم الإرهابية ، والاستيلاء على المواقع الحساسة وسرقة المعلومات وامتلاك القدرة على

1- محمد أبو بكر بن يونس، نفس المرجع ،ص68 .

نشر الفيروسات، و ذلك يرجع إلى العدد المتزايد من برامج الكمبيوتر القوية والسهلة الاستخدام والتي يمكن تحميلها مجانا.

3-2- **التجسس** :يقوم المجرمون بالتجسس على الدول والمنظمات والشخصيات و المؤسسات الوطنية أو الدولية ، و تستهدف خاصة : التجسس العسكري، السياسي، و الاقتصادي ، و ذلك باستخدام التقنية المعلوماتية، و تمارس من قبل دولة على دولة ، أو من شركة على شركة ... و ذلك بالإطلاع على المعلومات الخاصة المؤمنة في جهاز آلي ، و غير مسموح بالإطلاع عليها، كأن تكون من قبيل أسرار الدولة[1].

ثانيا : الجرائم المعلوماتية الواقعة على النظام المعلوماتي:

وهي الجرائم الواقعة على النظام المعلوماتي التي قد تستهدف سواء المكونات المادية لنظام المعلومات أو برامج النظام المعلوماتي، أو المعلومات المدرجة بالنظام المعلوماتي على النحو التالي:

1- **الجرائم الواقعة على المكونات المادية للنظام ألمعلوماتي:**

و يقصد به الأجهزة و المعدات الملحقة به و التي تستخدم في تشغيله كالأسطوانات الكابلات... و الاعتداء عليها يكون بالسرقة لهذه المعدات ، أو عن طريق الإتلاف العمدي كاحراقها، ضرب الآلات بشيء ثقيل، العبث بمفاتيح التشغيل خربشة الأسطوانات لكي لا تصبح صالحة للاستعمال.

2- **الاعتداء على برامج النظام المعلوماتي:**

و يتوجب هنا معرفة و دراية ذات درجة عالية في مجال البرمجة، و تقع هذه الجرائم إما على البرامج التطبيقية أو برامج التشغيل.

1- نسرين عبد الحميد نبيه،مرجع سابق، ص 91.

البرامج التطبيقية : و هنا يقوم الجاني بتحديد البرنامج ثم التلاعب فيه للاستفادة منه ماديا،و ذلك بتعديل **البرنامج** : و يكون الهدف من تعديل البرامج اختلاس النقود ،حتى و لو كان باستقطاع مبالغ قليلة لكن لفترات زمنية طويلة لتحقيق الفائدة ، بدون إثارة الشبهات.

أما التلاعب : فيأخذ عدة أشكال ، فقد يكون عن طريق زرع برنامج فرعي في البرنامج الأصلي مثلا يسمح له الدخول غير المشروع في العناصر الضرورية للنظام المعلوماتي، حيث يصعب اكتشاف هذا البرنامج لدقته و صغر حجمه.

برامج التشغيل: و هي البرامج المسئولة عن عمل نظام معلوماتي من حيث قيامها بتنظيم و ضبط ترتيب التعليمات الخاصة بالنظام.

و تقوم الجريمة هنا عن طريق تزويد البرنامج بمجموعة تعليمات إضافية ليسهل الوصول إليها بواسطة شفرة تسمح الحصول على جميع المعطيات التي يتضمنها النظام المعلوماتي. و تأخذ شكلين هما المصيدة : و هو إعداد برنامج به ممرات و فراغات في البرنامج و تفرعات إضافية، وهنا يمكن للمبرمج استخدام البرنامج في أي وقت ، و يصبح المهيمن على النظام و على صاحب العمل.

أما تصميم برنامج: هو قيام برنامج خصيصا يصعب اكتشافه لارتكاب الجريمة و مراقبة تنفيذها.

3- الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي:

إن المعلومات المعالجة آليا هي أساس عمل النظام المعلوماتي ، لأنها ذات قيمة مادية و اقتصادية، لذلك تعد هدفا للجرائم الإلكترونية من خلال التلاعب فيها أو إتلافها.

يكون التلاعب في المعلومات الموجودة على النظام المعلوماتي بطريقة مباشرة أو غير مباشرة، فيتم التلاعب المباشر عن طريق إدخال معلومات بمعرفة المسئول عن القسم المعلوماتي، كضم مستخدمين غير موجودين بالعمل بهدف الحصول على مرتباتهم، الإبقاء على مستخدمين تركوا العمل للحصول على مبالغ شهرية، أو عن طريق تحويل لمبالغ وهمية لدى العاملين بالبنوك باستخدام النظام المعلوماتي بالبنك، و تسجيلها و إعادة ترحيلها و إرسالها

لحساب آخر في بنك آخر، بهدف اختلاس الأموال . أما التلاعب الغير مباشر ، فيتم عن طريق التدخل لدى المعلومات المسجلة بالنظام ألمعلوماتي باستخدام أحد وسائط التخزين، أو التلاعب عن بعد بمعرفة أرقام و شفرات الحسابات ، قصد التلاعب في الشرائط الممغنطة ، أو باستخدام الجاني كلمة السر أو مفتاح الشفرة ، و إمكانية تسلل الجاني إلى المعلومات المخزنة و الحصول على المنفعة المالية من مسافات بعيدة[1].

إتلاف المعلومات في مجال المعلوماتية بالاعتداء على الوظائف الطبيعية للحاسب الآلي ، و ذلك بالتعدي على البرامج و البيانات المخزنة و المتبادلة بين الحواسب و شبكاته، و تدخل ضمن الجرائم الماسة بسلامة المعطيات المخزنة ضمن النظام المعلوماتي، و يكون الإتلاف ألعمدي للبرامج و البيانات كمحوها أو تدميرها الكترونيا ، أو تشويهها على نحو يجعلها غير صالحة للاستعمال.

الفرع الثالث عناصر المعلوماتية:

تعتبر شبكة الانترنت اكبر وسيلة اتصال تسهل نقل المعلومات والملفات بين الأشخاص بطريقة سهلة وسلسلة وبدون آي معاناة بأي وقت وبأقل التكاليف وبالصورة والطريقة التي تحب والتي تختارها أنت, حتى أصبح العالم اليوم عبارة عن قرية صغيرة والخبر لا يبقى على إخفاءه ساعة بسبب ظهور مواقع التواصل الاجتماعي هذه الشبكات جعلت العالم أكثر سهولة في التعاملات ونقل الأخبار وعلى التعارف وبناء المصالح المشتركة بين الأفراد بأقل التكاليف وأسهل الطرق حيث أن الأفراد من خلال هذه الشبكات صاروا قادرين على إبداء آراءهم وأفكارهم وتصوراتهم وكذلك كسب ثقافات مختلفة من خلال الاطلاع على الثقافات الأخرى وبناء جسور التواصل معها حتى بات العالم مهووس بهذه البرامج ولاستطيع مفارقة أجهزة الحاسوب والهواتف و الحواسب اللوحية, و من هاذا المنطلق العلمي و التكنولوجي لشبكة المعلومات آو شبكة الإنترنت و الأجهزة التكنولوجية المرتبطة بها لى غرار الحواسيب و

[1]– محمد أبو بكر بن يونس ،مرجع سابق،ص 69 – 70

الهواتف الذكية التي تسمح بولوج أي شخص لهذا النظام دون رقابة آو قيود فعلية مكنت بعض المجرمين من الاستثمار في هادا الوضع و هاذا من خلال تنفيذ أعمالهم الإجرامية المختلفة و منها جريمة النصب.

أولا: جهاز الحاسوب (الحاسب الآلي):

يعتبر جهاز الكمبيوتر أو الحاسب الآلي عبارة عن آلة أو جهاز له القدرة على استقبال البيانات المرسلة إليه و معالجتها إلى معلومات مهمة و ذات قيمة و يخزنها في أجهزة تخزين مختلفة و أيضا قادر على تبادل المعلومات و النتائج مع أجهزة أخرى متوافقة معه.

حيث يتم برمجة الحاسوب على القيام بعمليات منطقية و حسابية بشكل أسرع و آلي أكثر من البشر، و تقوم أيضا الحواسيب بتشغيل البرمجيات الخاصة مثل أنظمة التشغيل المختلفة مثل ويندوز و غيرها بحيث تقوم أنظمة التشغيل بتوضيح كيفية تشغيل المهمات و الأوامر للحاسوب .

- مكونات أجهزة الحاسوب:

يمكن تقسيم مكونات الحاسوب إلى قسمين رئيسيين، وهما العتاد والبرمجيات، وينقسم كل منهما إلى عدة أقسام.

العتاد – Hardware :

العتاد هو ترجمة الكلمة الإنجليزية Hardware، ويقصد بها الأجزاء الإلكترونية الصلبة أو الملموسة المكونة لجهاز الحاسوب، ويمكن تقسيم العتاد إلى عدة مجموعات كالتالي:

وحدة المعالجة المركزية – Central Processing Unit تسمى أحيانا بـ البروسيسور أو المعالج، و تعتبر وحدة المعالجة المركزية من أهم مكونات أي جهاز حاسوب، فهي الوحدة المسئولة عن تنفيذ الأوامر البرمجية، وإجراء العمليات الحسابية والمنطقية في أي جهاز كمبيوتر. ومن أشهر الأنواع المستخدمة في أجهزة الحاسوب الشخصية أو الخوادم هي معالجات إنتل (Intel) و معالجات إيه إم دي (AMD)، ويمكنك معرفة المزيد من خلال مقالة وحدة المعالجة المركزية – Central Processing Unit.

1-2الذاكرة الأساسية / الداخلية – Internal Memory : وهي عبارة عن شريحة إلكترونية، تستخدم في تسجيل وقراءة البيانات، ويوجد منها نوعان في جهاز الكمبيوتر وهم:

1-3- ذاكرة الوصول العشوائي–Random Access Memory: وتكتب إختصارا RAM وتستخدم في تخزين البيانات بشكل مؤقت حتى تتمكن وحدة المعالجة المركزية من قراءة و/أو تخزين البيانات بشكل مباشر وسريع، وتسمى بالعشوائية بسبب أن وحدة المعالجة المركزية تتمكن من قراءة البيانات المسجلة على أي جزء منها بنفس السرعة، وفي هذا النوع من الذاكرة يتم فقد البيانات المسجلة عليه عند إغلاق الجهاز، أي أنها ذاكرة متطايرة أو مؤقتة (Volatile).

1-4- ذاكرة القراءة فقط – Read Only Memory:تسمى اختصارا ROM، وهي نوع خاص من الذاكرة العشوائية، ولكنها للقراءة فقط، حيث لا يمكن لوحدة المعالجة المركزية تغيير أي بيانات مسجلة عليها، ولكن يمكن لوحدة المعالجة المركزية أن تقرأ منها بسهولة، وهي أيضا غير متطايرة (Non-Volatile) فالبيانات المسجلة عليها لا يمكن مسحها أو تغييرها، وتستخدم في أجهزة الحاسوب حتى تمكن وحدة المعالجة المركزية من التعرف على مكونات الحاسوب وأين يجد نظام التشغيل.

1-5- وسائط التخزين – Storage Devices: وهي عبارة عن أجهزة إلكترونية يتم توصيلها بجهاز الحاسوب لأغراض حفظ البيانات في حالة إنقطاع التيار الكهربائي، ومن أمثلتها القرص الصلب (Disk Drive Hard)، و القرص المدمج (Compact Disk).

1-6- أجهزة الإدخال والإخراج – Input/Output Devices :وهي عبارة عن أجهزة إلكترونية يتم توصيلها بجهاز الكمبيوتر بغرض إدخال البيانات إلى الجهاز أو عرض مخرجات النظام ومن أمثلة أجهزة إدخال البيانات، لوحة المفاتيح (Keyboard)، الماسح الضوئي (Scanner) والفأرة (Mouse)، أما أمثلة أجهزة الإخراج فهي الشاشة (Monitor)، والطابعة (Printer).

ويتم توصيل كل هذه الأجهزة والمكونات من خلال اللوحة الأم (Mother Board) وبالطبع يوجد أيضا أجزاء مكملة لعمل الحاسوب كـ مزود الطاقة (Power Supply)، وغيره من الأجزاء اللازمة لعمل جهاز الحاسوب.

ثانيا: البرمجيات – Software:هي عبارة عن إشارات كهرو–مغناطيسية قابلة للتطبيق المباشر على الحواسيب و الهواتف الذكية قادرة على معالجة البيانات و المعلومات المدخلة فيها. تقوم بتنفيذ مجموعة من الأوامر و التعليمات.

وهنا يتم تصنيف البرمجيات إلى قسمين رئيسيين،برمجيات النظام(System Software) و برمجيات التطبيقات (Application Software)

1–2 برمجيات النظام – System Software :وهي عبارة عن مجموعة من الملفات التي تحتوي على الأوامر البرمجية الضرورية واللازمة لتشغيل جهاز الكمبيوتر، ومن أمثلتها أنظمة التشغيل (Systems Operating)، تعريفات مكونات الكمبيوتر (Device Drivers)، وبعض الخدمات الأخرى بالإضافة إلى مترجمات لغات البرمجة المختلفة.

2–2 برمجيات التطبيقات–Application Software:أحيانا يتم إختصارها بـ البرامج– Programs وتعتبر برمجيات التطبيقات (البرامج) هي الواجهة لجهاز الحاسوب والتي تمكن مستخدم الكمبيوتر من التعامل معه، وتنفيذ المهمات من خلال الحاسوب، والبرامج هي عبارة عن مجموعة من الأوامر البرمجية التي يتم تطويرها من قبل مبرمج أو شركات برمجة لتقوم بوظائف محددة، فعلى سبيل المثال يوجد برامج لمعالجة النصوص مثل برنامج Word، ويوجد برامج لمعالجة الصور مثل برنامج Photoshop، والعديد من التطبيقات محددة المهام الأخرى.

وهنا يجب التنويه على أن البرامج تعتمد بشكل ما على الأوامر الموجودة في أنظمة التشغيل لكي تتمكن من العمل على جهاز الحاسوب.

شبكات الانترنت مجموعة من أجهزة الحاسوب المتصلة ببعضها بمكونات وأجهزة وبرمجيات لنقل وتبادل المعلومات بسهولة مع القدرة على التحكم بحيث يتم النقل بأمان

لمستخدمي الشبكة فقط يمكن تنفيذ شبكة في أى مكان شركة.. مصنع..مؤسسة بطرق توصيل وتصميمات هندسية مختلفة نتعرف على أنواع الشبكات و مميزاتها ومكوناتها.

ثانيا الهواتف الذكية :

الهواتف الذكية هو مصطلح يطلق على الهواتف التي تعمل بنظام تشغيل معين، حيث إنها تشبه الكمبيوتر الصغير، وتمكن مستخدميها من استخدام مختلف أنواع التطبيقات، واستخدام الإنترنت، بالإضافة إلى الخدمات الهاتفية، كالرسائل القصيرة، والاتصال، والكاميرا، مما ساهم في تلبية حاجات الناس، وزيادة القدرة على التواصل بينها، ومن مزايا الهواتف الذكية، أنّها تحتوي على نظام تشغيل قادرا على استغلال مميزات الهاتف التقنية، ومعالج، وذاكرة مسؤولة عن حفظ المعلومات والبيانات، والشاشة التي قد تكون شاشة لمس، أو شاشة عادية، بالإضافة إلى التطبيقات الموجودة على المتجر، والمثبّتة على الجهاز، وفي هذا الفرع سنتطرق على الهواتف الذكية وأنظمتها و نقصد بها الهواتف و الألواح الالكترونية على حد سواء كونها تعمل بنفس الأنظمة و البرامج.

-أنواع أنظمة تشغيل الهواتف:Androïde :

- النظام مفتوح المصدر مما يتيح للشركات المنتجة للهواتف استخدام النظام و تركيبه على أجهزتها مما يعطيه انتشار كبير و ضخم بشكل سريع.

- امكانية التعديل الجذري على النظام من قبل المطورين و توفير مزايا أكثر و حل المشاكل بحسب المطور.

- واجهة مستخدم مختلفة من شركة لأخرى مما يعطي إحساس لدى المستخدم أن الجهاز مختلف عن الآخر من الشركة الأخرى مثل Samsung و htc .

- دمج خدمات غوغل في نظام اندرو يد مما يعطي مستخدم خدمات غوغل امتياز أفضل

:Windows Phone

–نظام واعد جدا حيث سيصدر الإصدار 8 للهواتف و الذي يحتوي على واجهة ميترو الرائعة الموجودة على أجهزة ويندوز اللوحية و على أجهزة الكمبيوتر لاحقا.

– التوافق التام و التكامل بين هواتف الويندوز فون و الأجهزة اللوحية و الكمبيوترات التي تعمل بنفس النظام و كذلك التوافق مع ال XBOX و شبكته الاجتماعية.

– وثوق المطورين و المستخدمين بإمكانيات شركة مايكروسوفت و أنها تمشي على خطط واضحة و قوية.

– اهتمام مايكروسوفت بسوق التطبيقات و توفير الأدوات للمطورين و تسهيل الخدمات لهم مثل أبل.

– الاشتراك مع نوكيا ذات القاعدة الجماهيرية الكبيرة جداً للتسويق لنظامها عبر أجهزتها.

نظام IOS:

– استقرار النظام القوي جدا و صموده و لا يتطلب مواصفات قوية لعمل بكفاءة بل ما تضعه أبل هو ما يحتاجه النظام دون الإفراط بالمواصفات و بالتالي زيادة السعر على المستخدم (فكرة المثال في بداية الموضوع تفسرها هذه النقطة)

– الدعم القوي لأجهزة IOS و التوافق و التكامل التام مع جميع أجهزة أبل من أجل تسهيل حياة المستخدم، و هناك عدة أنواع تابعة لنفس النظام منها iPod – i Phone – i Pad –iMac بحساب واحد متكامل و إمكانية إدارة ملفاتي بين هذه الأجهزة بكل سهولة.

– العمر الافتراضي للجهاز طويل جدا و يكفي المستخدم إلى ثلاث سنوات أو أربع مع الدعم المستمر للجهاز، ولعل الآيفون 3GS أكبر مثال على هذا الأمر. بعكس أجهزة الأندوريد التي لا تتجاوز سنة بسبب قلة الدعم و طرح أجهزة جديدة كل فترة قصيرة.

– المواد المصنعة منها أجهزة أبل فاخرة و ذات جودة عالية و مميزة.

ثالثا: شبكات الانترنت:

تلعب عاملا رئيسيا في الحياة اليومية حيث تدخل في جميع المجالات والتعاملات وخصوصا **مجال المعاملات النقدية والبنكية وإدارة الشركات و غيرها :**

– و ظهرت بكثرة في **الحياة الترفيهية** حيث جذبت ملايين المستخدمين من هواة مواقع التواصل الاجتماعي والألعاب الترفيهية.

– مجالات تبادل المعلومات وعمل الأبحاث والتعلم عن بعد وإدارة الأعمال.

– مجال الأنظمة الأمنية وكاميرات المراقبة و شاشات العرض والتسوق الالكتروني.

– **تعريف شبكة الانترنت:**هي عبارة عن مجموعه من أجهزة الكمبيوتر متصلة ومترابطة مع بعضها البعض عن طريق مكونات وأجهزة وبرمجيات ضمن شروط وقواعد تسمى البروتوكولات.

مما يسمح بتبادل وانتقال المعلومات عبر الشبكة ومشاركتها.

– تعمل شبكات الانترنت بعدة طرق سلكية وهى التي يتم توصيلها بأسلاك مخصصه لنقل البيانات والمعلومات.

– تعمل بطريقة لاسلكية حيث فيها لا يتم توصيل أسلاك وتعمل من خلال أجهزة مزودة "بالواي فاي" ترسل وتستقبل البيانات بدون الحاجة إلى أسلاك.

و أما الإنترنت فتعرف بأنها وسيلة اتصال بين الناس عن طريق استخدام الحاسوب".

– **أنواع شبكات الانترنت:** تتعدد أنواع الشبكات وتقسم إلى عدة أقسام منها ما تم تقسيمه حسب التوزيع الجغرافي ومنها ما يتم تقسيمه حسب طريقة التصميم ومنها ما يتم تقسيمه حسب علاقة العمل ونوعه

– **شبكات التوزيع الجغرافي لشبكات الانترنت نوعان:** شبكات محلية وتختصر في **LAN** وهي تكون عبارة عن شبكة تربط عدة أجهزة كمبيوتر مع بعضها البعض في نطاق منطقة محددة ومحدودة وصغيرة نسبيا.

مثل شبكة انترنت في عمارة معينة أو مصنع معين أو عدة بنايات مرتبطة ببعضها البعض

– تتميز الشبكة المحلية LAN أنها منتشرة وتعمل بكفاءة وعليها إقبال في الاستخدام من قبل الشركات والمصانع والمنشآت التجارية.

– كما أنها ارخص في الاستخدام وقليلة التكلفة عن غيرها من الشبكات

– أنها تؤدى عملها وتنجز الغرض الذي أنشئت من اجله بكفاءة وفاعلية كبيرة

– **شبكة الانترنت ذات المجال الواسع WAN :** وهى عبارة عن شبكات تقوم على ربط مساحات كبيره و واسعة من البلدان والمدن والمحافظات والدول أيضا و تعد الأكثر استخداما حول العالم.

– تربط الأفراد والشركات والمؤسسات ببعضها البعض.

– تعمل على نقل البيانات والمعلومات بحريه مطلقه مما جعلها ثاني أكبر شبكة في العالم بعد شبكة الهاتف النقال.

– **حسب طريقة التصميم الهندسي :** يوجد العديد من تصميمات شبكات الحاسوب حيث يتميز كل تصميم بخصائص تميزه عن غيره

– **الشبكة الخطية:** وهى شبكة انترنت تصل بين جهازين أو أكثر من أجهزة الكمبيوتر أو الحاسوب المحمول على نفس الخط.

– وتتميز الشبكة الخطية أنها بسيطة وليست معقده.

– سهلة التركيب حيث يتم تركيبها في وقت قصير.

الشبكة النجمية: يتكون من عدة أجهزة ووحدة تحكم تقوم بالسيطرة على الشبكة.

– وتتميز بأنها إذا ما حدث عطل في جزء منها لا تؤثر على باقي الأجزاء.

– تستطيع بسهولة الكشف عن أماكن الخلل وسهولة إصلاحها.

– **من حيث طريقة التوصيل:** يمكن ربط الأجهزة بطريقة سلكية أو لاسلكية.

الطريقة السلكية: يتم توصيل الأجهزة باستخدام الأسلاك.

الطريقة اللاسلكية : تعد من أحدث وأهم شبكات الانترنت وانتشرت بطريقة سريعة لسهولة استخدامها وتكوينها حيث تعمل دون الحاجة إلى أسلاك أو كابلات وهى متوفرة في البيوت والشركات وفى كل المجالات.

مكونات شبكات الانترنت:

– أجهزة كمبيوتر أو حاسوب محمول وهى من أهم المكونات حيث لا تعمل بدونها

وظهرت حاليا بعض البدائل مثل أجهزة الهواتف الجوالة الحديثة التي انتشرت بكثرة الآن وتعمل على الاتصال بشبكات الانترنت.

– المرسل للبيانات وهو الفرد أو الجهة أو المؤسسة المسؤولة عن إرسال البيانات والمعلومات للأفراد عبر الشبكة.

– المستقبل وهو الفرد أو المجموعة أو الشركة أو المؤسسة التي ترسل لها البيانات أو المعلومات وتقوم باستقبالها

– وسيط من الكابلات أو أجهزة النقل اللاسلكية "الواى فاى" التي تقوم بدور الوسيط الذي ينقل المعلومات

– والمهم أيضا البرامج التي تقوم بإدارة العمل بين المرسل والمستقبل للبيانات والمعلومات

يمكنك تنفيذ شبكة انترنت خاصة لمنزلك أو شركتك أو مصنعك أو أي مكان عمل

كما يمكنك استخدام مقوي شبكة "الواى فاى" وإرسال الإشارات لأبعد مدى لتغطية أكبر.

و في هادا الشكل الحالي و المتطور جدا نظام المعلوماتية و شبكات الاتصال جعل مكن فئة المجرمين المعلوماتيين من ارتكاب جرائمهم بسهولة أكبر و منها جريمة النصب المعلوماتية.

المطلب الثاني :المجرم المعلوماتي

لا شك أن الشخص الذي يرتكب الفعل غير المشروع، ويتعدى فيه على حق من حقوق الغير، يعد في نظر القانون مجرما ويتعرض للعقاب إذا ما اقترف جريمته و هادا لعمومية و تجريد القاعدة القانونية ، وعليه يعتبر المجرم المعلوماتي كغيره من المجرمين أهلا لتحمل العقاب في حال اكتشاف و إثبات كما يطبق عليه مختلف الظروف القانونية و القضائية لإجرامه من حيث الظروف التي دفعته لارتكاب جريمته وأسبابها وصفاتها. إذا كان المجرم المعلوماتي يرتكب جرائمه وهو يمارس وظيفته في مجال الحواسب الآلية، فلا بد أن يكون إنسانا اجتماعيا، يقوم بواجباته ويمارس حقوقه الاجتماعية والسياسية، دون أي عائق في حياته العملية. ولابد أن يكون محترفا يتمتع بقدر كبير من الذكاء. ويمكن حصر سمات المجرم المعلوماتي فيما يلي:

الفرع الأول : سمات المجرم المعلوماتي :

يمكن حصر سمات المجرم المعلوماتي فيما يلي:

أولا:المجرم المعلوماتى مجرم متخصص:

قد تبين في عديد من القضايا أن عددا من المجرمين لا يرتكبون سوى جرائم الكمبيوتر أي أنهم يتخصصون في هذا النوع من الجرائم، دون أن يكون لهم أي صلة بأي نوع غير الجريمة المعلوماتية فهو مجرم في الغالب متخصص في هذا النوع من الإجرام.

ثانيا: المجرم المعلوماتى مجرم عائد إلى الإجرام:

يعود كثير من مجرمي المعلومات إلى ارتكاب جرائم أخرى في مجال الكمبيوتر انطلاقا من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم و تقديمهم إلى المحاكم لينتهي بهم الأمر كذالك في المرة التالية إلى تقديمهم إلى المحاكمة.

ثالثا: المجرم المعلوماتى مجرم محترف:

يتمتع المجرم المعلوماتى باحترافية كبيرة في تنفيذ جرائمه، حيث أنه يرتكب هده الجرائم عن طريق الكمبيوتر الأمر الذي يقتضى الكثير من الدقة والتخصص.

رابعا: المجرم المعلوماتى مجرم غير عنيف:

المجرم المعلوماتى من المجرمين الذين لا يلجئون إلى العنف بتاتا في تنفيذ جرائمهم وذلك لأنه ينتمي إلى إجرام الحيلة فهو لا يلجأ إلى العنف في ارتكاب جرائم وإلى جانب ما تقدم فالمجرم المعلوماتى مجرم ذكى, فضلا عن أنه متكيف اجتماعيا، أي لا يناصب أحد العداء وأيضا يتمتع بالمهارة والمعرفة و بالتالي قد تجده في الواقع بشوش و مسالم بينما يكون مجرم خطير عن طريق الحاسب .

خامسا :المجرم المعلوماتي مجرم دكي:

إن الإجرام المعلوماتي ينتمي إلى ما يمكن أن نطلق عليه تقنيات التدمير الناعمة، وبمعنى آخر يكفي أن يقوم المجرم المعلوماتي بالتلاعب في بيانات وبرامج الحاسب الآلي بمحو أهذه البيانات أو تعطيل استخدامها، فهو يحاول أن يحقق أهدافه بهدوء. و يتطلب كثيرا من الدقة والتخصص في هذا المجال للتوصل إلى التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر كما يحدث في البنوك مثلا. فالشخص القادر على فعل كل هادا بكل تأكيد ليس في زمرة الأغبياء.

سادسا المجرم المعلوماتي هو إنسان اجتماعي بطبعه:

يمارس عمله في المجال المعلوماتي أو غيره من المجالات الأخرى، وتطبيقا لذلك فكثير من جرائم المعلوماتية ترتكب بدافع النصب أو الحسد أو بدافع اللهو أو لإظهار مدى ما يتمتع به من قدرة على التفوق في مواجهة أمن الأنظمة المعلوماتية[1].

الفرع الثاني: خصائص المجرم المعلوماتي:

يتميز المجرم المعلوماتى كذلك بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين و هي موضحه كالأتي:

أولا: المجرم المعلوماتي على قدر كبير من المعرفة التقنية:

تميز المعرفة مجرمي المعلوماتية، حيث يستطيع المجرم المعلوماتي أن يكون تصورا كاملا لجريمته، ويرجع ذلك إلى أن المسرح الذي تمارس فيه الجريمة المعلوماتية أنظمة مماثلة وذلك قبل تنفيذ الجريمة .

ثانيا: المجرم المعلوماتي لديه الباعث :

الباعث وهو الرغبة في تحقيق الربح المادي بطريقة غير مشروعة ويظل هو الباعث الأول وراء ارتكاب الجريمة المعلوماتية ويرى البعض أيضا ما يخالف ذلك في أن الفضول و إثبات الذات.

كما قد يكون الباعث هو الانتقام من رب العمل، وأيضا مجرد الرغبة في قهر نظام الحاسب واختراق حاجزه الأمني.

ثالثا: يتمتع المجرم المعلوماتي بقدر من المهارة :

[1] نسرين عبد الحميد نبيه , مرجع سابق ص120

يتطلب تنفيذ الجريمة المعلوماتية قدرا من المهارة يتمتع بها الفاعل، والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة الآخرين، وهذه ليست قاعدة ثابتة في أنه لابد أن يكون المجرم المعلوماتى على قدر كبير من العلم ,وهذا ما أثبته الواقع العملي أن هناك من أنجح مجرمي المعلومات.

رابعا: يمتلك المجرم المعلوماتي الوسيلة:

ويراد بها الإمكانيات التي يحتاجها المجرم المعلوماتى لإتمام جريمته.هذه الوسائل قد تكون في أغلب الأحيان، وسائل بسيطة وسهلة الحصول عليها خصوصا إذا كان النظام من الأنظمة غير المألوفة، فتكون هذه الوسائل معقدة وعلى قدر من الصعوبة.

خامسا: .يمتلك المجرم المعلوماتي السلطة :

الخاصة بالدخول إلى النظام الذي يحتوى على المعلومات وأيضا قد تكون السلطة عبارة عن حق الجاني في الدخول إلى الحاسب الآلي وإجراء المعاملات، كما أنه يقصد بالسلطة الحقوق والمزايا التي يتمتع بهاالمجرم المعلوماتى والتي تمكنه من ارتكاب جريمته، فكثير من مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشرة على محل الجريمة عن طريق الحاسب.

سادسا: المجرم المعلوماتي يمتلك خيال نشط وحب انتحال الشخصيات.

سابعا : له شعور أنه فوق القانون.

ثامنا: المجرم المعلوماتي لديه حب المخاطرة والتلاعب[1].

الفرع الثالث: الأصناف المختلفة للمجرم المعلوماتي:

أولا: المخترقون Hackers : هم الأشخاص الذين يستخدمون مهارات كمبيوتر متقدمة للهجوم على أجهزة الكمبيوتر,ولكن ليس لديهم أي نوايا خبيثة وإنما لكشف العيوب.

[1] – نسرين عبد الحميد نبيه، مرجع سابق، ص 201 . [1]

ثانيا: القراصنة Crackers :هم الأشخاص الذين ينتهكون أمن النظام ولديهم نوايا خبيثة ,كذلك لديهم مهارة متقدمة بأجهزة الكمبيوتر والشبكات والمهارات اللازمة لتدمير أو للولوج أي موقع و تهكيره.

ثالثا :الأطفال أو المراهقون العابثون Kiddies Script :هم أشخاص ليسو ماهرين كثيرا ويقومون باختراق أجهزة الكمبيوتر باستخدام برامج اختراق يحملونها من الإنترنت .

رابعا: المتجسسون Spies :هم أشخاص يستهدفون أجهزة معينة ليس بشكل عشوائي ولذلك لسرقة معلومات معينة أو تدمير أجهزة معينة وغالبا ما تكون أهدافهم مدروسة مسبقا .

خامسا:الموظفون :Employees و يعتبرون من أكبر التهديدات الأمنية التي تهدد الشركات فهم يقتحمون أجهزة شركاتهم لعدة أسباب: منها عرض الضعف الموجود في نظام عندما ينوي العودة للعمل في شركاتهم.[1]

و يمكن تقسيمهم إلى :

5-**1 الموظفون الساخطون على مؤسساتهم:** يقومون باستخدام الكمبيوتر لمسح بعض المعلومات الخاصة بالشركة أو المؤسسة، كطريقة للانتقام من مؤسساتهم لأسباب يعرفها مرتكب هذا الفعل.

5-2 الموظفون العاملون في مجال الأنظمة المعلوماتية: نظرا لأن النظام المعلوماتي هو مجال عملهم الأساسي، ونظرا للمهارات والمعرفة التقنية التي يتمتعون بها، فإنهم يقترفون بعض الجرائم المعلوماتية التي يمكن أن تحقق أهدافهم الشخصية، ومنها الكسب المادي، وهم يمثلون الغالبية العظمى من مرتكبي تلك الجرائم[2] .

سادسا: الإرهابيون:terrorists Cyber :هم أشخاص متخصصون ولديهم مهارات عالية غالبا ما يهددون البنية التحتية لأجهزة الكمبيوتر والشبكات ليسببوا الذعر والمهاجمة و خلق إشاعات كاذبة عن جهات معادية لهم ,ويعتبر الإنترنت بحد ذاته من أهم أهدافهم.

---

1 – نسرين عبد الحميد نبيه, نفس مرجع ص 209.

2 – محمد ابو بكر بن يونس مرجع سابق ص 79 .

بسبب انتشار الجرائم الإلكترونية على نطاق واسع من العالم فقد وضعت عقوبات صارمة لكل من يحاول استخدام هذه التقنية لغرض سيئ ويحاول التعدي على نظام مكافحة جرائم المعلوماتية[1].

المبحث الثاني جريمة النصب التقليدية و جريمة النصب المعلوماتية :

المطلب الأول مفهوم جريمة النصب التقليدية:

لم يعرف المشرع الجزائري جريمة النصب بينما الفقه يعرفها بأنها الاستيلاء على مال الغير بطريق الحيلة بنية التملك أو الاستيلاء على مال منقول مملوك للغير , بناء على الاحتيال بنية تملكه و الشخص الذي يمارس ذلك يسمى النصاب أو المحتال .

ويعرف الاحتيال بأنه فعل إدعائي كاذب معزز بمظاهر خارجية يمارسها المحتال لكي يستولي على مال الغير .

تعتبر جريمة النصب من أهم الجرائم التي يعاقب عليها القانون الجنائي , فقد أصبح تجريم الكذب أو تغيير الحقيقة من أهم الأمور التي تعتني بها كافة التشريعات الجنائية المعاصرة و هذا راجع إلى طبيعة هذه الجريمة التي يلجأ فيها الجاني إلى أساليب ووسائل احتيالية توقع المجني عليه في غلط يدفعه إلى أن يسلم ما يملكه للجاني طواعية و اختيار دوم مقاومة , وغالبا ما يكون للمجني عليه دور فيها كأن يكون طعمه هو الذي جعله يقع ضحية للجاني أو أن سذاجته جعلته فريسة سهلة أمام الجاني الأمر الذي يدفعه إلى عدم الإبلاغ عنها.

وبالتالي فإن السبب الرئيسي للازدياد الملحوظ لجريمة النصب هو بسبب استمرار الضحايا الكثيرين بالتحلي بالبساطة و السذاجة من جهة و التحلي بالطمع من جهة أخرى , كما أن السلوك الإجرامي أصبح يتنوع بحيث يغطي كافة المجالات ويعد أكثر خطورة و إضرار من الشخص الطبيعي , فهو شخص جنائي مسئول لتمتعه بالإرادة والإدراك و التمييز ويشهد الواقع

[1] نسرين عبد الحميد نبيه,ص210

أنه فاعل نشط جنائيا بل و أقدر و أخطر جنائيا و تتعاظم صفته الجنائية بتعاظم دوره و إمكانياته الهائلة وتقنيته و تعقيد وسائله و ضخامتها .

الفرع الأول الأصل التجريمي لجريمة النصب :

لم يكن الحصول على مال الغير بالاحتيال معروفا كجريمة مستقلة في القانون الروماني فقد كان أحد صور جريمة سلب مال الغير التي تشمل أيضا السرقة و خيانة الأمانة فالنصب كجريمة مستقلة لم يبرز مستقلا إلا بعد قيام الثورة الفرنسية حيث كانت في ظل كل من القانون الفرنسي و القانون الروماني القديم مختلطة بجريمة السرقة وكان أول نص خاص بجريمة النصب في 1791 الذي أتت به الثورة الفرنسية .

الفرع الثاني خصائص جريمة النصب وتمييزها عن الجرائم الشبيهة لها:

إن جريمة النصب لها خصائص معينة تشترك في البعض منها مع الجرائم الأخرى الشبيهة لها و هي خصائص عامة و لها خصائص أخرى خاصة تتميز بها عن الجرائم الأخرى بما فيها جرائم الأموال الشبيهة بالنصب.

أولا: خصائص جريمة النصب :

يتصف الاحتيال من الواجهة القانونية بعدة خصائص فهو من جهة يقوم على الكذب و تغيير الحقيقة فالمناورات الاحتيالية التي تكون الجريمة من شأنها تشويه الحقيقة في ذهن المجني عليه بما يحمله على القيام بتسليم ماله إلى الجاني طواعية و اختيارا من جهة ثانية هي من جرائم الاعتداء على المال التي تمثل المساس بحق الملكية الوارد على المنقول .

إن جريمة النصب تمثل اعتداء على حرية الإرادة أي تصيب إرادة المجني عليه بعيب الرضا وهي أيضا جريمة مقصودة تتطلب قصدا جنائيا عاما يتمثل بالعلم بكافة عناصر الجريمة و اتجاه إرادة الجاني لتحقيق الجريمة , وقصدا جنائيا خاصا يتمثل في نية تملك الشيء محل الجريمة كما أن جريمة النصب يمكن أن تقع بطريقة الاشتراك ألجرمي إضافة إلى أن الشروع فيها مجرم و معاقب عليه[1] .

ثانيا: التمييز بين الاحتيال و المصطلحات ذات الصلة:

أ- التمييز بين الاحتيال و السرقة:

طبقا للنص المادة 350 من قانون العقوبات الجزائري فإن جريمة السرقة تتحقق بنزع الشيء من حيازة المجني عليه ونقله إلى حيازة الجاني دون علم و رضا المجني عليه على عكس جريمة النصب فإن الجاني يتلقى المال من المجني عليه بإرادته غير أن هذا الأخير مشوب بعيب الغلط , كما أنه في جريمة السرقة يعتمد الجاني على جهد جسماني للاستيلاء على المال المسروق بينما في جريمة النصب يعتمد الجاني على المجهود المعنوي حتى يصدقه المجني عليه.

ب- التمييز بين الاحتيال و التزوير :

إن وسائل الاحتيال تنطوي على أكاذيب لتغيير الحقيقة ولما كان جوهر التزوير تغيير الحقيقة فكثيرا ما يختلط الاحتيال بالتزوير , كما أم الاحتيال قد يشتبه مع التزوير في استعمال المحتال أوراق أو مستندات مزورة لتأييد أكاذيبه في الاستيلاء على مال الغير .

وللتفرقة بين الجريمتين فإن كل من الفقه و القضاء ذهب إلى القول أن الأكاذيب التي يستعملها الجاني ويتوصل بها إلى الاستيلاء على مال الغير لم تدول في المحرر. ففي هذه الحالة يعد الفعل احتيالا و لا يعد تزويرا وقد تكون الأكاذيب الواردة في المحررات كافية

[1] - محمد عبد الحميد مكي ،العلاقة بين الاحتيال و تسليم المال في قانون العقوبات ، منشورات جامعة طنطا، 1995 ،ص 130 .

لاعتبار الفعل احتياليا إذا كان المحرر الذي استعان به الجاني للاحتيال على الغير صحيحا لا تغيير فيه .

خلاصة القول أن كلا من المحتال و المزور يقومان على تغيير الحقيقة في ذهن المجني عليه و خداعه ويكمن الاختلاف في أن التزوير يتطلب عناصر لا تتطلب في الاحتيال فالتزوير يتعين أن يكون في محرر.

ج- تمييز جريمة النصب عن جريمة خيانة الأمانة:

تشترك جريمة النصب مع جريمة خيانة الأمانة في كونها من الجرائم الاعتداء على الأموال و أن الجاني يتسلم المال من المجني عليه برضاه في كليهما إلا أنهما يختلفان من حيث سبب التسليم و غايته.

1- التسليم في جريمة خيانة الأمانة يتم بموجب عقد من عقود الائتمان المنصوص عليها في نص المادة 376 من قانون العقوبات و تعتمد على الإرادة الحرة و السلمية للمجني عليه و التي لا يشوبها أي عيب من عيوب الرضا بخلاف جريمة النصب التي يكون فيها الرضا مشوب بعيب غلط .

2- إن التسليم في جريمة النصب عنصر جوهري في الركن المادي و هو نتيجة السلوك الإجرامي أما في جريمة خيانة الأمانة للتسليم هو شيء طبيعي و اعتيادي, وبدلا من أن يكون مكونا للجريمة فهو بالأحرى شرط سابق لها.

3- سبب التسليم في جريمة النصب هو وسائل الاحتيال أما سبب التسليم في خيانة الأمانة هو الائتمان أي انتهاك الجاني الثقة التي وضعها فيه المجني عليه الذي نقل إليه حيازة المال للحفاظ عليه بمجرد تسلمه المال.

ويظهر التمييز بين التسليم في الاحتيال والتسليم في السرقة في أمرين:

- **الأمر الأول** : أن التسليم في الاحتيال عنصر جوهري في الركن المادي نتيجة السلوك الإجرامي و هو وليد إرادة صاحبه وان كانت هذه الإرادة مشوبة بعيب الغلط أما في السرقة فالتسليم عمل قانوني مجرد قوامه نقل الشيء من سيطرة شخص إلى سيطرة شخص آخر بنية الحيازة.

– **الأمر الثاني** : إن جريمة السرقة لا تقع إلا على منقول مادي أما في الاحتيال فالتسليم لا يقتصر على الأشياء المادية بل يشمل أيضا إبرام تصرفات القانونية[1] .

الفرع الثالث المصلحة المحمية في الاحتيال :

يقع الاحتيال بالاعتداء على حق الملكية المنقولة المحمية قانونا و لكنه قد يصيب حقوق أخرى فهو يصيب حق المجني عليه في سلامة إرادته فبدلا من أن يتصرف و هو على بينة من أمره و يستوحي في تصرفه دوافعه الخاصة يظلل و يحمل على تصرف ضار به ويصيب الاحتيال مصلحة المجتمع في أن يسود حسن النية في المعاملات .

لقد تكلم المشرع الجزائري عن جريمة النصب في قانون العقوبات تحت عنوان النصب و إصدار شيك بدون رصيد و عرف جريمة النصب بموجب المادة 372 منه و تعد هذه الجريمة من الجرائم العمدية التي يعتدي فيها الجاني على أموال الغير بالطرق الاحتيالية التي حددها القانون بحيث يحمل المجني عليه لتسليمه المال بنية تملكه و يتبين لنا من خلال تعريف الجريمة أنه لقيامها يجب توفر ثلاث أركان الركن المادي و الركن المعنوي و الركن الشرعي[2] .

إن الشروع في النصب يتميز بأنه جريمة سلوك واحد خطر و هو سلوك الاحتيال و حدث نفسي واحد ناتج عن ذلك السلوك.

الفرع الرابع أركان جريمة النصب والاحتيال:

لابد في كل جريمة من توافر ركنين اثنين، وهما الركن المادي، والركن المعنوي ،أو الركن الشرعي ،وجريمة النصب والاحتيال لا بد فيها من وجود هذين الركنين، ليتم وصف التجريم على هذه العملية، ولكي يتضح الأمر لا بد من تبيان لهذه الأركان على التفصيل:

أولا :الركن المادي:

[1] محمد عبد الحميد المكي , نفس المرجع ص 132 و133

[2] رمسيس بهنام , قانون العقوبات , القسم الخاص منشأة المعارف , الإسكندرية,2005,ص1230

والذي يتمثل بوجود فعل مشاهد في الخارج يحس به، ويتكون هذا الركن من عناصر ثلاثة وهي:

1-1 النشاط الإيجابي "الاحتيال ".

1-2 النتيجة الإجرامية" الاستيلاء ".

1-3 علاقة السببية.

والمقصود بالنشاط الإيجابي هو: ممارسة المحتال لأساليب- لابد أن تكون محددة- لمزاولة عملية النصب والاحتيال طبقا للمبدأ القانوني "لا عقوبة ولا جريمة إلا بنص".. وهذه الأساليب هي:

أ- استعمال الطرق الاحتيالية.

ب-التصرف في مال الغير.

ج- اتخاذ اسم أو صفة كاذبة وغير صحيحة .

ومعنى استعمال الطرق الاحتيالية هو: إتيان المحتال مظاهر خارجية تدعم كذبة، وتكون الغاية من ذلك تحقيق أمور غير مشروعة.

والمظاهر الخارجية هي التي تلقي في روع المجني عليه، والمتمثل بالشخص العادي الطمأنينة،والتصديق فيسلّم بما يقوله الجاني أو يطمح إليه.

- **ومن تلك المظاهر**:الأوراق المزورة والتي يبرزها الجاني، ليدعم بها موقفه ،ويؤكد أمام المجني عليه صدق ما يقول، وهي غير مطابقة للواقع .

- **ومثال ذلك** : إبراز عقد وكالة ،أو شراكة مع أحد رجال الأعمال المشهورين، والمرموقين، وهي في حقيقتها وثيقة مزورة .

- **الاستعانة بالغير** : والذي قد يكون قريبا من الجاني كزوجته ، أو ولده، أو غير ذلك مما يدخل الطمأنينة على المجني عليه ، ويشترط القصد الجنائي في هذا المتدخل وإلاّ فالجريمة لا تقع عليه بل تقع على المستعين به .مباشرة بعض الأعمال الداعمة لكذب الجاني :

وذلك كقيادته سيارات فارهة، أو سكني فنادق شهيرة، أو إسراف في المصروفات، مما يغري الشخص العادي فينخدع به .

– **الغش التجاري:** والمتمثل بتقديم سلعة متشابهة مع السلعة الحقيقية مع اختلاف كبير في القيمة ،لإدخال الوهم في نفس المجني عليه، ومن ثم التعاقد معه، وممارسة الاحتيال عليه. استغلال الصفة: والقصد من ذلك أن يستغل الجاني صفة ما يتمتع بها، لتدعيم كذبه ،واحتياله كاستقلال رجل مشهور بالتدين، والصلاح أو ذي سلطة، أو منصب مرموق .

ولا يكفي مجرد هذه المظاهر بل لا بد من وجود الهدف منها وهو احد هذه الأمور الآتية :

– **وجود مشروع كاذب** : ويشمل جميع أنواع المشاريع التجارية والصناعية والمزارع والمالية

– **وجود واقعة مزورة** : وتشمل جميع أنواع الوقائع شريطة أن تكون مجانبة للحقيقة

– **إحداث الأمل والفأل لحصول ربح** :وذلك من خلال المقارنات والأسباب والدلائل الكاذبة والتي ينتج عنها بالطبع نتيجة كاذبة.

إحداث الأمل بتسديد وإرجاع المبلغ الذي أخذ بطريقة الاحتيال :ومثاله وعد الجاني بإعادة المبلغ المستلم من المجني عليه بصفته قرضا وتحرير كمبيالة بذلك أو شيك بدون رصيد أو قد أشهر إفلاس الجاني.

وأما الأسلوب التالي من العنصر الأول من الركن المادي وهو التصرف في مال الغير والمراد به: كون هذه الأساليب، والأنشطة من شأنها تخويل الجاني التصرف بمال غيره من الناس بدون وجه شرعي، ونتج التصرف بسبب هذه المظاهر الخادعة، والوعود الزائفة. و التصرف قد يكون ناقلاً للملكية كالبيع أو المقايضة أو الهبة، وقد يكون موثقاً للعين كالرهن ونحوه .

وأما الأسلوب الثالث من العنصر الأول ، الركن المادي فهو : اتخاذ اسم أو صفة مكذوبة . والمراد بذلك تسمي الجاني باسم له قيمة معينة ،أو انتحاله لصفة معتبرة ذات قيمة ،كاسم رجل أعمال، أو رجل ذي صفة مقدرة، أو وظيفة ذات طابع اجتماعي كبير،أو ذات طابع سياسي مخوف [1].

أما العنصر الثاني من الركن المادي وهو حصول **النتيجة الإجرامية** وهي " الاستيلاء :"فلا بد من حصول هذه النتيجة، وهي استيلاء الجاني على مال الغير، أو على شيء ذي قيمة ،يملكه الغير .ويشترط في ذلك أن يكون المال مملوكاً للغير وأن يكون المال له قيمة معتبرة .

1 – مولاي ملياني بغدادي، الإجراءات الجزائية في التشريع الجزائري، المؤسسة الوطنية للكتاب ،الجزائر،1995 ،ص 135.

وأما العنصر الثالث من الركن المادي فهي علاقة السببية ،والمراد بها: ترتب النتيجة "الاستيلاء" على النشاط الإجرامي المتمثل بالاحتيال ،بحيث يرجع الاستيلاء على هذا النشاط الإجرامي، ولولا وجوده لما حدث هذا الاستيلاء ،ولم يحصل سلب لمال المجني عليه ،أو بعضه .

فلا يكفي لقيام جريمة نصب أن يرتكب الجاني إحدى و سائل الاحتيال المنصوص عليها في المادة 372 من قانون العقوبات تم استيلاؤه على مال منقول مملوك للغير , و إنما يجب أن تقوم العلاقة السببية بين وسائل الاحتيال التي استعملها الجاني و تسلم المجني عليه المال , أي يجب أن يكون التسليم قد تم نتيجة لوسائل الاحتيال التي لجأ إليها الجاني[1] .

ولكن يلاحظ أن انتفاء العلاقة السببية لا يؤدي حتما إلى عدم العقاب وإنما قد تكون الواقعة شروعا في احتيال متى توافرت شروطه , كما إذا كان الجاني قد استنفذ من جانبه أفعال احتيال ولكنها مع هذا لم يؤد إلى النتيجة المبتغاة لسبب لا دخل لإرادة الجاني فيه كتفطن المجني عليه إلى احتيال الجاني أو تدخل شخص آخر في وقت مناسب ,فهنا يكون بصدد الشروع في احتيال لأن أفعال الاحتيال قد بدأ في تنفيذها و لكن خاب أثرها لسبب خارج عن إرادة الجاني .

ثانيا الركن المعنوي :ويقصد بالركن المعنوي هو: توفر القصد الجنائي , حيث إن جريمة النصب جريمة عمدية، تتطلب توفر القصد الجنائي المتمثل بالإرادة والعلم.

فتتجه إرادة الجاني إلى ممارسة السلوك الإجرامي بقصد تحقيقه النتيجة، وهي سلب مال الغير، أو بعضه، كما يجب أن يكون الجاني على علم ودراية بأنه يرتكب أمرا من شأنه التدليس، والتمويه، والمخادعة لاستيلاء مال الغير .

فجريمة الاحتيال أو النصب جريمة عمدية تتطلب توفر القصد الجنائي العام والقصد الخاص. ويتوفر القصد الجنائي العام فيها بعلم الجاني بأن الأفعال التي يأتيها يعدها القانون وسائل احتيال ومن شأنها خداع المجني عليه وحمله على تسلم المال، أما القصد الخاص

1 – نظير فرج مينا،الوجيز في الإجراءات الجزائية الجزائري، ديوان المطبوعات الجامعية، الجزائر 1992 ،ص100 .

فيتمثل في انصراف نية الجاني إلى الاستيلاء وتملك على الحيازة الكاملة لمال المجني عليه. فمن يتصرف في منقول أو عقار معتقدا أنه أصبح مملوكا له بطريق الميراث وهو لم يرثه بعد، لا تتوافر في حقه جريمة الاحتيال لتخلف القصد الجنائي العام. كذلك إذا لم يكن قصد الجاني منصرفا إلى تملك المال الذي تحصل عليه من حائزة بطريقة الحيلة انتفى قيام القصد الجنائي الخاص وانتفت بالتالي جريمة النصب، فمن يتوصل بوسائل الاحتيال إلى الحصول على منفعة مال من اخر لا يعد مرتكبا لجريمة النصب لأن العبرة هي نية الجاني في الاستيلاء على مال المجني عليه لا مجرد الحصول على منفعة هذا المال. ولا يمنع أن يكون الاستيلاء على المنفعة في هذه الحالة مكونا للجريمة المنصوص عليها في المادة 394 عقوبات إذا توافرت أركانها، إلا انه يشترط أن يتوافر القصد الجنائي العام والخاص في جريمة الاحتيال مع وقت الاستيلاء على المنقول أو العقار. وقيام القصد الجنائي بشقيه عند الجاني مرده إلى وقائع الدعوى [1]

وما تستخلصه منها محكمة الموضوع، ولا عبرة في توفره بالباعث الذي دفع الجاني إلى ارتكاب الجريمة[2].

ويتلخص مما سبق أن أركان جريمة النصب والاحتيال هي ما يلي :
وقوع فعل مادي يتمثل في فعل الاحتيال بإحدى الطرق المذكورة .
- حصول نتيجة من ممارسة هذا الاحتيال وهي الاستيلاء على نقود أو سندات أو متاع منقول
- قيام رابطة السببية بين الفعل المادي وهو الاحتيال والنتيجة وهي الاستيلاء على مال الغير
- توافر القصد الجنائي.

ثالثا الركن الشرعي : إن قانون العقوبات هو الذي يحدد الجرائم و يضع لها العقاب فلا وجود للجريمة بدون نص تشريعي و يعرف الفقهاء الركن الشرعي للجريمة على انه نص التجريم

1 - مولاي ملياني بغدادي، مرجع سابق ،ص 145.
2- نظير فرج مينا ،مرجع سابق، ص 102.

الواجب التطبيق على الفعل أو بعبارة أخرى هو النص القانوني الذي يبين الفعل المكون للجريمة و يحدد العقاب الذي يفرضه على مرتكبها

يقصد بالركن الشرعي إجمالا الصبغة غير المشروعة للفعل ويفترض الركن الشرعي خضوع الفعل للنص القانوني أي استفاء جميع الشروط التي تجعل نص التجريم واجب التطبيق عليه ومن هذا النص يكتسب الفعل صفة غير مشروعة وهي صفة غير مستقرة إذا هي قابلة للزوال إن خضع الفعل لسبب الإباحة و يفترض الركن الشرعي انتفاء أسباب الإباحة إذا توافر إحداها يصير الفعل مشروعا.

لقد نص المشرع الجزائري على جريمة النصب من خلال تطرقه لهذه الجريمة في قانون العقوبات لنص المادة 372 منه والتي جاء فيها كل من توصل إلى استلام أو تلقي أموالا أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من الالتزامات أو إلى الحصول على اي منها أو شرع في ذالك وكان ذالك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفة كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو بإحداث الأمل بالفوز بأي شيء أو في وقوع حادت أو أية واقعة أخري وهمية أو الخشية من وقوع أي شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة مالية من 500 دج الى 20000 دج.

على شيء ملموس مادي سواء كان مالا أو سندا ولا يقع النصب شأنه شأن ذلك سرقة العقار كما يشترط أن يكون للمنقول قيمة مالية.

أما في ما يخص الركن الشرعي للشريك يتمثل في استعارة هذا الأخير الصفة الإجرامية غير المشروعة لفعله من الصفة الإجرامية لفعل الفاعل الأصلي و بالتالي يصبح للمساهمة غير

المباشرة ركن شرعي مستقل عن الركن الشرعي للمساهمة الأصلية فيترتب على نشاط الشريك وجود مستقل عن الفاعل فتقوم مسؤولية الشريك حتى ولو لم يرتكب الفعل[1].

الفرع الخامس صفات النصاب و خطواته في النصب:

أولا صفات النصاب : يتميز المحتال ببعض الصفات السيئة التي تنبئ عن الشر والحقد والطمع وقلة الخوف من الله سبحانه، ويكاد يجمع المحتالون على التحلي بهذه الصفات التالية:

1- سوء الخلق .

2- قابلية التبرير العقلي للسلوك المتناقض.

3- الافتقار لقاعدة أخلاقية رصينة.

4- تقلب الرأي والمواقف مع الآخرين عند التعامل معهم.

5- عدم الثبات والاستقرار النفسي.

6- الرغبة الجامحة في كسر القانون السائد.

7- وجود خلفية إجرامية.

كما أن المحتال يمتاز بعدة مميزات منها ما يلي:

1- الذكاء الحاد، والرفيع.

2- القدرة على الابتكار، والتجديد .

3- اختلاق الحيل بمختلف الأساليب .

1- رشيد خلوفي، مجلس الدولة مجلس الدولة مجلة الإدارة، المدرسة الوطنية للإدارة مركز التوثيق و البحوث الإدارية، الجزائر المجلد 9 رقم 01سنة 1999 .

4- الفصاحة البارعة.

5- القدرة على التلون حسب الوضع المراد .

6- الجرأة، والوقاحة.

7- استغلال الظروف، والمواقف.

8- القدرة على التمثيل.

9- الاستعراض، والمباهاة، والاهتمام بالمظهر.

10- التجوال الدائم، وعدم الاستقرار.

11- انعدام الإحساس، والضمير الحي.

12- الطموح الشديد.

13- الخوف الدائم من المستقبل.

14- الاتصاف بالأخلاق المتدنية [1].

ثانيا: الخطوات الرئيسية للنصب التي يسلكها المحتال للاستيلاء على مال الغير:

1- تحديد موقع الشخص المراد خداعه وتقصي معلومات عنه.

2- كسب ثقة الشخص المراد خداعه من خلال الظهور بمظهر الحرص عليه، والاهتمام به.

3- إبراز الصفات الخادعة للشخص المراد خداعه، وإخفاء الصفات السيئة، وادعاء الاستقامة، والنزاهة، والشرف، والأمانة.

---

[1] محمد محرم محمد على, قضاء أمن الدولة في الإمارات العربية المتحدة: الجرائم الماسة بأمن الدولة الخارجي والداخلي ، جرائم تزييف العملة ، جرائم قانون دخول وإقامة الأجانب ، الجرائم الإرهابية, معهد القانون الدولي, دبي, 2006ص256

4- إثارة شهية الشخص المراد خداعه في جمع مال كثير في وقت قصير .

5- إقناع الشخص المراد خداعه بالفائدة الربحية المتوقعة .

6- إعطاء الشخص المراد خداعه أرقام، وإثباتات بشكل موثوق بها حول المبلغ المستثمر

7- دغدغة أحلام الشخص المراد خداعه في الثراء المأمول، والقادم

8- الحصول على رضي الشخص المراد خداعه .

9- الابتعاد عن الشخص المراد خداعه بعد الاصطياد، والوقوع به في الفخ.

10- إيقاع الشخص المراد خداعه بالمصيدة بشكل كامل، من خلال الخفة، والمهارة الفائقة[1] .

المطلب الثاني :جريمة النصب بالاستعمال الوسائل المعلوماتية (النصب المعلوماتي):

دقت أجراس الخطر لنية المجتمعات لحجم مخاطر ظاهرة جرائم المعلوماتية أو جرائم التقنية العالمية ، أو ما يعرف بجرائم نوابغ الانترنت ، فهي ظاهرة حديثة ظواهر ، بدأت مؤشراتها بالارتفاع منذ سنة 2000 ، و قد نجم عن هذه الجرائم التي تمتاز بالتقنية العالمية خسائر كبيرة العالمية خسائر كبيرة باعتبارها ، " بيانات ، معلومات ، و برامج بكافة أنواعها " فهمي تعتمد على الحاسب الآلي بشكل رئيسي ، يهدف فيها المجرم الإلكتروني أو النابغة الالكتروني إلى النيل من الحق في الاستئثار بالمعلومات باستعمال وسائل المعرفة التقنية ، و قد يتعدى ذلك إلى معطيات الحاسب الآلي المخزنة و المعلومات المنقولة [2].

1- محمد محرم على ، نفس المرجع ،ص89 .

2- انظر : قبلي علال ، بن لخضر عبد الكريم ، جرائم النصب الالكتروني ، مذكرة تخرج لنيل شهادة ليسانس في الحقوق ،سنة 2008-2009.

تظهر المخاطر الناجمة عن الجرائم المعلومات في كونها تمس الحياة الخاصة للأفراد وتهدد الأمن القومي، و السيادة الوطنية و تهدد إبداع العقل البشري ومن هنا وجب علينا إدراك ماهية هذه الجرائم و تحديد مفهومها القانوني.[1]

الفرع الأول: مفهوم جريمة النصب الإلكتروني:

بالنظر للتباين الموجود بين الجرائم الانترنت و الجرائم التقليدية وجد الفقهاء في حيرة من الثبات في رأي واحد فتمايزت أراء هو بحسب الموضوع و البيئة التي تنتمي إليها جريمة ن فظهرت العديد من التعريفات المتعلقة مرة بالجانب التقني و مرة أخرى بالجانب القانوني ، و لتحديد المفهوم الأساسي و الرئيسي للجريمة المعلوماتية ظهرت طائفتان أو اتجاهان :

- طائفة التعريفات القائمة على معيار واحد و هو قانوني و تتناول فيه كل من: السلوك محل التجريم، الوسيلة المستخدمة وموضوع الجريمة [2].
- طائفة التعريفات القائمة على النمط لكن هذه الطائفة تتمحور تعريفاتها و تتعلق بالتطور التاريخي الذي مرت به جرائم المعلوماتية ذات التقنية العالمية منذ ظهور الحاسوب كاختراع حديث أحدث ثورة في مجال المعلوماتية [3].

أولا :تعريف الجريمة النصب الإلكتروني: يحكم قانون العقوبات مبدأين أساسين أو لتها شرعية العقوبات التي تعرض انتقاء العقاب عند انتقاء النص ، و ثانيتها خطر القياس في النصوص التجريمية الموضوعية : و هنا ظهر الفراغ التشريعي في وضع تعريف القانوني يليق بنوع هذه الجرائم و بيان عناصرها و إثبات حجيتها ، ومن هنا يجب التميز بين الظاهرة الإجرامية و

1- عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية ، الكتاب الثاني ، دار الفكر الجامعي , مصر ,ب ط ، ص 204.

2- أنظر قبلي عادل، بن لخضر عبد الكريم، جرائم النصب الالكتروني، مذكرة تخرج لنيل شهادة ليسانس في الحقوق ، سنة 2007-2008 ،

3- د.عبد الفتاح بيومي حجازي ، مكافحة جرائم كومبيوتر و الانترنت ، المرجع السابق ، ص : 462-461-460.

الجريمة ، ووفقا لما سبق تعريف الجرائم المعلوماتية على أنها : " الأفعال غير مشروعة المرتبطة بنظم الحاسوب "

أما النص القانوني لجريمة النصب التقليدية الاستيلاء على حيازة مال الغير كاملة بوسيلة يشوبها الخداع تسفر على تسليم ذلك المال " حيث تنص المادة 372 ق.ع " **كل من توصل إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من الالتزامات أو إلى الحصول على إلى أي منها أو شرع في ذلـــك**

كان ذلك بالاحتيال لسلب كل ثورة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء وصفات كاذبة أو سلطة حالية أو اعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيء منها يعاقب بالحبس " [1].

و عرفه بعض الفقهاء بأنه " **الاستيلاء بطريقة لاحتيال على شيء مملوك للغير بنية تمله**"

كما يمكن لنا التمييز بين النصب و السرقة رغم تماثلها في الموضوع و الغاية في رضا المجني عليه حيث ينعدم في السرقة و يتوفر في النصب إلا أنه يتعرض لإحدى طرق الاحتيال من طرف الجاني.

ثانيا : نطاق جريمة النصب المعلوماتي: تتميز جرائم الانترنت بطبيعة خاصة تتمثل في صعوبة اكتشافها و ضبط مقترفيها كما تتميز أيضا بأساليب افتراقها إذ يغلب عليها الطابع الفني التقني عكس الجرائم البدوية التقليدية ، و نظرا للأهمية التي يلعبها الحاسوب في مجال التطور المعلوماتي إلا أن الحاسوب الآلي له سلبيات كماله من إيجابيات فمرتكبو جرائم الانترنت استغلوا لتطوير خبرائهم الوسائل التقليدية لارتكاب الجرائم حيث طور وسائل جديدة لتناسب هذا التطور التكنولوجي في مجال الحاسوب ليس لمواكبة و تنمية المعارف و إنما

1- انظر : القانون رقم 23/06 المؤرخ في 20 ديسمبر 2006 ، ص : 136.

للاعتداء عليه ، و تختلف الأساليب باختلاف العنصر الذي يون محلا للاعتداء (معدات الحاسوب المادية) أي الأسطوانات و الشرائط الممغنطة [1].

تستخدم عدة أساليب لارتكاب الجريمة الإلكترونية ، و تكون معدات الحاسوب المادية موضوعا لها وقد تمس هذه الجرائم أموالا خاصة بالأفراد كما قد تمس أموالا خاصة بالدولة إلا أنها تعد وسائل تقليدية لها:

– تدمير الدعامات التي تحتويها سواء بإحراقها ، أو تفجيرها باستخدام القنابل المتفجرة أو سكب سوائل ساخنة على الأجزاء الحساسة من الحاسب ، أو إلقاء رماد السجائر المشتعلة على الشرائط و الأسطوانات الممغنطة و هذا الأساليب لا تتطلب سوى معرفة فنية متواضعة تتمثل في مجرد سلوك مادي بالنتيجة الإطلاع البصري .

– للمعلومات التي تظهر على شاشة الحاسب، أو القيام بالتنصيب عليها فغي حالة تجسيدها في صورة سمعية أو عن طريق الاستعانة بوسيط يعمل على تكبير الصوت الصادر من الحاسب، و من هنا يحصل على ما يريده بطريقة مباشرة .

– أما الأساليب عالية التقنية و التي تتطلب معرفة فنية بالحاسوب حيث يقوم فيها المجرم الإلكتروني بما يتسمى بعملية السطو المسلح الإلكتروني ، يكون الهدف من هذه العملية التقاط أو تسجيل المعلومات و البيانات المعالجة الكترونيا ، و هي مرحلة الانتقال و البث من الحاسب بواسطة أجهزة شبكة اتصالات بعيدة « **lima tique** » و المعالجة عن بعد « **télétraitement** »كما يمكن عرض بعض الوسائل فيا يلي.

1– التقاط المعلومات التي توجد ما بين الحاسب و النهاية الطرفية : يحدث هذا الالتقاط بواسطة توصيل خط تحويل يعمل على تكبير الذبذبات الالكترونية ، و إرسالها إلى نهاية الطرفية التي تقوم بعملية التجسس ومن المكن أن يحدث أيضا باستخدام جهاز مرسل صغير يمكنه نفل البيانات عن بعد و يمكن الالتقاط كذلك عن طريق وضع هوائيات مطاردة بالقرب

1– هدي حامد قشقوش،جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية،بدون ط , بدون سنة ص 125.

من الهوائيات الاحتياطية ، و بالتالي يحدث التقاط الإشاعات العابرة عن طريق النقل الجوي للمعلومات عند بثها بالقمر الاصطناعي و احتجاز مضمونها [1].

2- التوصيل المباشر بواسطة خط تليفوني : يتم ذلك بوضع مركز تصنت يجعل من تسجيل الاتصالات أمرا يسيرا كما يمكن الاستعانة أيضا بوضع ميكروبات صغيرة لأدائها.

3- التقاط الإشاعات الصادرة عن الجهاز المعلوماتي : تكمن خطورة هذه الوسيلة في أنها يمكن أن تؤذي إلى إعادة تكوين خصائص المعلومات التي تبث و تنقل من خلال الأنظمة المعلوماتية ، و هذا الجناح تسجيل الإشاعات الصادرة عن الحاسب كما لا يحتاج إلى حل شفراتها.

4- التدخل الغير المشروع في نظام الحاسب بواسطة طرفية بعيدة : تعد هذه الوسيلة ألفية من أخطر الوسائل التي يلجأ إليها المحرم المعلوماتي ، إذ يكون بإمكانه نسخ أو تدمير بعض البيانات و المعلومات بكل يسر ولا يحتاج إلا لمجرد الحصول على حاسب الآلي "ميكروي" مع ضرورة التعرف على كلمة السر أو مفتاح شفرة نظام للحساب المجني عليه.

و هكذا فإن المجرم المعلوماتي أو مرتكبي جرائم الانترنت اكتفوا بالوقوف مذهولين أمام تكنولوجيا الحاسب و إمكانيته الفائقة التي بلغت حد الخيال من قدرة على التخزين و الاسترجاع بسرعة فائقة بالإضافة إلى دقتها و مرونتها في التشغيل ، بل نجد هؤلاء و قد استوعبوا هذا التكنولوجية بطريقة متقدمة جدا و استغلوا خبرائهم المكتسبة منها في تطوير الوسائل التقليدية لارتكاب و ابتكار وسائل جديدة و غير معروفة تتناسب مع التطور إنه الصراع أبدي بين الخير و الشر[2].

الفرع الثاني : خصائص جريمة النصب المعلوماتي:

1- هدى حامد قشقوش ، جرائم الحاسب الآلي في التشريع المقارن، مرجع سابق ص 129- 130

1- د. أحمد خليفة الملط ، الجرائم المعلوماتية ،دار الفكر الجامعي ، القاهرة ، الطبعة الثانية ، سنة 2006 ، ص 301- 2 .314

لجريمة النصب خصائص تتميز بيها و تتمثل فيما يلي :

1- جريمة الاحتيال هي جريمة التعدي على الملكية على المال بخلاف الجرائم القتل فالفاعل يخدع المجني عليه لحمله على تسليم المال أو ما في حكمه.

2- جريمة الاحتيال تقوم على تغيير الحقيقة و الواقع و ذلك كون الفاعل يستخدم وسائل الخداع و الكذب لي يتوصل إلى غاية و هي إتمام الجريمة.

3- جريمة الاحتيال من جرائم السلوك المتعدد و الحدث المتعدد ، ذلك أن الجاني يرتكب سلوك مادي ذو مضمون نفسي يتمثل في أساليب الإحتيال التي يلجأ إليها للتأثير على ك المتعدد و الحدث المتعدد ، ذلك أن الجاني يرتكب سلوك مادي ذو مضمون نفسي يتمثل في أساليب الإحتيال التي يلجأ إليها للتأثير على إرادة الشخص المخاطب بهذه الأساليب.

4- جريمة الإحتيال هي جريمة ذات طابع ذهني بخلاف الجرائم التي تعتمد على الجهد العضلي أو الجسدي فهي جريمة تعتمد على الذكاء المجروم و دهانه [1].

5- جريمة الإحتيال تصنف ضمن جرائم الأموال :

فقد جرت غالبية التشريعات على التفرقة بين قسمين من الجرائم هي الجرائم المضرة بالمصلحة العامة و الجرائم المضرة بالأفراد و قد درج شراح القانون على تقسيم الجرائم المضرة بالأفراد إلى قسمين أيضا هما : جرائم الإعتداء على الأشخاص و جرائم الإعتداء على الأموال و جرائم الأموال هي التي تنقص أو تعدل من العناصر الإيجابية للذمة المالية أو تزيد من عناصرها السلبية.

1- إنها من الجرائم التي تستلزم غالبا التخصص و الدراية من قبل الجاني بمجال نشاطه:

حيث يعتاد المحتالين على استخدام أسلوب معين لارتكابها حيث خصص به لانه يكون على دراية بضحايا ، و كيفية خداعهم و النصب عليهم.

1- عبد القادر الشبخلي ، جريمة الإحتيال في قوانين عقوبات الدول العربية ، الطبعة الأولى ، منشورات الحلبى الحقوقية ، بيروت لبنان ، سنة 2009 ، ص 37-38.

2- لأنها من الجرائم التي تنتشر في المدن ، و المناطق المتقدمة حضاريا و المزدهرة صناعيا و تجاريا و إقتصاديا:

و الأكثر هذه المناطق عرضة تلك التي تنتشر فيها المعاملات الورقية ، و المعاملات القائمة على السرعة الإئتمان و الثقة المتبادلة بين الأفراد و المؤسسات حيث يستغلها المحتالين لتمرير أفعالهم الإحتيالية.

3- إنها من الجرائم الواقعة على حرية الإرادة:

أي تصيب إرادة المجني عليه بعين الرضاء، لأنه بدلا من أن يتصرف المجني عليه بإرادته الحرة ، و يكون على بينة من أمره ، ووعي بتصرفاته يضلله محتال و يغرر به .

الفرع الثالث: أركان جريمة النصب ألمعلوماتي:

من المسلم به أن لجريمة النصب الإلكتروني ركنين ، ركن مادي و ركن معنوي إلا أن الطبيعة الخاصة للتعاملات الإلكترونية و خاصة أنها ترد على منقولات ذات طبيعة معنوية تعطي هذه الأركان مفهومها مختلفا عما هو مقرر بالنسبة للمنقولات المادية التقليدية ، و يتضح ذلك من دراسة الركن المادي في الفرع الأول بما فيه من سلوك إجرامي و نتيجة إجرامية و علاقة سيئة و الفرع الثاني الركن المعنوي " العمد ، القصد المتعدي و الخطأ غير العمدي "[1].

أولا الركن المادي:

يتمثل في سلوك إرادي يترتب على نتيجة إجرامية، تربطها بالسلوك الإجرامي رابطة سيئة مادية هذا هو الركن المادي في جريمة الانترنت و باستقرائنا للتعريف نستنتج انه يتكون من سلوك إرادي و نتيجة إجرامية و رابطة سيئة.

1- قبلي علال ، بن لخضر عبد الكريم ، جرائم النص الإلكتروني ، مذكرة تخرج لنيل شهادة ليسانس في الحقوق ، سنة 2007، 2008 .

1- **سلوك إجرامي** : يعتبر السلوك المادي عبر الانترنت محلا للتساؤل ، لا سيما فيها يتعلق ببدائية أو الشروع في ارتكاب الجريمة ، و هو يختلف عما هو الحال في الـعالم المادي ، و ذلك لأن ارتكاب الجريمة عبر الانترنت يحتاج بالضرورة إلى منطق تقني ، أي أنها تتم عبر الانترنت أو باستخدام الحاسوب و الانترنت و من أمثلة السلوك المادي في الجريمة عبر الانترنت المصرفي الذي ينوي سرقة مبلغ من المصرف الذي يعمل فيه باستخدام الانترنت ، ثم الدخول إلى شبكة المصرف عبر مزودات مجهولة يمكن الاستعانة من خلالها ببرمجيات اختراق موضوعية على موقع يتم تحديدها باستمرار في هذا المثال فإن المصرفي المذكور يمارس النشاط المادي للاختلاس عن طريق الحاسوب و الانترنت [1].

2- **النتيجة الإجرامية:** يعد هذا العنصر أحد عناصر الركن المادي في الجريمة غلى جوار السلوك الإجرامي و علاقته السببية، و تثير مسألة النتيجة الإجرامية في جرائم الانترنت

مشاكل عدة أهمها، تحديد هل الجريمة المرتكبة سلوك و نتيجة في العالم الافتراضي أم أن هناك امتداد للنتيجة ليتحقق منتهاها في العالم المادي ؟ [2].

3- **العلاقة السببية** : هي العنصر الثالث من العناصر التي يتكون منها الركن المادي في الجريمة الالكترونية و يجب لقيام جريمة الانترنت أن تكون هناك رابطة مادية ما بين السلوك المادة و النتيجة الإجرامية المتحققة فمثلا يجب لتحقيق جريمة انتهاك الحق في الخصوصية عبر الانترنت أن يكون هناك دخول على الانترنت باستخدام حاسوب عامل و القيام بالاختراق الحواسب المختلفة في مسارها ، ثم بعد ذلك التعدي على خصوصية موقع ما و كذلك يمكن اعتبار علاقة السببية قائمة بمجرد ثبوت الضرر في مجر البيت ، و هذا ما قررته محكمة استئناف مقاطعة **Columbia british** الكندية في إحدى أحكامها.

1-عبد الفتاح بيومي حجازي ، مكافحة جرائم كومبيوتر و الأنترنت ، المرجع السابق ، ص : 468.

2- عبد الفتاح بيومي حجازي ، مكافحة جرائم كومبيوتر و الأنترنت ، المرجع نفسه ، ص : 468 .

إن كل من جريمة تحدث باستعمال الانترنت إنما تحدث كلها أو بعضها حسب الأحوال في العالم الافتراضي ، و إذا كان النشاط المادي كله يحدث في العالم الافتراضي و كذا العلاقة السببية فإن النتيجة الإجرامية لها كيان منفصل لكونها تحدث بشكل انقسامي ما بين حدوثها في العالم جزئيا أو كليا.

و من أهم الآثار المترتبة عنها تؤثر على قواعد الاختصاص في الدول كما أن جرائم الانترنت تنشر فيها فكرة النتيجة المحتملة ، و ذلك راجع إلى طبيعة النشاط التقني الذي قد يترتب عليه عدة نتائج منها ، انتشار الفيروسات بقصد القرصنة ، فإن ذلك يعتبر نتيجة محتملة تشمل الجريمة التي ليس لها منحني إطلاقا أي الحالة التي لا كون فيها للضحية وجود مادي و إنما رقمي فقط [1].

ثانيا الركن المعنوي:

يتعلق بشخصية الجاني و بمسلكه الذهبي و النفسي كما للركن المعنوي ثلاث صور في الجرائم المتعلقة بالانترنت و هذه الصور هي :

1-العمد : ينبغي لارتكاب الجريمة الإلكترونية أن يكون مرتكبها نابغة في استعمال الحاسوب ، أي أنه يجب أن يكون مكتبا من المعرفة و التعليم التخصصي ليتمكن من ممارسة هذا النوع من وسائل الإيصال و في هذه الحالة يكون وقوعها في صورة واحدة و هي صورة العمد حيث أن المجرم الإلكتروني يكون قد خطط ودبر لارتكاب هذه الجريمة سواء من أجل الحصول على معلومة أو لاختراق شبكة حاسوب آخر كجريمة النصب تتطلب من الفاعل إرادة ارتكاب السلوك تحقيق نتيجة ، و قد يكون القصد عاما أو خاصا.

يتحقق القصد العام إذ اعلم المجرم أنه يرتكب فعل تدليس من شأنه ارتفاع المجني عليه في الغلط الذي يحمله على تسليم مؤلفه ففي جرائم النصب المعلوماتي يستخدم الجاني أسلوبا

1 - أنظر : قبلي علال ، بن لخضر الكريم ، جرائم النصب الإلكتروني ، مذكرة تخرج لنيل شهادة ليسانس في الحقوق ، سنة 2007-2008.

للإيهام بوجود ائتمان كاذب أو يتوصل للاستيلاء على مال الغير كله أو بعضه متى وقع على فواتير الشراء باسم كاذب أو استغل صفة كاذبة لتحويل أموال الغير من حساب إلى آخر عن طريق التلاعب المعطيات أو البيانات الالكترونية و يجب عمله بهذه الوقائع ، و مع ذلك تتصرف إرادته إليها رغم عمله بأن فعله من الأفعال التدليسية [1].

أما القصد الخاص هو نية التملك ، فبقوم متى كان الهدف الجاني من هذا الاحتيال الاستيلاء على مال مملوك لغيره ، علما بأنه لا عبرة بالبواعث في ارتكاب جريمة النصب سواء كان الباعث نبيلا أم خسيسا ، كما يتوافر القصد الخاص في النصب المعلوماتي ، متى قام الجاني مثلا باستخدام البطاقة وهو عالم أن رصيده فارغ أو أن بطاقته موقوفة و يستخدمها[2].

2- القصد المتعدي : يتوفر القصد المتعدي في جرائم الانترنت في الحالة التي يتجاوز فيها قصد الشخص الهدف الذي كان يسعى لتحقيقه مثلا : إذا كان القصد مجرد اللهو في مسارات القطارات ، فيتعدى الأمر ذلك تدمير بيانات تحريك القطارات عبر الحاسوب و تكون النتيجة حدوث خسائر مادية و بشرية و بهذا يتعدى النتيجة الهدف الذي كان يصبو إليه محترف الكومبيوتر فيصبح من مجر لاه في أجهزة الحاسوب إلى جرم الإلكتروني[3] .

3- **الخطأ غير العمدي:** يحتل الخطأ مرتبة هامة في الركن المعنوي في جرائم أنترنت إذ أن معظم جرائم الانترنت تحدي نتيجة لخطأ عنبر مقصودة كتدمير أجهزة المؤسسة لإفراط الموظف المسئول في استخدام حاسوبها بدلا من حاسبوه الخاص في العمل على حساب الخاص ناسيا متاعب الفيروسات و معتمدا فقط على مهارته في تجنبها دون إدراج برامج القضاء على الفيروسات أو محاربتها في الكومبيوتر أو ينقل الفيروسات أو محاربتها في

---

[1]- د- عبد الفتاح بيومي حجازي ، النظام القانوني لحماية التجارة الإلكترونية ،دار الفكر الجامعي ن الإسكندرية ، مصر ، بدون طبعة ، سنة 2002..

2- عبد الفتاح بيومي حجازي ، النظام القانوني لحماية التجارة الإلكترونية ،المرجع السابق .

3- أحمد خليفة الملط ، المرجع السابق ، ص 322.

الكمبيوتر أو ينقل الفيروسات من القرص المرن إلى أجهزة المؤسسة فشكل تدميرا كليا أو جزئيا المعلومات أو البيانات بالأخص إذا تنقل فيروس إلى شبكة أو نظام حاسوب لمؤسسة مالية أو فدرالية [1].

الفرع الرابع النظام المعلوماتي محل لجريمة النصب :

إن التجارة الإلكترونية تثير العديد من المشكلات القانونية و العملية الهامة التى تحتاج إلى بحث متعمق و تركيز الأضواء عليها و من أهم تلك المشكلات هي كيفية حماية المستهلك نظرا لعدم توافر أطراف العقد و كذا محل العقد في مكان واحد .

واستكمالا لما سلف نجد أن التجارة الإلكترونية تتسم بعدة خصائص و أهمها:

أ – عدم وجود علاقة مباشرة بين طرفي العقد.

ب – عدم الاعتماد على الوثائق الكتابية فى التعامل

ج – تجاوز الحدود الزمنية و الجغرافية

د – اتساع مجال التجارة الإلكترونية

هـ – فكرة النشاط التجاري [2]

و وفقا لهذه السمات المميزة للتجارة الإلكترونية نجد أن المستهلك المتعامل مع هذا النمط من المعاملات الإلكترونية يكون معرضا أكثر من غيره للوقوع فريسة لعمليات النصب و الاحتيال التي قد تقع في مجال الفضاء السيبيري و لكن هل يمكن للقوانين الوطنية العادية التصدي لمثل هذا النوع من الجرائم وفقا لما سلف سرده من واقع الآراء الفقهية و القانون الجنائي الجزائري.

أولا: النظريات الفقهية في إمكانية تطبيق نصوص النصب التقليدية على النصب المعلوماتي:

1– أحمد خليفة الملط ، المرجع السابق ، ص 322.

2 -jean larguiez, Philipe conte, opt , cit , page 121.

للمعاقبة على جريمة النصب في الفضاء السيبيري و في نطاق التجارة الإلكترونية نجد أننا أمام ثلاثة آراء مختلفة في هذا الشأن و هي على التصنيف التالي :

الرأي الأول: عدم انطباق النصوص الجنائية على جريمة النصب في إطار التجارة الإلكترونية و يرى أنصار هذا الرأي أن جريمة النصب لا تقوم إلا إذا خدع شخصا مثله وأن يكون الشخص المخدوع مكلفا بمراقبة البيانات وغلى ذلك لا يتصور خداع الحاسب الآلي بوصفه آلة ومن ثم لا يطبق النص الجنائي الخاص بالنصب والاحتيال لافتقاده أحد العناصر اللازمة لتطبيقه.وهذا الاتجاه تتبناه تشريعات مصر وألمانيا والد نمارك وفنلندا واليابان والنرويج والسويد ولكسمبرج وايطاليا.

الرأي الثاني : التوسع في النصوص الجنائية حتى تشمل جريمة النصب في إطار التجارة الإلكترونية و يرى أنصار هذا الاتجاه إلى حتمية تطبيق و فهم النصوص العقابية في إطار جريمة النصب حتى تحتوى تلك الجرائم الواقعة في الفضاء الإلكتروني في إطار معاملات التجارة الإلكترونية .و قد أخذ بهذا الاتجاه عدد كبير من الدول و منها بريطانيا واستراليا وكندا.

الرأي الثالث: انطباق النصوص الجنائية المتعلقة بالنصب على بعض الجرائم الإلكترونية

وتمثل هذا الرأي الولايات المتحدة الأمريكية حيث تطبق النصوص المتعلقة بالغش في مجال البنوك والبريد والتلغراف والاتفاق الإجرامي لغرض الغش على حالات النصب المعلوماتي[1].

ثانيا :امتداد الركن الشرعي ليشمل جريمة النصب المعلوماتية : على ضوء المادة 372 نلاحظ أن المشرع الجزائري اكتفي بالكذب المجرد حول الاسم و الصفة دون أن يكون مقترنا بالمظاهر الخارجية أو الأفعال المادية كما أورد قائمة المناورات الاحتيالية على سبيل الحصر و عبر عنها بعبارات مرنة تضم جل أنواع التدليس أو الخداع حتى يتم احتوائها.أيضا أن المشرع نص على المنقول دون تحديد طبيعته و دون تقييده بأن يكون مال منقول.

1- الإشكالات القانونية في تجريم الاعتداء على أنظمة المعلومات ، عباوي نجاة, مقال بعنوان .

و كون أن المادة السالفة الذكر تسعى لحماية الأشخاص الطبيعية و المعنوية على حد سواء من فعل النصب و الاحتيال سواء أكان الضحية إنسان أو آلة.

هنا تبقى السلطة التقديرية للجهات القضائية التي تنظر في الملفات المعروضة أمامها إما بتطبيق النصوص التقليدية أو رفض الملف هذا لخطورة النصابين بصفة عامة بما بالك النصاب الإلكتروني.

ثالثا: بعض صور النصب الواقعة على المتعاملين فى التجارة الإلكترونية:

إن صور النصب و الاحتيال في التجارة الإلكترونية لا يمكن حصرها و لكن يمكن أن نذكر عدد منها على سبيل المثال ومنها

أ – عدم الوفاء بالسلعة المتعاقد عليها بالرغم من سداد المستهلك لثمنها

ب – انتحال اسم أحد مواقع التسويق الشهيرة

ج – الترويج لسلعة مقلدة شبيهة بمنتج أصلى عالي الثمن و الجودة

د – الترويج لسلع غير معروفة باستخدام الإعلان الكاذب أو المضلل

و سنتناول تلك الأمثلة بشي من التفصيل على النحو الآتي :

أ – عدم الوفاء بالسلعة المتعاقد عليها بالرغم من سداد المستهلك لثمنها

و خير مثال على ذلك ما قامت به وزارة العدل الأمريكية فى شهر ديسمبر من عام 1994 من إدانة شخصين بالخداع و التحايل عبر الشبكة الدولية – الإنترنت – فقد وضعا إعلانات على الشبكة ، و وعدوا بإرسال السلع التي يتم طلبها الكترونيا من العملاء فور دفع قيمة السلعة إلكترونيا و لكن المشتركين الذين طلبوا السلعة و قاموا بالدفع لم يتسلموا السلعة و كانت العقوبة هي السجن خمسة أشهر و غرامة 32 ألف دولار .

ب – انتحال اسم أحد مواقع التسويق الشهيرة

وتتم تلك العملية من الاحتيال بأن يقوم المجرم باستغلال اسم أحد المواقع الشهيرة بالتسويق أو أحد مواقع المنتجات المختلفة الشهيرة و يقوم بإنشاء موقع مماثل له سواء أكان ذلك في الاسم المتشابه معه إلى حد كبير أو في واجهة و نافذة ذلك الموقع حتى يخدع المتعامل معه و يوهمه أنه ذات الموقع الشهير تمهيدا للاحتيال عليه و سلبه أمواله بلا مقابل .

ج – الترويج لسلعة مقلدة شبيهة بمنتج أصلى عالي الثمن و الجودة

و في هذا الافتراض يقوم المجرم المعلوماتى بعرض منتجات مقلدة وتشبه الأصلية الى حد كبير مع إيهام المستهلك بأنها ذات السلعة بثمن أقل كعرض خاص من الموقع .

و تحمل تلك الجريمة بعدا آخر و هي جريمة التعدي على حقوق الملكية الفكرية لهذا المنتج و لكن سنأتي إلى هذا المحور فيما بعد.

د – الترويج لسلع غير معروفة باستخدام الإعلان الكاذب أو المضلل

و في هذه الحالة يقوم المنتج لسلعة غير مشهورة بالإعلان لها بإعلان كاذب و الكذب هو الإخبار عن شيء بخلاف ما هو عليه في الواقع وهو يقوم على عنصرين

أولا : مضمون زائف.

ثانيا : قصد تزييف الحقيقة: أما الإعلان المضلل فهو الذي يكون من شأنه خداع المستهلك فهو لا يذكر بيانات كاذبة بل يصاغ فى عبارات تؤدى إلى خداع المستهلك المتلقي [1].

1 – أبو العلا النمر، **المشكلات العملية و القانونية في التجارة الالكترونية**" ،دار النهضة العربية للنشر و الطبع و التوزيع الطبعة الأولى ،2004. ص 209.

الفصل الثاني الإطار الإجرائي المقرر لمتابعة جريمة النصب المعلوماتية :

نقصد به الإجراءات التي تسير بها الدعاوي بالعمومية على اختلافها سواء في قانون العقوبات او القوانين المكملة له, و الإجراءات هي التي تسمح بتحريك هذه الدعاوي العمومية و هي محددة في قانون الإجراءات الجزائية.

فالدعوى العمومية هي هي إدعاء النيابة العامة بالسم المجتمع لملاحقة مرتكبي الجرائم و المطالبة بتوقيع العقوبة عليه أمام الجهات القضائية و هي بدلك تحرك الدعوى العمومية و تباشرها و هنا النيابة العامة لا تعاقب بل تتخذ مجموعة من الإجراءات و تطلب من القضاء توقيع العقاب بما يقتضيه قانون العقوبات , فبمجرد وقوع الجريمة تنشأ الدعوى العمومية أي ينشأ حق الدولة في العقاب.

فيمكن تعريف قانون الإجراءات الجزائية بأنه مجموعة القواعد القانونية التي تبين الإجراءات و الطرق الواجب إتباعها لتحريك الدعوى العمومية و سلطات الهيئات القائمة عليها على غرار الشرطة القضائية النياية العامة و غيرها , بغية التطبيق السليم للقانون على من يشتبه إرتكابه للجريمة فهو يحدد كافة هذه الإجراءات من وقوع الجريمة مرورا بالتحقيق الى غاية الفصل فيها بحكم قضائي.

و هنا القضاء ساكن ينتظر أن يصله الملف ليفصل فيه و بالتالي المتحرك هو النيابة فهي تستمد سلطاتها من قانون الإجراءات الجزائية.

فقانون الإجراءات الجزائية يحدد لنا الأجهزة القضائية و الشبه قضائية و اختصاصاتها كما ينظم طرق البحث و للتحري و التحقيق و جمع الاستدلالات في كل الجرائم. كما يحدد نظام الاختصاص بالنسبة للمحاكم و المجالس أو الجهات القضائية بصفة عامة و أيضا يحدد لنا نظام الإثبات و وسائله و كيفياته .

و في ضل غياب النص القانوني الذي يجرم صراحة جريمة النصب المعلوماتية و يقر بمعاقبة هذه الأخيرة بصيغة منفردة كونها من الجرائم المستحدثة و التي باتت تشكل خطرا حقيقيا على الحقوق المالية للأفراد من جهة و تعمل على تقويض الاقتصاد الوطني من جهة أخرى.

فجريمة النصب المعلوماتي جريمة لا تعترف بالحدود الوطنية والإقليمية كما يتميز مرتكبوها كما سبق الذكر فالذكاء الإجرامي و الفطنة كما أنهم أشخاص ماكرون و هادا ما تأكده معظم الأبحاث في مجالات علم الإجرام و علم الضحية و علم النفس الجنائي و غيرها من المجالات التي تعنى بدراسة السلوكيات الإجرامية.

و بالتالي نجد كنتيجة منطقية قصور واضح في الإجراءات لغياب الموضوع فالإجراءات هي السكة التي يمشي فيها الموضوع و من غير المعقول أن تجد السكة دون وجود الموضوع.

و عليه نقول أن غياب التدخل التشريعي أصبح يشكل نقص و قصور في متابعة هته الجريمة في أحيان كثيرة و لأجله بات لزاما على المشرع تداركه من اجل احتواء هته الجريمة في ضل القانون و القضاء و الاكتفاء بالنص العام أو النص التقليدي من أجل متابعتها.

و لو أن المشرع الجزائري و من خلال الأمر 04/09 و 14/04 تطرق للجريمة المعلوماتية بصفة عامة و تدارك خلالها لبعض الإشكاليات من خلال الوقاية ضد الجرائم المعلوماتية و مكافحتها.

فجريمة النصب كغيرها من الجرائم الأخرى لها أركان و عناصر و لو أن خصائصها ذات طابع الكتروني كونها تمارس عن طريق الوسائل المعلوماتية. و من هادا المنطلق كان التركيز في الفصل الثاني على الجانب الإجرائي من خلال التطرق لنظام الاختصاص القضائي لجريمة النصب و نظام الإثبات المعتمد في إطارها.

و عليه قسمنا الفصل الثاني إلى مبحثين أساسيين :

المبحث الأول قواعد الاختصاص في جريمة النصب بالاستعمال الوسائل المعلوماتية.

المبحث الثاني طرق إثبات جريمة النصب المعلوماتية.

المبحث الأول: قواعد الاختصاص في جريمة النصب المعلوماتي:

إن من الحقوق التي كفلها الدستور للمواطنين هو حق اللجوء إلى القضاء و ضمانا لحسن سير العدالة و لتقريب العدالة من المواطنين أقر المشرع عدة مبادئ منها التقاضي على درجات (اختصاص نوعي) و هادا يؤدي إلى تحديد درجة المحكمة المختصة (محكمة ابتدائية, مجلس قضائي, قطب جزائي, محكمة عليا).

و أقر تعدد المحاكم ذات الدرجة الواحدة مما يؤدي إلى وضع قواعد تبين اختصاص المحكمة التي تنظر في الدعوى من بين المحاكم من نفس الدرجة الواحدة . و هادا يؤدي إلى نتيجة حتمية و هي وجوب إيجاد قواعد تبين نصيب كل محكمة من النزاعات المعروضة و هو ما يعرف بالاختصاص .

و هو ما نص عليه المشرع في قانون الإجراءات الجزائية فالاختصاص هو السلطة التي يقررها القانون لجهة قضائية معينة للنظر في دعاوى من نوع معين و الاختصاص الجزائي هو السلطة التي خولها القانون إلي الجهات القضائية الجزائية للنظر في الدعاوى العمومية باختلافها. و يعرف بأنه صلاحية مباشرة الجهة القضائية لإجراءات المتابعة و التحقيق و الحكم بمقتضى القانون في الدعوى.و يقصد بالمحكمة المختصة التي يمنحها القانون سلطة الفصل في هذه الأخيرة .

و عليه سنبين الموقف الفقهي و القضائي و التشريعي من مسألة الاختصاص كما سنبين موقف المشرع الجزائري و التشريعات المقارنة لنقف في الأخير على توصيات الإتفاقيات الدولية في نفس الشأن.

المطلب الأول: الموقف الفقهي و القضائي و التشريعي من مسالة الاختصاص القضائي:

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

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

وفي حالة قيام التنازع إيجابي في الاختصاص 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 حولا مستحدثة وابتكارا 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 المعلوماتية عندما يرتكب شخص جريمة في إحدى الدول وتجري محاكمته في دولة أخرى.

وبالتالي فإذ كان الأصل أن عناصر الركن المادي للجريمة تكتمل في مكان واحد أو بالأحرى في نطاق إقليم واحد استثناءا في الجرائم المعلوماتية 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 أم المكان الذي تحققت فيه النتيجة.

وإذا كنا بصدد جريمة معلوماتية أو أمام جريمة نصب معلوماتية عبر الإنترنت عن طريق الإعلانات الكاذبة مثلا فهناك صعوبة قانونية كبيرة في تحديد المحكمة المختصة للنظر في القضية بسبب طابع شبكة الانترنت العابرة للحدود، فقد يبث المتهم الإعلان الكاذب ممن بلد معين لإيهام الشخص المجني عليه من بلد أخر ،فقوم هذا الأخير بتسليم ماله إلى المتهم كما أنه قد يستخدم تقنيات التمويه مثل تقنية ال VPN التى تسمح بتمويه الدولة التي ارتكبت فيها الجريمة و بل حتى تغير هده الأخيرة ال adresse ip الخاص بالحاسوب الذي ارتكبت منه الجريمة هو الأخر باتالي يصبح الأمر أكثر تعقيدا .

وبالتالي هل يؤول الاختصاص للتحقيق في الاحتيال المعلوماتي لدولة المتهم أو الضحية أو جهة أخرى ؟

– وللإجابة على هذه الإشكال وجب علينا دراسة موقف الفقه و القضاء و التشريع في هذا الرأي .

الفرع الأول: معايير تحديد الاختصاص القضائي بالنسبة لجريمة الاحتيال المعلوماتي وفقا للآراء الفقهية :

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 التقليد بر الانترنت ،حيث يرجع الاختصاص إما لمحكمة المكان الذي أرتكب فيه التقليد وإما لمكان نشره بالإضافة إلى هذه المعايير تم الإيجاد معايير أخرى مرتبطة أيضا بجرائم المرتكبة ضد الأحداث حيث ينعقد الاختصاص في النوع من الجرائم لمكان ارتكاب الجريمة ، وقد يكون المكان الذي شوهد فيه الموقع غير مشروع .

الملاحظ من خلال مختلف هذه المعايير المستحدثة أنها تجاوزت المعايير التقليدية لانعقاد الاختصاص وجاءت بمفهوم جديد لمكان ارتكاب الجريمة الالكترونية يتماشى وينسجم مع طبيعة هذه الجرائم، مما يستدعي البحث وإيجاد معايير تتماشى مع مختلف الجرائم

إلكترونية الأخرى، فعلى سبيل المثال بالنسبة لمسالة تفتيش المعلومات والبيانات المعالجة إلكترونيا خارج إقليم الدولة ثار جدل بشأنها[1].

– **فالرأي الأول:** يرى أن من غير المشروع أن تقوم السلطات دولة ما بالتدخل وتفتيش النظم المعلوماتية الموجودة في إقليم دولة أخرى، بهدف كشف وضبط أدلة لإثبات جريمة كانت قد وقعت على أراضيها وذلك استنادا إلى مبدأ الإقليمية.

– **أما الرأي الثاني:** فيري 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 الاختصاص القضائي للجرائم التي ترتكب بواسطة شبكة المعلومات الدولية للانترانت، نجد أن معظم التشريعات قامت بتطبيقها في مسالة الاختصاص الجزائي الدولي، إلا أن طريقة تبني هذا الحل اختلفت من دولة إلى أخرى، فهناك من ساير موقف الفقه وهناك من ساير موقف القضاء، وهناك جانب أخر أتبع الاتفاقيات الدولية.

أولا : تطبيق مبدأ الإقليمية على جريمة الاحتيال المعلوماتية:

يقصد بمبدأ إقليمية القانون الجزائي لدولة ما يطبق على كل جريمة ترتكب على إقليم هذه الدولة سواء أكان الجاني يحمل جنسية هذه الدولة أم يحمل جنسية دولة أجنبية وسواء أكان المجني عليه مواطنا أم أجنبيا.

ويجب التذكير بأن المحكمة المختصة وكذا سلطة التحقيق المختصة وفقا لمبدأ الإقليمية الذي يسود معظم التشريعات المقارنة هي محكمة المكان الذي وقعت فيه الجريمة أو جزء منها أي وقع فيه الركن المادي أو جزء منه وإذا طبقنا ذلك على جريمة الاحتيال المعلوماتية نتذكر أن جريمة الاحتيال من الجرائم المركبة، حيث يتشكل فيها الركن المادي من أولا ممارسة احد

[1] –عادل عبد العال إبراهيم خراشي،إشكاليات التعاون الدولى في مكافحة الجرائم المعلوماتية و سبل مكافحتها،دار الجامعة الجديدة مصر سنة2015ص7 .

الطرق الاحتيالية من الجرائم المركبة حيث يتشكل فيه الركن المادي من أولا ممارسة أحد الطرق الاحتيالية، ثانيا: الاستيلاء على مال الغير وثالثا: علاقة السببية، التي تتمثل في إقناع المتهم المجني عليه بتسليم مله وحدوث هذا التسليم بناءا على ذلك وبالتالي فإن المحكمة المختصة بمحاكمة المتهم في جريمة الاحتيال المعلوماتية هي تلك المحكمة التي تمارس في دائرتها المتهم نشاطه الاحتيالي وكذلك محكمة المكان الذي تم فيه تسليم المال وفي هذا الصدد انقسم رأي الفقهاء إلى ثلاث اتجاهات لتحديد مكان وقوع الجريمة مذهب السلوك أو النشاط الإجرامي بوصفه معيارا لتحديد مكان وقوع الجريمة.

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

على الرغم من الحجج التي جاء بها الاتجاه الأول إلا أنه تعرض لجملة من الانتقادات من جانب أخر من الفقه وهي أن الاتجاه الأول لم يبدي اهتماما للمكان الذي تحقق فيه الضرر أو النتيجة الإجرامية، كما أن تمام الجريمة لا يكون إلا في المكان إلي ظهرت فيه أثارها الضارة التي كان الجاني يقصدها أو يرغب في تحقيق أثارها ، بالإضافة إلى أن تقادم الجريمة يبدأ احتسابه من الوقت الذي تحققت فيه النتيجة الجريمة ،كما يؤخذ في الحسبان جسامة الضرر كأساس لتقدير التعويض وأن الضرر شرط أساسي لقيام المسؤولية المدنية فهذا الاتجاه يأخذ بمبدأ وحدة الجريمة وعد الفصل بين عناصرها، كذلك يمتاز في نظر المدافعين عنه بأنه أكثر واقعية على اعتبار 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 امتناع أي فعل سلبي، وقد تم تبنيه في بعض التشريعات المقارنة منها القانون الألماني.

- **المذهب المختلط**

أمام الانتقادات التي تعرض لها كلا الاتجاهين السابقين برز اتجاه الثالث يرى أن الجريمة تعد واقعة في مكان حصول النشاط الإجرامي (العمل التنفيذي) وكذلك المكان الذي تحققت فيه النتيجة الإجرامية أو الذي من المتوقع أو من المنتظر تحقيها فيه وهذا الاتجاه حضي بموافقة أغلب الفقه، ويعد مبرره في أن الركن المادي لجريمة يقوم على ثلاثة عناصر، وهي الفعل أي نشاط الإجرامي والنتيجة والعلاقة السببية، وما يعني أن الجريمة وقعت في كل مكان تحقق فيه عنصر من عناصر الركن المادي للجريمة وهذا الاتجاه أخذت به بعض التشريعات المقارنة منها قانون العقوبات النرويجي وكذلك الدنماركي و الصيني و الايطالي كما تبنته محاكم بعض الدول ، منها فرنسا في عدد من الأحكام إذا ذهبت إلى أن اختصاصها يمتد ليشمل كل الأمكنة التي كانت مسرحا للجريمة وقت وقوعها.

وتجدر الإشارة إلى أنه بالرجوع إلى مبررات التي استند إليها كل اتجاه فإن الاتجاه الثالث هو الأرجح لأنه تجاوز ما أخد به كل من الاتجاهين الآخرين، كما أنه وسع في نطاق الحماية الجزائية وفي تمديد الاختصاص القضائي و بالتالي يمكن اعتباره اتجاه شامل و جامع[1].

إلا أن 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 الآمر حد نزع الصفة المادية كلية عن هذا الفعل.

وهكذا تعتبر مجرد مكالمة هاتفية مع شخص في دولة أخرى مبررا لاعتبار الجريمة وقعت فوق إقليم الدولة وبالتالي يجب صياغة معيار الاختصاص الإقليمي للجريمة الالكترونية وفالمثل هذه المعطيات الجديدة: تطبيق المبادئ الأخرى على الجريمة الآحتيال المعلوماتية:

[1] – هشام محمد فريد رستم،الجوانب الإجرامية المعلوماتية ،مكتبة الآلات الحديثة للنشر ،سنة 1994 ،ص 70 .

تجدر الإشارة إلى أن تقدم العلمي الرهن وتطور وسائل الاتصال الحديثة كالانترنت وسائر صور الاتصال ت الالكتروني عبر الأقمار الصناعية، أتاح فرصا هائلة لخروج على مبدأ الإقليمية وتبني معايير جديدة ،لفض مسألة تنازع الاختصاص القضائي لآن معيار الآقليمية 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.

أ- مبدأ العينية:

يقصد بمبدأ الذاتية أو العينية بتطبيق القانون الجزئي على الجرائم التي تمس المصالح الأساسية للدولة، والمرتكبة خارج إقليمها أي كانت جنسية مرتكبها، وهذا المبدأ يفرضه حرص الدولة على حماية مصالحها الأساسية مثل ارتكاب جناية أو جنحة مخلة بأمن الدولة أو تقليد خاتم لدولة أو تزوير عملة أو سندات مصرفية وتطبيقا لذلك فإن جريمة الآحتيال المعلوماتي ليست ضمن الجرائم التي تمس بالمصالح الأساسية للدولة.

ب- مبدأ الشخصية:

يقصد بمبدأ الشخصية كلاحقة القانون الوطني للأشخاص الذي يحملون جنسية الدولة ، بينما وجدوا وليحكم أفعالهم الإجرامية المرتكبة في الخارج ويطبق مبدأ الشخصية بطريقتين إيجابية وسلبية ويقصد بالطريقة الايجابية تطبيق القانون الجزائي على مرتكب الجريمة الذي يحمل جنسية الدولة ولو ارتكبت الجريمة خارج إقليمها ، وهذا لتجن 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 الاعتداءات الجرمية عليهم.

وتجدر الإشارة غل أن المشرع الجزائري نص على الاختصاص الشخصي في المادتين من ق. إ.ج برط أن كون الجاني متمتعا بالجنسية الجزائرية وإن كان الجاني مزدوج الجنسية فالعبرة بالجنسية الجزائرية[1].

ج- مبدأ العالمية أو الصلاحية الشاملة:

ينطوي هذا المبدأ على نوع من التعاون الدولي في مكافحة الإجرام، فهو يضمن عدم إفلات المجرمين الذين سولت لهم أنفسهم ارتكاب جرائم في الدولة ما ثم الفرار إلى دولة أخرى تملصا من المسؤولية .

وعليه فالأجنبي الذي يرتكب جريمة في الدولة ويلقى القبض عليه في .... من الدول المتنازعة وفقا لأحد المعايير الاختصاص دولة أخرى ويمكن محاكمته في الدولة التي ألقى القبض عليه فيها بشرط أن لا تطلب الدولة التي أرتكب فيها الجرم تسليمه لها.

وتطبيقا لذلك إذا قام هولندي موجود في الخارج مثلا اختراق النظام المعلوماتي لمصرف إيطالي وتحويل الأرصدة إلى حسابه احتياليا، ثم حضر غلى الجزائر وألقي عليه فيها القبض فيمكن محاكمته وفقا لمبدأ العالمية[2].

وبناءا على ما تقدم، فإننا لا نجد مانعا من تطبيق مبدأ الإقليمية ومبدأ العينية ومبدأ الشخصية ومبدأ العالمية، على جريمة الاحتيال الالكتروني أو أحد الجرائم المعلوماتية الأخرى لآن القواعد الإجرائية الجزائية يمكن تفسيرها تفسيرا موسعا إضافة غلى إمكانية اللجوء للقياس عند فقدان النص الإجرائي، وذلك خلافا القواعد الموضوعية وبالتالي للتغلب على التنازع الايجابي للاختصاص يجب إعطاء الأولوية لآي من الدول المتنازعة وفقا لأحد معايير

---

[1]- محمد طارق عبد الرؤوف ،الحق جريمة الإحتيال عبر الإنترنت الأحكام الموضوعية و الأحكام الجزائية،منشورات الحلبي الحقوقية ص 220 .

[2]- مؤمون محمد سلامة،قانون العقوبات ،القسم العام،دار النهضة العربية،ط2 ،سنة2001 ،ص 77 .

الاختصاص الأكثر جدوى وفعالية لضمان ملاحقة الجريمة ويبدوا الإقليمية هو أكثر قبولا فالدولة التي يقع في إقليمها الجريمة كلها أو بعضها جزء من النشاط الإجرامي المكون لركنها المادي أو النشاط التبعي له أو بصفة عامة الدولة التي يوجد في إقليمها متحصلات الجريمة تبدوا أرجح الدول اختصاص جاء بملاحقته الجريمة ومتابعة فاعليها ، ولا يجد هذا الحل مبررا فقط في اعتبارات وإنما أيضا في جدواه العملية حيث أنه أين تقع الجريمة كلها أو جلها تصبح أدلة الآثبات متوافرة ويصبح من السهل إجراء تحقيقات الكفيلة لإظهار الحقيقة ، ثم يأتي بعد مبدأ الإقليمية ، مبدأ الإقليمية حيث يكون هو الملائم لمعظم الجرائم الالكترونية التي يتوزع الاختصاص للدولة التي يحمل جنسيتها مرتكب هذه الجريمة فإن تعددت جنسياته.

الفرع الثاني: موقف المشرع الجزائري و التشريعات المقارنة من مسألة الاختصاص القضائي:

تعددت القوانين الجزئية التي يمكن أن تحكم جرائم الشبكة المعلوماتية بتعدد الدول المرتبطة بها، لآن المشكلة الأساسية تكمن في أنها لا تعرف حدودا جغرافية وليست ملكا لأحد و لا تخضع لسيادة دولة معينة.

أولا: موقف المشرع الجزائري من مسألة الاختصاص القضائي المحلي:

حدد المشرع الجزائري معايير الاختصاص المحلي للجرائم المعلوماتية في قانون الإجراءات الجزائية في المواد ،40،37،329 ونجد أن المشرع الجزائري تخطى مشكلة امتداد التفتيش خارج الإقليم الوطني بموجب ما رسمه القانون.

لطن المشكل الاختصاص القضائي وملائمة القانون الواجب التطبيق تظل قائمة في مجال الجرائم المعلوماتية لأنه وإن بادر المشرع الجزائري بتعديل قانون الإجراءات الجزائية بموجب القانون14/04 المؤرخ في 2004[1]/11/10، حيث عدل المادة 329 من قانون الإجراءات الجزائية وذلك لجواز تمديد الاختصاص المحلي للمحكمة، ليشمل اختصاص محاكم

1- القانون رقم 04-14 المؤرخ في 10 نوفمبر 204 المعدل للأمر 66-156 المتضمن ق الإجراءات الجزائية جريدة رسمية رقم 71.

أخرى عن طريق تنظيم في الجرائم.المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة، وقد جاء عقب ذلك المرسوم التنفيذي رقم:348/06 [1] المؤرخ في 2006/10/05 والمتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق ، ليجسد فعلا بموجب المادة الأولى منه مجال اختصاص بعض المحاكم في إطار الجرائم الماسة بالأنظمة المعالجة الآلية للمعطيات.... لآن مشكلة الاختصاص القضائي المحلي تضل قائمة إذا وقعت النتيجة الإجرامية في إقليم الدولة الأجنبية .

1- اختصاص وكيل الجمهورية:

نصت المادة 37 من قانون الإجراءات الجزائية على الاختصاص المحلي لوكيل الجمهورية يتحدد بمكان وقوع الجريمة أو بمحل إقامة الأشخاص المشتبه في مساهمتهم في اقترافها أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب أخر.

ومن المستجدات التي أستحدثها المشرع الجزائري في تعديل قانون الإجراءات الجزائية لسنة2004-2006 وما يتعلق بتمديد الاختصاص ، بحيث نصت المادة 2/37 يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية و الجرائم المسماة بالمعالجة الآلية للبيانات و المعطيات وجرائم تبييض الأموال والإرهاب والجرائم الخاصة بتشريع الصرف.

ب- اختصاص قاضي التحقيق:

بالنسبة لقاضي التحقيق نصت المادة 40 /1 على أن اختصاصه المحلي بتحدد بمكان وقوع الجريمة أو محل إقامة أحد المشتبه في مساهمتهم في اقترافها، أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان القبض قد حصل لسبب أخر.

[1] - مرسوم تنفيدي رقم 06-348 المؤرخ في 2006/11/05 جريدة رسمية رقم 63 صادرة بتاريخ 11/08/ 2006.

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

ج- الاختصاص المحلي لجهات الحكم

عدل المشرع الجزائري الاختصاص المحلي بالنسبة لجهات الحكم حيث نصت المادة 329 من قانون الإجراءات الجزائية المعدلة بموجب القانون رقم:14/04 السالف الذكر، تختص محليا بالنظر في الجنحة المحكمة محل ارتكاب الجريمة أو محل إقامة أحد المتهمين أو شركائهم، أو محل القبض عليهم ولو كان هذا القبض قد وقع لسبب آخر.

وعن معيار مكان وقوع الجريمة فهو يختلف حسب طبيعة الجريمة إذا تحدد بالنسبة للجريمة الوقتية بالمكان الذي وقع فيه تنفيذ الفعل، وبالنسبة للجريمة المستمرة ويتحدد بكل مكان قامت فيه حالة استمرار الفعل، وبالنسبة للجرائم المتتابعة يعتبر مكان ارتكاب الجريمة كل مكان تقع فيه أحد الأفعال[1].

لكن الاختصاص لا يثير أي إشكال عندما يتعلق بالجرائم المعلوماتية المرتكبة داخل الإقليم الجزائري، وإنما الأشكال يكمن في الجريمة المعلوماتية التي تمتد مجريات التحقيق و التحري فيها خارج الإقليم الجزائري، إذا أن الوضع كهذا بصدد عولمة الجريمة.

---

[1] جدي نسيمة,جرائم المساس بأنظمة المعالجة الآلية للمعطيات,مذكرة لنيل شهادة الماجستير في القانون الجنائي سنة 2014/2013

وقد حاول المشرع الجزائري إيجاد حل لهذه النقطة، إذا نص في المادة 15 من قانون 04/09 [1]على:أنه وفضلا عن الاختصاص المنصوص عليه في قانون إجراءات الجزائية،تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجانب وتستهدف مؤسسات الدولة الإستراتجية الاقتصاد الوطني أو الدفاع الوطني أو المصالح العامة للدولة.

ثانيا: موقف التشريعات المقارنة من مسألة الاختصاص القضائي:

بالرغم من لجوء معظم التشريعات إلى مبدأ إقليمية النص الجزائي والمبادئ الأخرى المشار إليها لحل مشكلة الاختصاص القضائي المعلوماتي، إلا أن طريقة تبني لحل اختلفت من دولة لآخري.

ثانيا: موقف التشريعات المقارنة من مسألة الاختصاص القضائي:

بالرغم من لجوء معظم التشريعات إلى مبدأ إقليمية النص الجزائي والمبادئ الأخرى إليها المشار إليها لحل مشكل الاختصاص القضائي المعلوماتي، إلا أن طريقة تبني الحل اختلفت من دولة لآخري.

أ – موقف المشرع البريطاني:

بموجب قانون إساءة استعمال الكمبيوتر لعام 1990، فإن القضاء البريطاني يختص بالجرائم التي تنص عليها هذا القانون، إذا اقترفت ضمن الاختصاص الإقليمي للدولة، أي إذا كان الحاسوب الجاني أو حاسوب الضحية داخل إقليم الدولة، كما تم إحداث اختصاصات

القانون رقم 09-04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام [1]و الاتصال جريدة رسمية رقم 47 مؤرخة في 2009/08/16.

قضائية جديدة بموجب قانون العدالة الجزائية البريطاني لعام 1993، حيث تناولت هذه الاختصاصات معظم الجرائم الاحتيال العابرة للحدود وغيرها[1].

ب- موقف المشرع الفرنسي:

تضن قانون العقوبات الفرنسي لعام 1992 القواعد المتعلقة بتنازع الاختصاص من حيث المكان والمنصوص عليه في المواد من 113-إلى 7/113، وقد تضمنت هذه القواعد مبادئ الآقليمية والعينية والشخصية التي قام القضاء الفرنسي بتطبيقها على جرائم الآنترنات

فجاء في مضمون التشريع الفرنسي أنه يطبق على جرائم المرتكبة داخل الإقليم الجمهورية الفرنسية وهذا حسب نص المادة 113فقرة 5 من قانون العقوبات.

وبالرجوع للمادة 2/113 من نفس القانون يكفي فقط تحقق أحد التاركان المكونة للجريمة لتطبيق النص الفرنسي، وهذا ما حكمت به محكمة باريس في حكمها بتاريخ2002/02/26 والذي قضت فيه بان القاضي الفرنسي مختص في إرتكاب الجرائم المعلوماتية، ومتى تحقق أحد أركان الجريمة على الإقليم الفرنسي.

كما يطبق النص الفرنسي أيضا على الرسائل الغير مشروعة المرسلة عبر شبكة الآنترنات في فرنسا مهما ما كان الموقع المرسل في العالم ، فبمجرد تلقي المرسل غليه الرسالة يشكل ذلك النتيجة الإجرامية والتي تعد أحد أركان الجريمة المعلوماتية، وهذا ما قضت به الغرفة الجزائية لمحكمة النقض في قرار لها بتاريخ2007/02/07.

المطلب الثاني: موقف الاتفاقيات الدولية حول مسألة تنازع الاختصاص.

لا يمكن أن تثار مشكلة تنازع الاختصاص على مستوى الداخلي للدول، وإنما المسألة ترح عندما يعطي الاختصاص لأكثر من دولة بسبب إختلاف جنسية وتعدد المكان الذي

[1]- زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري و الدولى، دار الهدى عين مليلية ،الجزائر ،ص174.

ارتكبت فيه الجريمة والحل، الأمثل لهذه المشكلة هو إبرام الاتفاقيات الدولية الثنائية أو متعددة الأطراف التي تتوحد من خلالها وجهات نظر الدول وتحدد ضوابط الاختصاص الإقليمي لكل دولة وتظهر معالم هذا التعاون في قبول حالات تفويض الاختصاص في اتخاذ إجراءات التحقيق وجمع الأدلة و الاعتراف بالأحكام الجنائية الأجنبية.

الفرع الأول: توصيات المجلس الأوربي و الإصلاحات الجديدة في مجال الجرائم المعلوماتية:

نظرا للتطور السريع في مجال تكنولوجيا الكمبيوتر و الآنترنات وشعور الدول الأوربية بأهمية النظر في الإجراءات الجزائية في هذا المجال، أصدر المجلس الأوربي التوصية رقم13/90 في 1995/09/11 تناولت المشاكل الإجراءات الجزائية المتعلقة بتكنولوجيا المعلومات، جاء فيها لأن يفترض التحقيق مد الإجراءات إلى الأنظمة حاسب ألي أخر قد تكون موجودة خارج الدولة وتتطلب التدخل السريع، وحتى لا يمثل مثل هذا الأمر اعتداء على سيادة الدولة أو القانون الدولي وجب وضع قاعدة قانونية صريحة تسمح بمثل هذا الإجراء ولذلك كانت الحاجة ملحة لإبرام اتفاقيات تنظم وقت وكيفية اتخاذ مثل هذه الإجراءات[1].

كما يجب أن تكون هناك إجراءات سريعة ومناسبة ، ونظام إتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة ويتعين عندئذ أن تسمح السلطة الأخيرة بإجراء تسجيلات للتعاملات الجارية وتحديد مصدرها وهذا كله لا يتأتى إلا باتفاقيات دولية.

الفرع الثاني الاتفاقيات الأوربية حول جريمة الافتراضية بودابست: تشكل نصوصها منظومة تعاون ولي تتسم بالمرونة وتعمل على إحداث تقارب بين التشريعات الجنائية الخاصة بهذه الجرائم ،وتكفل إستخدام الوسائل الفعالة في البحث والتحقيق وما يتعلق بالنصوص الخاصة بالتعاون الدولي.

[1]- عادل عبد العال إبراهيم خراشي،ص79 .

نصت المادة 22 من هذه الاتفاقية إلى المبادئ التي يجب اعتمادها من قبل الأطراف 383 لتحديد اختصاص القضائي فيما يتعلق بالجرائم المنصوص عليها في اتفاقية وهذه المبادئ هي:

أولا: مبدأ الإقليمية:

نصت الاتفاقية على هذا المبدأ في الفقرة 1 البند أ من المادة 22 وطبت من كل دولة طرف في هذه الاتفاقية أن تعاقب على الجرائم المنصوص عليها إذا ارتكبت الجريمة ضمن نطاق الجغرافية للدولة.

فاعلي السبيل مثال: يعد هذا اختصاص منعقد، إذا كان نظام الحاسوب العائد للمتعدي ضمن الإطار الإقليمي ولو كان المعتدي مقيم خارج الدولة ، أو إذا كان نظام الحاسوب العائد للضحية في إطار الإقليمي لدولة ، كما يعد الاختصاص الإقليمي متوفر إذا كان مصدر الإرسال أو جهة الوصول داخل إقليم الدولة .

ثانيا :مبدأ النسبية الاختصاص المكاني (إقليم اعتباري)

نصت الاتفاقية على هذا المبدأ في الفقرة 1 البندين "أ" و "ب" من المادة 22 وطلب من كل دولة طرفا في هذه الاتفاقية أن تكون مختصة جزائيا بالجرائم المرتكبة على السفن التي ترفع علم الدولة أو الطائرات المسجلة وفقا لقانون فيها [1] .

وعلى الرغم من ضرورة التعاون الدولي و تضافر الجهود من أجل تفعيله، إلا أن هناك العديد من العقبات التي تعترض سبيله من أبرزها : عدم وجود اتفاق عام بين الدول على مفهوم الجرائم الالكترونية.

عدم وجود توافق بين قوانين الإجراءات الجزائية للدول بشأن تحقيق في تلك الجرائم ونقص الظاهر في مجال الخبرة لدى الشرطة وجهات الادعاء و القضاء.

ثالثا: مبدأ الجنسية

[1]– محمد طارق عبد الرؤوف الحق مرجع سابق ص 202 .

نصت الاتفاقية على هذا المبدأ في الفقرة 1 البند د من المادة 22، وطلبت من كل دولة طرف في هذه الاتفاقية أن تكون مختصة جزائيا عندما يرتكب مواطنوا أي من هذه الدول جريمة في الخارج، إذا كان هذا السلوك يشكل الجريمة وفقا للدولة التي ارتكبت على أرضها الجريمة[1].

رابعا : مبدأ التعاون الدولي في مكافحة الإجرام أو الصلاحية الشاملة أو العامية:

نصت الاتفاقية على هذا المبدأ في الفقرة 3 من المادة22 والتي تنص بأنه في حال رفض أي دولة طرف في هذه الآتفاقية تسلم مرتكب الجريمة المتواجد على أرضها وعلى أساس مبدأ الجنسية فيجب على هذه الدولة الرافضة القيام بإجراءات التحقيق والمحاكمة وفقا لقانونها الوطني.

وإذا كانت جريمة الحاسوب تدخل في اختصاص أكثر من دولة من الدول الأطراف مثل جريمة الاحتيال وجرائم العدوان الفيروسي، فن على هذه الدول التشاور فيما بينها لتحديد مكان الملائم للمحاكمة[2].

كما نصت الاتفاقية في المادة 29 منها على أنه يحق لكل طرف أن يطلب من الطرف الأخر الحفظ السريع للمعلومات المخزنة، عن طريق إحدى الوسائل الكترونية الموجودة داخل النطاق المكاني لذلك الطرف الآخر، والتي ينوي الطرف الطالب المساعدة أن يقدم طلبا للمساعدة بشأنها بغرض القيام بالتفتيش أو لدخول بأي طريقة مماثلة أو الحصول أو الكشف على البيانات المشار إليها 385.

الفرع الثالث: القانون العربي الاسترشادي (النموذجي بشأن مكافحة الجرائم التقنية و أنظمة المعلومات 2004:

---

[1]– محمد طارق عبد الرؤوف الحق مرجع سابق ص210

[2]– طارق إبراهيم الدسوقي عطية،الأمن ألمعلوماتي النظام القانوني لحماية المعلوماتية، دار الجامعة الجديدة ،الإسكندرية، سنة 2015، ص576 .

تناول القانون العربي النموذج بشان مكافحة جرائم الكمبيوتر و الآنترنات مسألة تنازع الاختصاص القضائي الدولي وذلك في المادة 22 من هذا القانون تحت عنوان إطار تطبيق القانون على ما يلي تسري أحكام التشريع الجنائي للدولة على الجريمة المعلوماتية إذا إرتكبت كليا أو جزئيا داخل حدودها وفقا لمبدأ الإقليمية كما تختص المحاكم فيها بنظر الدعوى المترتبة على تلك الجرائم وعلى الدول العربية عقد إتفاقيات لتبني المعيار الأول بإتباع في حالة تنازل الاختصاص بين الدول[1].

كما يسري التشريع الجنائي للدولة على الجرائم المعلوماتية التي تقع خارج الحدود ،إذا كانت نخلة بأمنها وفقا للقواعد العامة المنصوص عليها في قانون العقوبات

وقد تناول هذا النص مسألتي القانون الواجب التطبيق والمحاكم المختصة بشأن الجرائم المعلوماتية 386.

يلاحظ من النص المادة السالفة الذكر أنه لكي أخد بمبدأ شخصية القانون الجنائي ، النص الجنائي وعلى ذلك أيا كان نوع الجرائم المعلوماتية وسواء وقعت على الشبكة المعلوماتية داخلية أو عن طريق الانترانت وسواء كان ذلك داخل الدولة أو خارجها شرط أن يكون القانون الوطني صالحا للتطبيق عليها فإن المحاكم الوطنية هي المختصة دون غيرها بالنظر في هذه الجرائم.

الفرع الرابع : الاتفاقية العربية لمكافحة الجرائم التقنية المعلومات رقم 19 لسنة 2012:

تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة الجرائم التقنية المعلوماتية للوقاية من أخطار هذه الجرائم والتحقيق فيها وملاحقة مرتكبيها وبالنسبة لمسألة الاختصاص نصت المادة 30 من الاتفاقية على أنه :

[1] – طارق إبراهيم دسوقي عطية نفس المرجع ص 577 .

1- تلتزم كل دولة طرف في تبني الإجراءات الضرورية لمدة اختصاصها عن الجرائم المنصوص عليها في افصل الثاني من هذه الاتفاقية وذلك إذا ارتكبت الجريمة كليا أو جزئيا أو تحققت :

أ- في إقليم الدولة الطرف:

ب- على متن السفينة تحمل علم الدولة الطرف

ج-على متن طائرة مسجلة تحت قوانين الدولة الطرف.

د- من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة مرتكبة من مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي فيه مكان ارتكابها أو إذا ارتكبت خارج المنطقة اختصاص القضائي لأي دولة .

هـ- إذا كانت الجريمة تمس أحد المصالح العليا للدولة

1- تلتزم كل دولة طرف بتبني إجراءات الضرورية لمد الاختصاص الذي يغطي الجرائم المنصوص عليها في المادة 31 /1 من هذه الاتفاقية في الحالات التي يكون فيها الجاني المزعوم حاضر في إقليم تلكمه إل الدولة الطرف ولا يقوم بتسلمه إلى طرف أخر بناءا على جنسية بعد طلب تسليم.

2-إذا أدعت أكثر من دولة طرف في الاختصاص القضائي المنصوص عليها في هذه الاتفاقية فيقدم طلب الدولة التي أخلت الجريمة بأمنها أو مصالحها تم الدولة التي وقعت الجريمة في إقليمها ثم الدولة التي يكون الشخص المطلوب من رعاياها وإذا أتحدث الظروف تقدم الدولة الأسبق في الطلب التسليم في المادة 387[1] .

بناءا على ما تقدم وبما أن قواعد الإجرائية بخلاف القواعد الموضوعية يمكن تفسيرها تفسيرا موسعا إضافة إلى إمكانية اللجوء إلى القياس، لا نجد مانعا من تطبيقا مبدأ الإقليمية

[1] - طارق إبراهيم دسوقي عطية ، نفس المرجع ص 580 .

والعينية و الشخصية على جريمة النصب المعلوماتي، كما نقترح على المشرع الجزائري معالجة مسالة الاختصاص القضائي من مختلف جوانبها ، في الجرائم الإلكترونية[1].

المبحث الثاني نظام الإثبات في جريمة النصب بالاستعمال الوسائل المعلوماتية (نصب معلوماتي):

المطلب الأول إثبات جريمة النصب المعلوماتية بوسائل الإثبات التقليدية:

إن التعامل في الجريمة المعلوماتية تتطلب إجراءات روتينية متفق عليها وذلك من أجل حماية الدليل، غير أن وسائل حفظ الأدلة واستنتاجها تختلف من الجريمة التقليدية إلى الجريمة المعلوماتية الرقمية سنحاول التركيز على الجريمة المعلوماتية بصفة عامة كونها شاملة من جهة و من جهة أخرى فجريمة النصب ألمعلوماتي تعتبر جريمة معلوماتية و تعتمد بشكل رئيسي على نظام المعلومات.

الفرع الأول :المعاينة في الجرائم المعلوماتية و جريمة النصب :

[1] – محمد طارق عبد الرؤوف الحق، مرجع سابق ص221 .

تعتبر المعاينة من أهم إجراءات التحقيق والتي يمكن من خلالها الحصول على الدليل الجنائي بحيث يجوز للنيابة العامة أن تقوم به في غيبة المتهم إذا لم يتيسر له حضوره، وباعتبار أن المعاينة لها أهمية قصوى فسوف نتناولها من عدة جوانب.

أولا :الإطار القانوني للمعاينة في الجرائم المعلوماتية:

ينبغي عند التطرق للإطار القانوني للمعاينة الوقوف عند التعريف بها، وتبيان أهميتها وطبيعتها، والسلطة المختصة بإجرائها وكيفية الانتقال، وشروط معاينة مسرح الجرائم المعلوماتية والذي سنورده كالتالي:

1 – تعريف المعاينة وطبيعتها وأهميتها في مجال الجرائم المعلوماتية:

1 – 1 تعريف المعاينة:

يقصد بالمعاينة الانتقال إلى الأماكن التي وقعت فيه الجريمة لإثبات حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة عن الجريمة وعن مرتكبها، وبالتالي يجب على السلطات المختصة بإجراء المعاينة الانتقال إلى أماكن وقوع الجريمة فور ارتكابها، حتى لا يكون هناك فارق زمني طويل بين وقوع الجريمة وإجراء المعاينة التي تسمح للجاني بتغيير أو إزالة كل أو بعض الآثار المادية للجريمة التي تساعد في التنقيب عن الحقيقة، وحتى لا يقع الشك في الدليل المستنبط منه وهذا ما تضمنته نص المادة **42** من قانون الإجراءات الجزائية الجزائري[1] .

1-2- السلطة المختصة بإجراء المعاينة لمسرح الجرائم المعلوماتية:

الأصل أن انتقال المحقق الجنائي لإجراء المعاينة أو لمباشرة أي إجراء آخر من إجراءات التحقيق أمر متروك للسلطة التقديرية له، فلا يقوم به إلا إذا كانت مصلحة من ورائه

---

[1]– عمرو حسين عباس،" بحث في أدلة الإثبات الجنائي والجرائم الإلكترونية المعلوماتية، بحث مقدم إلى المؤتمر الإقليمي الثاني حول تحديات تطبيق الملكية الفكرية في الوطن العربي، خلال الفترة من26 –2008/04/27 ، مقر جامعة الدول العربية ، ص 16 ، أنظر الموقع الإلكتروني . www.arabip.center.com/public/events/papers/paper 2-4. pdf .

– وانظر المادة 42 من قانون رقم 66–155 المتضمن قانون الإجراءات الجزائية المعدل و المتمم بالقانون رقم 06–22 ، المؤرخ في 2006/12/20 ج.ر.ع 84 المؤرخة في 2006/12/24.

لذلك جرى أن المعاينة هي من إجراءات التحقيق التي يترك أمر تقدير لزوم القيام بها إلى السلطة التي تباشر التحقيق [1]، وهذا ما قضت به نص المواد (79،80، 42) من قانون الإجراءات الجزائية الجزائري على أن المعاينة تجرى إما من طرف قاضي التحقيق، وذلك بعد إخطار وكيل الجمهورية الذي له الحق في مرافقته، وكما يمكن تمديد اختصاص قاضي التحقيق إذا استدعت ضرورة الحالة إلى دوائر اختصاص محاكم مجاورة، كما يتم أيضا إجراء المعاينة من طرف ضباط الشرطة القضائية الذين عليهم إخطار وكيل الجمهورية فور وصول خبر وقوع الجريمة إلى علمهم وانتقالهم بدون تمهل إلى أماكن الواقعة الإجرامية.

2- شروط صحة معاينة مسرح الجرائم المعلوماتية:

حتى تحقق المعاينة الغرض المرجو منها في كشف غموض الحادث ومعرفة الفاعل يجب التقييد بعدة شروط كالتالي:

2-1 سرعة الانتقال إلى مكان وقوع الجريمة المعلوماتية:على السلطة المختصة بالتحقيق الانتقال فور وصول خبر وقوع الجريمة إلى علمها إلى مكان الواقعة[2].

2-2 السيطرة والتحكم على مكان وقوع الجريمة المعلوماتية: عند وصول سلطة التحقيق لمكان الحادث لمعاينته وجب أن تقوم بالسيطرة عليه وذلك:

- بمنع أي شخص من مبارحة مكان الواقعة ريثما تنتهي الضبطية القضائية من تحرياتها [3].

- منع تواجد أي شخص بداخل مسرح الجريمة حتى لا يؤدي إلى تغيير الآثار والأدلة المستمدة من الواقعة سواء بقصد أو بخطأ.

-حماية كل ما له علاقة بالحادث من وسائل وأشياء وأشخاص.

-قيام الخبراء كل حسب اختصاصه برفع الآثار بمسرح الجريمة.

---

[1]-عبد الفتاح بيومي حجازي، مرجع سابق، ص 102.

[2]- راجع المادة 42 من ق إ.ج.ج.

[3]-المادة 50 من ق .إ.ج.ج .

2- 3 الترتيب في المعاينة:ولضمان إجراء معاينة بصورة مرتبة ومتسلسلة ينبغي على السلطة المختصة الالتزام بالطرق التالية:

-تحديد نقاط البدء في المعاينة.

-عدم الانتقال من مكان لآخر إلا بعد التأكد من معاينته تماما [1].

2-4 الدقة والعناية الفائقة في معاينة مسرح الجرائم المعلوماتية: وذلك بوصف المنطقة التي ارتكبت فيها الجريمة، وإذا كانت هذه الأخيرة داخل مبنى فيجب معاينة كل منافذ الدخول والخروج، وكذا وصف المحتويات فيما هو مرتبط بالجريمة، كأجهزة الكمبيوتر والماسح الضوئي (السكانير) والطابعة والأسطوانات المدمجة، وغير ذلك من الوسائل المستخدمة في اقتراف الجريمة المعلوماتية.

2-5 التحفظ على مسرح الجرائم المعلوماتية بعد المعاينة: لأن الهدف من الحفاظ على آثار الجريمة بعد انتهاء من المعاينــة هو مــن أجل إمـكانية العودة إليه كّلما أراد المحقق أو القاضي كشف غموض أو التأكد من آثار معينة.

2-6 تدوين المعاينة:ويكون ذلك كتابيا ورسميا وتصويريا.

ثانيا معاينة مسرح الجرائم المعلوماتية:

يتولى قاضي التحقيق معاينة الآثار التي خلفها مستخدم شبكة الانترنت والتي تتمثل في الرسائل المرسلة منه أو التي يستقبلها وكل الاتصالات التي قام بها من خلال الكمبيوتر والشبكة العالمية، وكما أن الآثار الرقمية المستمدة من أجهزة الكمبيوتر قد تكون ثرية فيما تحتويه من معلومات مثل صفحات المواقع المختلفةWeb pages والبريد الإلكترونيemail ، الملفات المخزنة في الكمبيوتر الشخصي ،files stare... الخ.

- **الخطوات الواجب مراعاتها قبل الانتقال إلى مسرح الجرائم المعلوماتية:**

[1]- خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ، مرجع سابق ، ص 158-160.

– يجب على المحقق الجنائي أو ضابط الشرطة القضائية قبل الانتقال لإجراء المعاينة الالتزام بالخطوات التالية:

1– الحصول على معلومات مسبقة عن مسرح الجريمة من مالك المكان، ونوع وعدد أجهزة الكمبيوتر المتوقع مداهمتها وشبكاتها.

2– توفير الوسائل الضرورية للاستعانة بها في الفحص والتشغيل كالأجهزة والبرامج.

3– قطع التيار الكهربائي في المكان الذي تجرى فيه المعاينة لمنع الجاني من القيام بأي فعل يؤدي إلى تغيير أو محو آثار الجريمة.

4–إعداد فريق التفتيش من مختصين وفنيين [1].

ثانيا : قواعد معاينة مسرح الجريمة المعلوماتية:

1– القواعد الفنية لمعاينة مسرح الجريمة المعلوماتية:

باعتبار أن لمعاينة مسرح الجريمة المعلوماتية فائدة في كشف الحقيقة عنها وعن مرتكبها، فإن عند مباشرتها لابد من مراعاة قواعد وإرشادات فنية أهمها ما يلي:

– تصوير الحاسب والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة بمكانه مع التركيز بوجه خاص على تصوير الأجهزة الخلفية للحاسب وملحقاته، مع مراعاة تسجيل وقت وتاريخ ومكان التقاط كل صورة [2].

– عدم نقل أية مادة معلوماتية من محل الجريمة قبل إجراء الاختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أية مجالات لقوى مغناطيسية) ممرات مغناطيسية (يمكن أن تتسبب في محو البيانات المسجلة

–القيام بحفظ المستندات الخاصة بالإدخال والمخرجات الورقية للحاسب التي لها صلة بالجريمة، لرفع ومضاهاة ما قد يوجد عليها من بصمات.

---

[1]– نبيلة هبه هروال، مرجع سابق،ص219 .

[2]– عبد الله حسين على محمود مرجع سابق ص 350.

– المحافظة على محتويات سلة المهملات وعدم تضييعها، مثل أوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة.الخ، وفحصها ورفع البصمات التي قد تكون على الأجزاء التي لها صلة بالجريمة المرتكبة [1].

–وضع مخطط تفصيلي للمنشأ الذي وقعت به الجريمة، مع كشف تفصيلي بالمسؤولين بها ودور كل واحد منهم [2].

2– الإجراءات الأمنية الواجب مراعاتها في مسرح الجرائم المعلوماتية:

عند وصول الفريق إلى مسرح الجريمة يقوم بالتأمين والسيطرة على المكان والبدأ بالتفتيش على النحو التالي:

– السيطرة على أماكن المحيطة بمسرح الجريمة عن طريق إغلاق الطرق والمداخل، وكذا رصد الاتصالات الهاتفية من وإلى مكان الإغارة مع إبطال أجهزة الهاتف النقال، والتحفظ على جميع الأشخاص الموجودين فيها.

– وضع حراس على كل جهاز حتى لا يتمكن أحد المتهمين من تغيير أو إتلاف المعلومات.

– تحديد أجهزة الحاسب الآلي الموجودة في مسرح الجريمة و تحديد مواقعها[3].

– القواعد التحريزية الواجب إتخاذها من مسرح الجرائم:

وتتمثل هذه القواعد فيما يلي:

– ضبط وتحريز الدعائم الأصلية للمعطيات التي لها دلالة عند عرضها للمحكمة وعدم الاكتفاء بضبط النسخ، وكذا عدم الضغط على القرص بوضع أشياء ثقيلة عليه.

– توفير الحرارة والرطوبة المناسبة لتخزين الأحراز المعلوماتية وعدم وضعها في أماكن متربة أو مغبرة، لأن ذلك يؤثر على السطح المغناطيسي مما يجعله غير قابل للقراءة أو الكتابة.

---

[1]– أحمد بلال، الحماية الجنائية لبرامج الحاسب الآلي، رسالة للحصول على درجة الماجستير في العلوم الجنائية، كلية الحقوق، جامعة القاهرة، 2007،ص246–247.

[2]–خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص173 .

[3]- عبد الله حسين على محمود، مرجع سابق، ص368 .، 36.

– حماية وتأمين البرامج المضبوطة قبل تشغيلها فنيا.

– وضع علامات مادية خاصة تميز كل دليل إلكتروني عن غيره[1]

الفرع الثاني: التفتيش في الجرائم المعلوماتية وجرائم النصب

أولا : الإطار العام للتفتيش في الجرائم المعلوماتية:

يقع التفتيش على محل منح له القانون حرمة خاصة باعتباره مستودع السرّ، وقد يكون المحل شخص أو مسكن أو محل ألحقه القانون في حكم المسكن [2]، ويباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أدلة أو أشياء يكون كشفها مفيدا لإظهار الحقيقة; و كشف المجرم المعلوماتي أو النصاب المعلوماتي [3]، وسوف نتعرض في هذا المجال إلى التعريف بالتفتيش، خصائصه، ومدى قابلية جرائم الحاسوب والشبكات الإلكترونية للتفتيش عن أدلة الجريمة.

1– تعريف التفتيش:

لا يختلف معنى التفتيش في الجريمة التقليدية عن الجريمة المعلوماتية، وبالتالي يقصد به إجراء من إجراءات التحقيق الذي يهدف الوصول إلى أدلة تفيد إظهار الحقيقة وإسنادها إلى المتهم المنسوب إليه التهمة، حيث تباشر السلطة المختصة بالدخول إلى نظم المعالجة الآلية للمعطيات بما تحتويه من مدخلات وتخزين ومخرجات، وذلك من أجل البحث عن الأفعال والسلوكات المرتكبة وغير المشروعة.والتي تشكل جناية أو جنحة [4] .

2– خصائص التفتيش:

---

[1]- من بين هذه الدستور االدساتير الجزائرية ، من خلال نص المادة 40 من قانون رقم (08-19)، المؤرخ في 15-11-2008، ج.ر.ع ، 63 المؤرخة في 16-11-2008، و المتضمن الدستور الجزائري المعدل و المتمم ، و التي تنص على ما يلي : "تضمن الدولة عدم انتهاك حرمة المسكن، فلا تفتيش إلا بمقتضى قانون..

[2]-خالد ممدوح إبراهيم، فن تحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص180 .

[3]- لمادة 81 من ق.إ.ج.ج .

[4]– علي محمود علي حموده،" الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي"، المؤتمر العالمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، منظم المؤتمر أكاديمية شرطة دبي، مركز البحوث و الدراسات ، ع 1، دبي – الإمارات العربية المتحدة 26 –28 نيسان 2003 ، ص 24.

يتميز التفتيش بناءا على التعريف السالف الذكر بعدة خصائص هي كالتالي:

2-1 أنه إجراء من إجراءات التحقيق: يعتبر التفتيش من أوامر التحقيق الابتدائي والذي يدخل ضمن الاختصاصات العادية لقاضي التحقيق، وهذا ما قضت به نص المادة **(68 - 1)** واستثناءا يجوز لضباط الشرطة القضائية القيام بهذا الإجراء بناءا على شروط وهذا ما بينته نص المادة **(17 -1)** من خلال ما يلي: يباشر ضباط الشرطة القضائية...، وإجراء التحقيقات الابتدائية " [1].

2-2 أنه يهدف إلى البحث عن أدلة مادية:

إن الهدف من التفتيش هو الوصول إلى الأدلة المادية للجريمة والتي تؤثر في اقتناع القاضي لأنه في الغالب ما يترك الجاني في مسرح الجريمة بعض الوسائل والأدوات التي يكون قد استخدمها في ارتكاب الجريمة، أو بصمات الأصبع إلى غير ذلك من الأدلة التي يستعين القاضي بها في الإثبات.

2-3 أن تكون الأدلة ناشئة عن جناية أو جنحة تحقق وقوعها:

باعتبار التفتيش عمل من أعمال التحقيق فلا يجوز إجراءه إلا إذا وقعت الجريمة بالفعل، وكانت مما يصفها القانون بجناية أو جنحة، بالتالي لا يجوز التفتيش في المخالفات نظرا لضآلتها، ولعدم خطورتها [2].

2-4 أن يقع التفتيش على محل يتمتع بحرمة المسكن أو الشخص:

يقع التفتيش على حرمة المسكن أو الشخص، ذلك أن قيام ضابط الشرطة القضائية بالبحث والتحري في الطرق العامة أو في الغابات...الخ، لا يعد تفتيشا لانتفاء حرمة المكان، وعليه فهو إجراء من إجراءات الاستدلال والذي يدخل في اختصاصاتهم العادية.

---

[1]- راجع المادة 68-1 المادة 17-1 ، ق إ م إ.

[2]- هلالي عبد اللاه أحمد، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي دراسة مقارنة ، ط1 ، دار النهضة العربية، القاهرة، 1997 ، ص48-49 .

2-5 أن يتم التفتيش وفقا للإجراءات القانونية المقررة:

يتم القيام بإجراء التفتيش وفقا للشروط القانونية، بحيث يجب مباشرته طبقا لإجراءات صحيحة فإذا شاب التفتيش الواقع على نظم الحاسوب عيب فإنه باطل[1]، لأن التفتيش الذي يقوم به المحقق بغير الشروط المنصوص عليها في القانون يعتبر باطل بطلان مطلق، وبالتالي لا يجوز التمسك بما ورد في محضر التفتيش وكما لا يجوز للمحكمة الاعتماد عليه في إصدار حكمها.

3- مدى قابلية جرائم الحاسوب والشبكات الإلكترونية لتفتيش عن أدلتها:

قد يرد محل التفتيش في البيئة المعلوماتية على المكونات المادية أو المعنوية للحاسب الآلي والتي نتعرض إليها فيما يلي:

3-1 مدى خضوع مكونات الحاسوب المادية والمعنوية للتفتيش عن أدلة الجريمة:

تشمل مكونات الحاسوب المادية على الأشياء الملموسة وملحقاته [2]، والتي تتمثل في شكل وحدات كوحدة الذاكرة، لوحة المفاتيح والشاشة ووحدة التحكم، وكل واحدة لها مهمة محددة، فهي لا تواجه صعوبات تعيق إجراءات التفتيش باعتبارها من المكونات المادية[3]، والتي يمكن إيجادها في مسكن المتهم أو مسكن غير المتهم [4]، والتي قد تتواجد أيضا في مكان عام، فهي بذلك تخضع للقواعد التي تحكم ذلك المكان، كما قد تتواجد هذه المكونات في حيازة شخص خارج مسكنه، فهي بذلك تخضع لقواعد تفتيش الأشخاص بوصف المكونات المادية

---

[1]- طارق إبراهيم الدسوقى عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، د.ط، دار الجامعة الجديدة، الإسكندرية، د.س.ن، ص 371 .

[2]- علي حسن الطوالبه،" مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي"، دراسة مقارنة بحث منشور على شبكة الانترنت على موقع التالي: www.policeme.gouv bh/reports/2011/April/13-14-2011/634383168746341670.pdf

[3]- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، ط1 .، دار الثقافة للنشر والتوزيع، 2011 ، ص[3] 158 .

[4]- راجع المادة 82و 83 من ق إ م إ .

للحاسوب أحد ملحقاته، وسواء كان الشخص الحائز المالك أو الغير، أما بالنسبة لمكونات الحاسوب المعنوية والمتمثلة في المعلومات والبيانات المعالجة آليا، فهي محل خلاف باعتبارها غير مادية[1] .

3-2 -حالة وجود جهاز متصل بجهاز المتهم داخل الدولة:

تكمن المسألة في هذه الحالة في تجاوز الاختصاص المكاني للسلطة المختصة بالتفتيش، كما أنه يعتبر بمثابة العدوان على حقوق الأفراد وحرياتهم، ذلك عند قيام سلطة التحقيق بتفتيش جهاز له علاقة بجهاز المتهم داخل الدولة.

وقد أجازت بعض التشريعات للأشخاص القائمين على التفتيش امتداد هذا الأخير على سجلات البيانات المتصلة في النهاية الطرفية للحاسوب في منزل المتهم مع جهاز أو نهاية طرفية في مكان أخر، حيث أنه يمكن امتداد الحق في تفتيش المساكن إلى نظم المعلومات الموجودة في موقع أخر حينما يهدف ذلك إلى إظهار الحقيقة دون وجوب صدور إذن مسبق من قاضي التحقيق وذلك بشرطين هما:

- أن تكون النهاية الطرفية المتصلة بالحاسب الآلي موجودة داخل الدولة المعنية.

- أن تتضمن النهاية الطرفية المتصلة بالحاسب الآلي بيانات مخزنة تستهدف إظهار الحقيقة[2]

وبخصوص القانون الجزائري فقد تضمن في التعديل الجديد لقانون الإجراءات الجزائية نصوص قانونية إجرائية فيما يخص بتوسيع بعض الصلاحيات في مجال التفتيش، ذلك في بعض أنواع من الجرائم من بينها الجريمة المعلوماتية، حيث يجوز لقاضي التحقيق أن يأمر ضابط الشرطة القضائية للقيام بالتفتيش أو حجز ليلا أو نهارا في أي مكان على امتداد التراب الوطني في الجرائم الإلكترونية و منها جريمة النصب الإلكتروني [3].

3-3 حالة وجود جهاز متصل بجهاز المتهم خارج الدولة:

---

[1]- موسى مسعود ارحومة، مرجع سابق، ص .7.

[2]- فايز محمد راجع غلاب، مرجع سابق، ص312-313.

[3]-راجه المادة 47 من ق إ م إ.

تعد هذه المسألة من المشكلات التي تواجه إجراء التحقيق وبالخصوص مسألة التفتيش، ذلك لما توصلت إليه الدول من خلال برمجيات يمكنها القيام بإجراء التفتيش والذي لا يستند إلى مبرر قانوني من جهة، وباعتباره اعتداء على خصوصيات الأفراد وأجهزة حواسبهم من جهة أخرى[1].

غير أن مشكلة تفتيش مكونات الحاسب الآلي خارج الإقليم الوطني الجزائري قد حَلت، وذلك بموجب القانون رقم (09-04) لسنة 2009 من خلال تعاون السلطات الأجنبية وفقا لمبدأ المعاملة بالمثل في إطار اتفاقيات دولية في هذا الصدد[2].

وتتصل هذه المسألة مباشرة بالبعد الدولي فلا يمكن الحديث عن القضاء عليها إلا في ظل تعزيز وتبادل التعاون الدولي في إطار اتفاقيات دولية أو إقليمية أو ثنائية [3] مع تفعيل آليات المساعدة الدولية في مجال القضائي وتسليم المجرمين، وذلك باحترام مبدأ المساواة بما يفضي أنه لا مجال للدول المتقدمة في مجال المعلوماتية الرقمية أن تتحكم في أنظمة الغير والتجسس عليها بحجة ما يقتضيه إجراء التحقيق من تمديد التفتيش عن بعد بين الدول[4].

4- السلطة المختصة بتفتيش النظم المعلوماتية: الأصل أن تقوم بإجراء تفتيش نظم الحاسب الآلي سلطة التحقيق الأصلية المتمثلة في قاضي التحقيق والنيابة العامة، إلا أنه يجوز لضباط الشرطة القضائية أن يقوموا بهذا الإجراء بناء على تفويض صادر من السلطة المختصة، وهذا ما سنبينه تباعا.

أ-إجراء تفتيش النظم المعلوماتية بمعرفة سلطة التحقيق الأصلية:

---

[1]- عمر محمد أبو بكر بن يونس، مرجع سابق، ص315-316.

[2]- راجع فقرة 3 من المادة 5 القانون رقم (09-04) المؤرخ في 05-08-2009.

[3]- لقد حدث في ألمانيا جريمة غش بيانات الحاسب الآلي، أين اتضح عند جمع إجراءات التحقيق وجود اتصال بين الحاسب الآلي المتواجد في ألمانيا مع شبكة اتصالات في سويسرا التي تم تخزين المشروعات فيها، وقد تمكنت سلطات التحقيق الألمانية من ضبط ملفات البيانات عن طريق التماس المساعدة المتبادلة بين الدولتين، راجع علي محمود علي حموده، مرجع سابق، ص26 .

[4]- فايز محمد راجح غلاب، مرجع سابق، ص315- 316

إن المشرع الإجرائي المصري أناط الاختصاص بالتفتيش كإجراء تحقيق للنيابة العامة كسلطة أصلية ولقاضي التحقيق في حالات خاصة [1] ، وهذا عكس ما قضى به المشرع الجزائري حيث جعل سلطة تحقيق الأصلية من اختصاص قاضي التحقيق [2] باعتباره مختص بإجراء كل التحقيقات بما فيها التفتيش، لكن في كل الحالات التي يقوم فيها بهذا الإجراء لابد من إخطار وكيل الجمهورية الذي له الحق في مرافقته [3] ، واستثناءا يجوز لوكيل الجمهورية أن يقوم ببعض إجراءات التحقيق، لأن الاختصاص الأصيل بمباشرته يعود لقاضي التحقيق وحده دون سواه [4].

ولا يكفي توافر صفة قاضي التحقيق لكي يقوم بإجراء التفتيش، بل لابد أن يكون مختصا سواء من ناحية الاختصاص المكاني أو النوعي، فيتحدد اختصاص قاضي التحقيق محليا إمَا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في ارتكابهم الجريمة أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان القبض قد حصل لسبب آخر.

كما يجوز تمديد الاختصاص المحلي إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم وذلك في جرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية وغيرها.

بالإضافة إلى الاختصاص المكاني يجب أن يتوافر الاختصاص النوعي المتمثل في نوع الجريمة التي يختص بها المحقق بالتفتيش، وبالنسبة للقانون الجزائري نجد أن قاضي التحقيق يختص بإجراء التحقيقات بما فيها التفتيش في الجنايات والجنح المتلبس بها[5] .

---

[1]– هلالي عبد اللاه أحمد ، مرجع سابق ، ص133.

[2]– يجب الإشارة إلى أن قاضي تحقيق لا يختص بالقضية إلا بناء على طلب من وكيل الجمهورية أو شكوى مصحوبة بإدعاء مدني ، و ذلك بعد أخذ بعين الإعتبار نص المواد 67 و 73 ، و بعد دخول القضية في حوزته يكون مختصا وله أن يقوم بكل الإجراءات راجع نص المادة 38–1 من ق.إ.ج.ج.

[3]- راجع المواد 79 ، 82 من ق .إ .ج .ج.

[4]– راجع المواد 56–1 ، 59 –1 ، 117–1 من ق إ . ج ،ج .

[5]– راجع المادة 40 من ق إ . ج . ج.ج.

ويبدو أنه لما كانت سلطة التحقيق الأصلية غير مطالبة بالقيام بالتفتيش بنفسها في كل الحالات إذ قد لا يكون لها وقتا كافيا، خاصة إذا تعددت الأمكنة التي يتم تفتيشها أو الأشخاص المراد تفتيشهم، ففي هذه الحالة يجوز لقاضي التحقيق أن يندب أحد قضاة التحقيق أو أحد ضباط الشرطة القضائية [1]، وهذا ما سوف نراه.

ب – إجراء تفتيش النظم المعلوماتية بمعرفة ضباط الشرطة القضائية: يتمتع قاضي التحقيق وحده بالاختصاص الأصيل لإجراء التحقيق، ونظرا لكثرة هذه الإجراءات وتنوعها أجاز لها لقانون أن يندب غيره – ضباط الشرطة القضائية –للقيام ببعضها وفقا لشروط يجب توافرها وتطبيقها بحذافيرها [2].

وبالتالي فإن ضابط الشرطة القضائية المنتدب الذي يختص في الجريمة التقليدية هو نفسه الذي يختص في الجريمة المعلوماتية، ويتحقق إجراء التفتيش نظم المعلوماتية بمعرفة ضابط الشرطة القضائية، في الحالات التالية [3]هي:

-**التفتيش بناء على إذن قضائي بإجرائه:** باعتبار أن قاضي التحقيق غير ملزم في كل الحالات بمباشرة التفتيش، فإنه يجوز له أن يندب أحد ضباط الشرطة القضائية للقيام بهذا

---

[1]– هلالي عبد اللاه أحمد ، مرجع سابق ، ص 138.

[2]– و من شروط الواجب توافرها للقيام بالإنابة القضائية ما نصت عليه المواد 138 ، 139 ، 142 ، من ق إ ج ج التي تتضمن ما يلي : أن تصدر الإنابة من قاضي التحقيق المختص إقليميا ، و أن تصدر إلى قاضي ، أو ضابط الشرطة القضائية ، وأن تنصب الإنابة من قاضي التحقيق المختص إقليميا ، و أن تصدر إلى قاضي ، أو ضابط الشرطة القضائية ، و أن تنصب الإنابة على إجراء أو بعض إجراءات التحقيق الإبتدائي ، و عليه إذا كان التفويض عاما ، كانت الإنابة باطلة ، و يجب أن تكون الإنابة صريحة و مكتوبة ، و غيرها من شروط التي يجب مراعتها.

[3]– طارق إبراهيم الدسوقي عطية ، مرجع سابق ، ص 428.

الإجراء و هذا ما يسمى بالإنابة القضائية، لذلك فلا يجوز لضباط الشرطة القضائية القيام بإجراء التفتيش إلا بعد حصوله على إذن من السلطة المختصة [1].

وقد حدد المشرع الجزائري الاختصاص المكاني لضباط الشرطة القضائية ويكون ذلك إما بمكان وقوع الجريمة، أو بمكان إقامة المتهم، أو بمكان القبض عليه، وكما مدد اختصاصهم في حالة الاستعجال إلى كافة دائرة الاختصاص المجلس القضائي الملحقين به، ومدد أيضا بالنسبة لبعض الجرائم الخطيرة منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إلى كامل الإقليم الوطني [2].

-**التفتيش بناء على حالة التلبس بالجريمة:** لا يختلف التفتيش في حالة التلبس في نظم الحاسب الآلي عن الجريمة التقليدية، لذلك يجوز لضابط الشرطة القضائية المنتدب في أحوال التلبس بالجنايات والجنح المعلوماتية تفتيش نظم الحاسب الآلي[3] ، هذا ما تضمنته نص المادة 44 من قانون الإجراءات الجزائية الجزائري.

-**التفتيش بناء على موافقة المتهم:** يجب أن تكون الموافقة من طرف صاحب الشأن بالتفتيش صريحة ومكتوبة بخط يده، فإذا كان لا يعرف الكتابة يذكر ذلك في المحضر ويذكر فيه هذه الموافقة؛ أما بخصوص جرائم الحاسب الآلي فإنه لا توجد نصوص قانونية مشابهة تخص تفتيش نظم المعلوماتية بناء على موافقة المتهم سواء في مصر أو في القانون المقارن، لذلك فإن هذا الفراغ يمكن تغطيته بالقواعد التقليدية [4].

ثانيا – الشروط الشكلية لتفتيش الجرائم المعلوماتية و جريمة النصب المعلوماتية:

---

[1]– راجع المادة 44 من ق إ .ج.ج المادة 40 من الدستور الجزائري.

[2]– راجع المادة 16 من ق .إ.ج.ج.

[3]– طارف إبراهيم الدسوقي عطية ، مرجع سابق ، ص 437.

[4]– هلالي عبد اللاه أحمد ، مرجع سابق ، ص 162.

إلى جانب الضوابط الموضوعية لتفتيش نظم الحاسب الآلي، هناك ضوابط أخرى ذو طابع شكلي يجب مراعاتها والأخذ بها أثناء القيام بالتفتيش، والتي تتمثل فيما يلي:

1-الأشخاص المطلوب حضورهم أثناء التفتيش:

يشترط لقيام التفتيش كضمانة حضور صاحب المكان المراد تفتيشه، حيث اعتبر غالبية الفقه أن حضور المتهم للتفتيش من الأحكام الأساسية التي يجب الالتزام بها ويترتب على مخالفتها بطلان إجراء التفتيش[1].

2-أسلوب تنفيذ التفتيش:

قام القانون الأمريكي بتنظيم أسلوب تنفيذ التفتيش في نظم الحاسب الآلي، حيث يبدأ رجال الشرطة بالهجوم في الوقت نفسه وبشكل سريع على جميع منافذ المكان، باعتبار أن هذه الخطة تقلل من وقوع إصابات بين فرق رجال الشرطة، وبعد ذلك يقومون بسرعة فائقة باستبعاد الأشخاص المشتبهين فيهم على الحواسب الموجودة في المكان حتى لا يتم تغيير أو حذف أو تدمير الأدلة التي تثبت إدانتهم، حيث يوضع المتشبه فيهم في غرفة مع حراسة أمنية، وتفتيشهم في نفس الوقت مع إعلامهم أن كل أقوالهم ستأخذ بعين الاعتبار ويمكن أن يكون دليل إدانتهم، حيث يوجد مكان في المنزل يعتبر النقطة الساخنة والتي يكون فيها جهاز حاسب آلي متصل بخط هاتفي أو أكثر من ذلك.

وفي هذه الحالة يتم وضع النقطة الساخنة في فريق يتكون من خبيران فنيان أجاز لهم القاضي بالتفتيش، فالأول يسمى بالمكتشف مهمته نزع مقبس الكهرباء الخاص بسائر الأجهزة، ويقوم بالبحث عن الأقراص والمستندات وغير ذلك، والثاني يسمى بالمسجل مهمته تصوير كامل الأجهزة والأدوات المتصلة بها على الحالة التي تم ضبطها، كما يقوم أيضا بتصوير جميع الغرف الأخرى المتواجدة في المكان كضمانة لعدم إدعاء أحد المشتبه فيهم بسرقة منزله

[1]- فايز محمد راجح غلاب ، مرجع سابق ، ص 334.

وقت التفتيش، بالإضافة إلى أجهزة الفيديو والتسجيل الصوتي التي يتم من خلالها ترقيم الأشياء المضبوطة [1].

3- تحديد ميعاد التفتيش:

يعتبر ميعاد التفتيش أحد أهم الضمانات الشكلية، بحيث لا يجوز إجراؤه خارج الأوقات المحددة قانونا ما عدا في الأحوال الاستثنائية المقررة قانونا [2].

فلا يجوز البدء في التفتيش قبل الساعة الخامسة صباحا ولا بعد الساعة الثامنة مساءا، إلا إذا طلب صاحب المنزل ذلك، أو وجهت نداءات من الداخل، أو في الحالات الاستثنائية التي أقّرها القانون [3]، منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والتي يجوز إجراء التفتيش فيها في كل ساعة من ساعات الليل والنهار بناء على إذن مسبق من وكيل الجمهورية المختص، ذلك لأن المكونات المعنوية للحاسب الآلي وشبكة الاتصال قد تكون عرضة لإخفاء أو تغيير أو تدمير أو تلاعب بالبيانات المخزنة.

والتي تعتبر أدلة إلكترونية لإظهار الحقيقة، مما قد يؤدي بالجاني في ظرف ثواني إلى إفساد هذه الأدلة وعرقلة عمل التحقيق، لذلك استوجب هذا الأمر على التشريعات الحديثة إضافة الجريمة المعلوماتية كإستثناء عن أوقات التفتيش نظرا لطبيعة أدلتها الخاصة [4].

تلعب الضبط والخبرة دورا هاما في مجال الإثبات الجنائي للأدلة المعلوماتية خاصة في ظل تزايد تطور التكنولوجيا الرقمي، فبعد انتهاء المحقق الجنائي من إجراء التفتيش يقوم بضبط الأشياء التي يراها ضرورية، ومن ثم يأتي دور الخبير الذي يقوم بالتنقيب عن الحقيقة بناء على الأشياء المضبوطة، ثم يقدم الدليل المستنبط للقاضي الذي يمكن أن يبني حكمه بناء عليه،

---

[1]-عبد الله حسين علي محمود، مرجع سابق، ص 382.

[2]- فايز محمد راجح غلاب ، مرجع سابق ، ص 328.

[3]- راجع المادة 47 من ق .إ.ج.ج.

1- فايز محمد راجح غلاب ، مرجع سابق ، ص 329 -330.

وهذا ما سوف نعالجه من خلال مطلبين، في المطلب الأول الضبط في الجرائم المعلوماتية، أما في المطلب الثاني الخبرة القضائية في الجرائم المعلوماتية.

الفرع :الثالث الضبط في الجرائم المعلوماتية و جريمة النصب:

باعتبار أن النتيجة المترتبة عن إجراء التفتيش هو الضبط ، ففي هذه الحالة يجب إتباع إجراءات ضبط الأشياء والأدلة الرقمية، وهذا ما سيتم توضيحه بتعريف الضبط وطبيعته ومحله.

أولا: تعريف الضبط وطبيعته ومحله:

يقصد بالضبط في قانون الإجراءات وضع اليد على شيء مرتبط بجريمة تمت ويفيد في كشف الحقيقة عنها وعن مرتكبها، وهو من حيث طبيعته القانونية قد يكون من إجراءات الاستدلال أو التحقيق، فإذا كان الشيء في حيازة شخص واقتضى الأمر تجريده من حيازته وقت ضبطه كان الضبط بمثابة إجراء تحقيق، أما إذا كان نزع الشيء قد تم دون الاعتداء على حيازة قائمة، فيكون الضبط بمثابة إجراء استدلال[1].

ومن حيث محل الضبط فإنه لا يرد إلا على الأشياء المادية، لأن الأشياء المعنوية لا تصلح لأن تكون محلا لوضع اليد عليه [2]، والشرط اللازم لصحة الضبط أن يكون الشيء مفيد في كشف الحقيقة فكل ما يحقق هذا الهدف يصح ضبطه كما أن الضبط لا يرد إلا على الأشياء، أما الأشخاص فلا يصلحوا محلا للضبط، وإنما المصطلح الأصح هو القبض والقبض يختلف تماما عن ضبط الأشياء [3].

ثانيا: مدى صلاحية ضبط الأدلة في الجرائم المعلوماتية

ثمة صعوبة إلى اعتبار مكونات الحاسب الآلي من الأشياء التي يمكن ضبطها وبالخصوص ضبط الشبكة الإلكترونية والمكونات المعنوية للحاسب الآلي التي تشمل محتوى

---

[1]– خالد عياد الحلبي ، إجراءات التحري و التحقيق في جرائم الحاسوب و أنترنت ، ط ، 1 ، دار الثقافة للنشر و التوزيع ، عمان ، الأردن ، 2011 ، ص 168.

[2]– أحمد بلال ، مرجع سابق ، ص 264.

[3]– عبد الله حسين على محمود ، مرجع سابق ، ص 397.

أنظمة المعالجة الآلية للمعطيات، وفيما يلي نلقي الضوء على مدى قابلية كل من المكونات المادية والمعنوية والرسائل ومراقبة الاتصالات الإلكترونية لأن تكون محلا للضبط.

1 – ضبط المكونات المادية للحاسب الآلي:

إن ضبط المكونات المادية للحاسب الآلي وملحقاته الذي يشمل على جهاز الحاسوب ومكوناته الأساسية والثانوية لا تثير أية صعوبة، لأن الضبط يرد على أشياء مادية كالدعامة المادية للبرامج والأسطوانات والأشرطة [1] .ومن المكونات المادية التي تكون محلا للضبط ما يلي:

وحدة المعالجة المركزية، لوحة المفاتيح والشاشة والفأرة، والأقراص والأشرطة المغناطيسية التي يقوم البعض بتخزينها في البنوك أوفي مراكز التوثيق الحكومية الأمنية، ولوحة الدوائر الإلكترونية، وأجهزة الاتصال عبر شبكة الانترنت كأجهزة المودم [2].

حيث أنه تخضع للضبط وحدة الذاكرة الرئيسية سواء كانت لقراءة البيانات، أم كانت معدة للقراءة والكتابة معا، وضبط وحدة التحكم ووحدة المخرجات وما تشمله من وسائل، كالشاشة والطابعة، وضبط والصلب وحدات التخزين الفرعية التي تشمل على أقراص ممغنطة بنوعيها المرن FLoppy disk ، والصلب Hard disk والأشرطة المغناطيسية Magnetic tape ، وضبط وحدة المدخلاتinput unit بما تشمله من مفردات كلوحة المفاتيح Key board ، ونظم الإدخال المرئي Machine vision ، system ، نظام القراءة الضوئي، نظام الفأرة Mouse system، و نظام القراءة الضوئية للحروفOptical character Reader system[3] .

وفيما يتعلق بضبط مكونات الحاسوب المادية في القانون الجزائري فإنه لا يوجد أي مانع من تطبيقها، مثلها مثل غيرها من الماديات التي تفي النصوص التقليدية بمواجهتها موضوعيا وإجرائيا، ومن القواعد التي تتعلق بإجراء الضبط وتطبق على المكونات المادية للحاسوب هو

---

[1]– عفيفي كامل عفيفي، جرائم الكومبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون، دراسة المقارنة، ط2، منشورات الحلبي الحقوقية، بيروت– لبنان، 2007، ص 373.

[2]– عبد الله حسين على محمود، مرجع سابق، ص398–399.

[3]– هلال عبد اللاه أحمد ، مرجع سابق ، ص 198–199. [3]

أن الضبط يعتبر إجراء من إجراءات التحقيق، لذا فلا يجوز ضبط الأشياء إلا وفقا للقانون وذلك بأمر من النيابة العامة أثناء التحقيق ومن القاضي أثناء المحاكم [1]، فيتوجب عند إحصاء الأشياء المضبوطة التي تفيد في كشف الحقيقة وضعها في أحراز مختومة، ولا يجوز فتحها إلا بحضور المتهم مصحوبا بدفاعه [2] ، كما يتوجب كذلك عدم ضبط الأوراق والمستندات التي يسلمها المتهم لمحاميه أو للخبير الاستشاري لأداء مهامه.

وباعتبار أنه لا خلاف حول ضبط مكونات الحاسب الآلي المادية ومواجهتها إجرائيا بالنصوص التقليدية، فإنه توجد بعض التشريعات تضمنت صراحة النص على تفتيش المكونات المادية [3] ، ومن هذه التشريعات قانون المنافسة الكندي والقانون الإنجليزي الصادر في عام 1990والذي يطلق عليه قانون إساءة استخدام الحاسب [4].

الحصول على المعلومات والبيانات وضبطها للوصول إلى الأدلة [5]، غير أن المسألة الصعبة تكمن في الخلاف حول مدى خضوع المكونات غير المادية للحاسوب للضبط وفقا للنصوص التقليدية وكذا في إجراءات ضبطها سواء تعلق الأمر ببرامج الحاسوب أو بياناته [6].

1-1 برامج الحاسب الآلي:

إن الأمر يتعلق بكيفية ضبط الأدلة في حالة استخدام الوسائل الفنية في نسخ أو إتلاف البرنامج كالفيروسات مثل حصان طروادة، مع قلة خبرة وتدريب الضبطية القضائية وسلطة التحقيق في جمع الأدلة في مجال الفني والتقني وهذا من الناحية الأولى، ومن الناحية الثانية تتمثل في قيام عملية ضبط الوسائل التقنية بواسطة الأنظمة والشبكات المعلوماتية الكبيرة، حيث يؤدي الضبط إلى عزل النظام المعلوماتي بالكامل عن دائرته لفترة زمنية يمكن أن تطول أو

---

[1] – فايز محمد راجح غلاب ، مرجع سابق ، ص 342-343.

[2] – راجع المادة 84 من ق .إ.ج.ج.

[3] – فايز محمد راجح غلاب ، مرجع سابق ، ص 248.

[4] – هلالي عبد اللاه أحمد ، مرجع سابق ، ص 199.

[5] – عفيفي كامل عفيفي، مرجع سابق، ص، 378.

[6] – فايزمحمد راجح غلاب ، مرجع سابق ، ص 344.

تقصر والذي يسبب خسائر وأضرار بالجهة مستخدمة النظام، وكذلك ينتج عن ذلك عدم مبادرة مستخدمي النظام المعلوماتي استعدادهم للتعاون ومساعدة سلطة التحقيق لما يمثله الضبط لهم من الاعتداء على حقوق الآخرين [1].

2-1 بيانات الحاسب الآلي:

التي تعد دليلا على ارتكاب الجريمة، هناك صعوبات كثيرة منها (Data) بالنسبة لضبط البيانات عدم وجود دليل مرئي يمكن للضبطية القضائية فهمه عن طريق القراءة، كما تتميز الجرائم التي يكون محلها بيانات الحاسب بعدم وجود أثار مادية يمكن من خلالها الاستدلال على أدلة في ارتكاب الجريمة ويظهر ذلك بشكل واضح في جرائم الاختلاس والتزوير باستخدام الحاسب الآلي، كذلك فالبيانات التي يمكن التوصل إليها يستطيع الجاني تدميرها أو محوها في مدة قصيرة، وهو ما يلزم للمحقق من فصح البيانات مع ضخامتها، ناهيك عن نقص الخبرة الفنية لعملية الفحص وما تتطلبه من تحديد البيانات التي تصلح كأدلة إدانة من عدمه، والأمر يزداد تعقيدا في حالة الأنظمة المعلوماتية المتصلة بنهاية طرفية أخرى تتعدى حدود الدولة إلى إقليم دولة أخرى [2].

-وقد نظم المشرع الجزائري القواعد الخاصة بضبط البيانات المعلوماتية وفقا للقانون رقم (09-04) تحت تسمية حجز المعطيات المعلوماتية"، حيث قضت المادة (**06**) من نفس القانون على نسخ المعطيات محل البحث، وكذلك المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية التي تكتشفها السلطات المختصة عند القيام بالتفتيش في المنظومة المعلوماتية، وتكون هذه المعطيات تفيد إظهار الحقيقة وقابلة للحجز، وتوضع في الأحراز مع وجوب قيام السلطة المختصة بحماية سلامة المعطيات المخزنة في المنظومة المعلوماتية، كما يجوز استخدام الوسائل التقنية وفقا لما يستهدفه التحقيق لتشكيل أو إعادة تشكيل هذه المعطيات بشرط عدم المساس بمحتوى المعطيات.

---

[1]- عفيفي كامل عفيفي، مرجع سابق، ص 374.

[2]- مرجه نفسه ، ص 375.

أما المادة (**07**)من نفس القانون نصت على أنه في حالة استحالة إجراء الحجز وفقا لما نصت عليه المادة (**06**) وذلك لأسباب فنية، فعلى السلطة المختصة بالتفتيش القيام بالتقنيات الواجبة للمنع من الوصول إلى محتوى المعطيات أو نسخها مع الاحتفاظ بها من طرف الأشخاص المصرح لهم بذلك كذلك نص المادة (**08**)تعلقت بالمعطيات التي يشكل محتواها جريمة، فعلى السلطة المباشرة بالتفتيش أن تصدر أمر بتكليف أي شخص مؤهل فنيا وتقنيا لاستخدام الوسائل التقنية المناسبة من أجل منع الإطلاع على محتوى هذه المعطيات؛ أمّا المادة (**09**)من نفس القانون، فيتضح من خلالها أن المعلومات المتحصل عليها عن طريق المراقبة وفقا لهذا القانون، لا يجوز استخدامها إلا في الحدود الضرورية التي يقتضيها التحري أو التحقيق القضائي، وذلك تحت طائلة العقوبات التي نص عليها التشريع المعمول به[1].

ومن خلال مضمون هذه النصوص، نجد أن المشرع الجزائري تنبه للقصور الموجود في مصطلح ضبط الكيانات المنطقية للحاسوب، حيث استخدم مصطلح حجز وليس ضبط باعتبار أن مصطلح حجز يتلاءم مع الأشياء غير المادية [2].

2- ضبط الرسائل ومراقبة الاتصالات الإلكترونية:

سهلت ثورة المعلومات الاتصال بين الأفراد التي انعكس أثرها على مختلف ميادين الحياة، ومن ناحية أخرى فقد سببت الكثير من أضرار شخصية عن طريق جرائم عدّة مستحدثة خصوصا انتهاك أسرار الأشخاص بواسطة الوسائل الإلكترونية، ونظرا لصلة المراسلات بالحياة الخاصة للأفراد[3].

عمدت الدول على حماية هذه الأسرار الشخصية عن طريق إرساء نصوص دستورية تضمن عدم الاعتداء على خصوصية المراسلات [4]، ومن بينها الدستور الجزائري الذي تضمن

---

[1]- راجع المواد من 6-9 من قانون (09-04) المؤرخ في 05-08-2009 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام و الاتصال و مكافحتها.

[2]- فايز محمود راجع غلاب ، مرجع سابق ، ص 350.

[3]- علي محمود علي حموده ، مرجع سابق ، ص 32.

[4]- علي محمود على حموده ، مرجع سابق ، ص 32.

منع الإطلاع على المراسلات سواء كانت بريدية أو برقية أو هاتفية وذلك في نص المادة **39**) (من الدستور الجزائري التي تنص على أنه ":سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة "[1].

غير أن القوانين الإجرائية تجيز ضبط الرسائل ومراقبة المحادثات الهاتفية وفقا لقواعد وشروط معينة، من أجل المحافظة على حقوق المجتمع ونظام الأمن والآداب العامة، وبناء على ذلك فهل تمتد المراسلات العادية إلى سائر المراسلات الإلكترونية المستخدمة؟ [2] وهذا ما سنبينه من خلال ضبط المراسلات الإلكترونية بالنسبة للبريد الإلكتروني، والتنصت والمراقبة الإلكترونية لشبكات الحاسب الآلي فيما يلي:

3-1 البريد الإلكتروني:

يقصد بالبريد الإلكتروني استخدام شبكات الانترنت من أجل نقل الرسائل بدلا من الطرق التقليدية، وباعتبار أن استعماله سهل أضحى من أكثر وسائل الانترنت استعمالا في الوقت الحالي.

وأهم مسائل تتعلق بالبريد الإلكتروني هو وجوب المحافظة على سريته، وهو ما أدى إلى اصطناع برامج تشفير خاصة به، حيث لا يمكن الإطلاع على رسائل الأشخاص إلا لمن يعرف الشيفرة.

ولقد ساعد ذلك على ظهور التوقيع الإلكتروني في تيسير عملية التراسل عبر البريد الإلكتروني [3]، فالتوقيع الإلكتروني يقوم بعملية محددة ويمنح مصداقية للوثيقة أو المحرر

---

[1]- المادة 39 من قانون رقم 08-19 المؤرخ في 15 نوفمبر 2008 ، المتضمن الدستور الجزائري المعدل و المتمم.

[2]- فايز محمد راجح غلاب ، مرجع سابق ، ص 351.

[3]- علي محمود على حموده ، مرجع سابق ، ص 32.

الإلكتروني بحيث يمكن من خلال هذا إكساب الوثيقة مصداقية لدى الغير أو الطرف الآخر مستقبل هذا المحرر أو الوثيقة [1].

وبهذا الخصوص ثار خلاف حول طبيعة الرسائل الإلكترونية واختلافها على الرسائل الورقي ة حيث يعتبرها البعض عبارة عن موجات كهرومغناطيسية وذبذبات إلكترونية تختلف تماما على المستندات المادية الورقية، والبعض الآخر يعتبرها مستند تقليدي، فالمستند أصبح مفهومه الذي يتفق مع ثورة الاتصالات عن بعد بأنه كل أسلوب به تحدد فكرة معينة أو تعبير محدد من خلال كتابة ورقية أو كتابة إلكترونية.

وقد أسفر الخلاف الحاصل حول طبيعة الرسائل الإلكترونية ومفهوم المستند، إلى تضارب بعض الأحكام التي تجرّم فعل الإطلاع عليها من طرف الغير من عدمه وفقا لما تضمنته النصوص التقليدية[2]

وبالرجوع إلى النصوص القانونية يلاحظ بأن القانون الجزائري استحدث مصطلحات تقنية جديدة في نصوص قانونية جديدة تتلاءم مع ضبط الرسائل الإلكترونية في العديد من الجرائم في حالة التلبس أو التحقيق الابتدائي، ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وهذه النصوص خصت عن النصوص التقليدية بجوانب تقنية تجيز بمقتضاها لقاضي التحقيق أو ضابط الشرطة القضائية المناب له باعتراض المراسلات وتسجيل الأصوات والتقاط الصور [3].

---

[1]– مخلوفي عبد الوهاب ، التجارة الإلكترونية عبر الأنترنت ، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق ، كلية الحقوق و العلوم السياسية ، قسم الحقوق ، جامعة الحاج لخضر ، باتنة ، 2011 ، ص 196.

[2]–فايز محمد راجح غلاب ، مرجع سابق ، ص 352.

[3]– المواد من 65 مرر – 65 مكرر 10 من الباب الثاني من الكتاب الأول في الفصل الرابع تحت عنوان "اعتراض المراسرالات و تسجيل الأصوات و اتلقاط الصور "من القانون رقم (06–22) المؤرخ في 20 ديسمبر 2006 ، يتضمن قانون الإجراءات الجزائية المعدل و المتمم.

وهذا ما يتضح من خلال نص المادة **65 مكرر** من قانون الإجراءات الجزائية ، حيث قضت هذه المادة على أنه في حالة الضرورة لإجراء أساليب تحريات خاصة في بعض من الجرائم منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، يجوز لوكيل الجمهورية المختص أن يأذن باعتراض المراسلات التي تتم عن طريق وسائل الاتصالات السلكية واللاسلكية، أو وضع ترتيبات تقنية دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام من طرف شخص أو عدة أشخاص في أماكن خاصة أو عامة أو التقاط صور شخص أو عدة أشخاص يتواجدون في مكان خاص، وتتم هذه العمليات المأذون بها تحت المراقبة المباشرة لوكيل الجمهورية المختص، أما في حالة فتح تحقيق قضائي تتم العمليات بناء على إذن من قاضي التحقيق وتحت رقابته المباشرة[1] .

وكما نصت المادة (**03**) من قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها على ما يلي" :مع مراعاة القوانين التي تراعي سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في الإجراءات الجزائية في هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية "[2].

3-2 التنصت والمراقبة الإلكترونية لشبكات الحاسب الآلي:

يقصد بمراقبة المحادثات الهاتفية وتسجيلها بأنها إجراء من إجراءات التحقيق، تباشرها السلطة المختصة للبحث عن أدلة إثبات الجريمة ضد شخص نسبت إليه ارتكابها أو لديه أدلة تتعلق بها، وكانت هذه الجريمة على درجة من الخطورة لاتخاذ مثل هذا الإجراء الاستثنائي [3].

---

[1]– المادة 65 مكرر نت ق. إ .ج.ج.

[2]–المادة 03 من قانون رقم (09-04) لسنة 2009.

[3]–على محمود على حمودة ، مرجع سابق ، ص 34.

فقد أجازت بعض التشريعات التنصت والمراقبة الإلكترونية، منها التشريع الفرنسي والذي أجاز على اعتراض الاتصالات عن بعد بما في ذلك شبكات تبادل المعلومات، وكما أجاز التشريع الهولندي لقاضي التحقيق أن يأمر بالتنصت على شبكات الاتصالات الحاسب الآلي إذا كان الهدف منها ضبط الجرائم الخطيرة، وكذا إمكانية مراقبة التلكس والفكس ونقل البيانات[1].

أما بالنسبة للقانون الجزائري فقد استحدث في **ديسمبر** سنة **2006** نصوص قانونية تتعلق باعتراض المراسلات وتسجيل الأصوات والتقاط الصور، والتي تضمنت عدة أحكام منصوص عليها من المواد **(65 مكرر 5 إلى 65 مكرر10)** والتي نذكرها كالتالي:

-قيام العمليات المذكورة في نص المادة **(65 مكرر5)** بشرط عدم المساس بالسر المهني بالنسبة لأماكن التي يشغلها أشخاص ملزمون بالمحافظة على أسرار الآخرين.

-وفي حالة اكتشاف جرائم أخرى بصورة عارضة، فلا يكون هذا سببا في بطلان الإجراءات.

- يجب أن يتعلق الإذن بجميع العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة سكنية أو غيرها والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها.

-يجب أن يكون الإذن مكتوبا وسليم لمدة أقصاها (04) أربعة أشهر قابلة للتجديد بحسب مقتضيات التحري والتحقيق.

-يجوز لوكيل الجمهورية أو لقاضي التحقيق أو لضابط الشرطة القضائية المأذون له، تسخير كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للقيام بالجوانب التقنية للعمليات المشار إليها في المادة(65 مكرر 5).

-تحرير محضر من طرف السلطات المختصة بالبحث والتحري عن كل عملية اعتراض أو تسجيل للمراسلات، وكذلك عمليات وضع الترتيبات التقنية وعملية التقاط والتثبيت والتسجيل الصوتي والسمعي البصري، كما يذكر في المحضر تاريخ وساعة بداية ونهاية العمليات.

---

[1]-مرجع نفسه ، ص 35-34.

-يوصف أو ينسخ ويودع المراسلات أو الصور أو المحادثات المسجلة في إظهار الحقيقة من طرف ضباط الشرطة القضائية المناب له ذلك، وكذلك نسخ وترجمة المكالمات الأجنبية بمساعدة مترجم يسخر لهذا الغرض [1].

غير أن هذه الأحكام لم تتضمن صراحة الرقابة على الاتصالات الإلكترونية، ومن أجل ذلك فقد شمل المشرع الجزائري فصل ثاني خاص بمراقبة الاتصالات الإلكترونية في القانون رقم (09-04) لسنة **2009** المتعلق بالوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وذلك من خلال وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية، وقد تعلقت بنوعين من الرقابة، رقابة وقائية هدفها الوقاية من الجرائم الخطيرة المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها؛ أما الثانية فهي رقابة ضبطية قضائية تتضمن حالتين:

-**الحالة الأولى:** عندما يقتضي الأمر التحري والتحقيق في ذلك لاستصعاب القيام بذلك بالطرق العادية دون اللجوء إلى المراقبة.

-**الحالة الثانية:** وذلك في ظل متطلبات التبادل والمساعدة القضائية بين الدول [2].

الفرع الرابع: الخبرة القضائية في الجرائم المعلوماتية و جرائم النصب

تقدم الخبرة عونا كبيرا للقضاء ولجميع جهات المختصة بالدعوى الجنائية من خلال أداء مهمتها التي بدونها يستحيل الوصول إلى رأي بشأن المسائل الفنية، والتي من خلالها يمكن التوصل إلى ظهور الحقيقة المبنية على حقائق علمية فنية والذي يعتبر العنصر المميز لها عن غيرها من إجراءات الإثبات [3] وفي هذا المجال نتطرق إلى دراسة القواعد القانونية التي تحكم الخبرة القضائية في الجريمة المعلوماتية كفرع أول و القواعد الفنية التي تحكمها كفرع ثاني، وكذا مدى كفاية النصوص التقليدية في معالجة المسائل المتعلقة بالخبرة كفرع ثالث.

---

[1]- المواد من 65 مكرر 5 – 65 مكرر 10 من ق.إ.ج .ج.

[2] -المادة 04 من القانون رقم (09-04) المؤرخ في 05-08-2009.

[3]- أحمد بلال ، مرجع سابق ، ص ، 256.

أولا :القواعد القانونية التي تحكم الخبرة القضائية في الجرائم المعلوماتية

تظهر أهمية الخبرة في مجال الجريمة المعلوماتية لتعلقها الوثيق بالحاسبات وشبكات الاتصال المرتبطة بالتخصصات العلمية والفنية الدقيقة، ومع التطور السريع لها يصعب على المختصين مواكبتها واستيعابها، بالإضافة إلى أنه لا يوجد خبير يستطيع التعامل مع جميع الجرائم المعلوماتية نظرا لتعدد أنماط هذا النوع من الجرائم [1]، وسوف نتعرض في هذا الفرع إلى التعريف بالخبير والخبرة، وأنواعها، ومجالاتها في الجرائم المعلوماتية.

2- تعريف الخبرة والخبير:

تعد الخبرة إجراء من إجراءات جمع الأدلة بعد إحاطة الموضوع بمعلومات فنية تسمح باستنتاج والوصول إلى الدليل، فالخبرة تعتبر وسيلة من وسائل الإثبات التي تهدف إلى كشف بعض الأدلة أو تحديد مدلولها من خلال الاستعانة بالمعلومات العلمية، حيث يستند القاضي إلى الخبرة لاتخاذ القرار المناسب.

أما الخبير فهو كل شخص تكمن له دراية بمسألة من المسائل وله كفاءة فنية وعلمية خاصة [2]

2- تعيين الخبير المعلوماتي:

إن أهم صعوبة تواجه الخبرة هي تكوين الخبير المناسب للاستعانة به، باعتبار أن الخبرة في مجال المعلوماتية لا تعتمد على الشروط التقليدية الخاصة بتعيين الخبير، بل يتطلب الأمر شروط تتلاءم مع التطورات الطارئة في مجال تكنولوجيا المعلومات والجرائم الواقعة عليها خاصة في المسائل الفنية والعلمية [3]،فيحتاج الشخص لكي يكون خبيرا قضائيا في مجال

---

[1]- عبد الله حسين على محمود ، مرجع سابق ، ص 392.

[2]- عبد الناصر محمد محمود فرغلي ، محمد عبيد سيف سعيد المسماري ، مرجع سابق ، ص 24.

[3]- عمر محمد أبو بكر بن يونس ، مرجع سابق ، ص 103.

الجريمة المعلوماتية بشكل خاص أن يتمتع بشروط خاصة، حيث يجب أن يكون مؤهلا ومهنيا ومتحصلا على شهادة ودراسات عليا في فرع التخصص، وأن يخضع للتدريب العملي والقانوني مع استمراريته للتدريب والدراسة خلال مسيرته الوظيفة من أجل مواكبة كل جديد يطرأ على تخصصه لأداء مهمته [1]، فيتطلب من الخبير أن يكون ملما بالجوانب الفنية والتقنية، ومنها ما يلي:

– المعرفة بتركيب الحاسب وصناعته وطرازه ونوع نظام تشغيله الرئيسية والفرعية والأجهزة الطرفية الملحقة به وكلمات المرور وأكواد التشفير...الخ.

– طبيعة البيئة التي يعمل في ظلها الحاسب من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية وتحديد أماكن التخزين والوسائل المستخدمة لذلك.

–المواضيع الرقمية المحتمل تواجد فيها أدلة الإثبات والصور أو الأشكال التي تتخذها.

–الكيفية التي يمكن بواسطتها عزل النظام المعلوماتي دون إتلاف أو تغيير أو إفساد الأجهزة.

–الكيفية التي يتم بواسطتها نقل الأدلة إلى الأوعية دون أن يترتب على ذلك إتلافها.

–التمكن من تحويل أدلة الإثبات غير المرئية إلى أدلة مقروءة والمحافظة على الأدلة المستخرجة بصورة نسخ أو مطبوعات بشكل يمكن للقاضي أن يفهمها ويستوعبها[2].

وعليه فإن اختيار الخبير في مجال الجريمة المعلوماتية يتحدد بنوعية الجريمة المرتكبة، نظرا لأن الحاسبات وشبكة الاتصال ذات نماذج متعددة، وبالتالي لا يوجد خبير لديه معرفة متعمقة

1–عبد الناصر محمد فرغلي ، عبيد سيف سعيد المسماري ، مرجع سابق ، ص 26.

2– عبد الله حسين على محمود، مرجع سابق ، ص 394 ، 395.

مع كافة أنواع الحاسبات وبرمجياتها وشبكاتها، كما أنه ليس هناك خبير قادر على التعامل مع أنواع الجرائم التي تكون هذه الوسائل الإلكترونية محلا لارتكابها أو أداة لها [1].

فقد يكون الخبير سببا لفقدان الأدلة لعدم التخصص الدقيق في المسألة التي تطلب ضرورة الخبرة وقد تحتاج إلى أكثر من خبير(4)'، فيجب أن يكون الخبراء في مجال الأدلة الرقمية على وعي تام لأن اي خطأ في التفسير يؤدي إلى إتلاف أو محو الدليل الرقمي كحالة الخطأ في طريقة الحصول على الدليل الرقمي أو عدم تحريز الأدلة [2]، كما قد يتم إتلاف الأدلة بسبب خطأ الخبراء والجهة المجني عليها[3].

3- أنواع الخبرة في المجال المعلوماتي:

3-1 الخبرة الخاصة: تعتبر الخبرة الفردية من أهم مظاهر الخبرة السائدة في مجال تكنولوجيا المعلومات والانترنت فالمؤسسات الكبرى المتخصصة في هذا مجال تعمل جاهدة على الاستعانة بأشخاص ثبتت كفاءتهم في مجال الحاسب الآلي والانترنت، فهناك من الدول تقوم بمحاولة التعرف على قراصنة الذين تحولوا مع مرور الزمن إلى رموز وطنية من جراء تحركاتهم عبر الشبكة الإلكترونية [4].

---

[1]– فايزمحمد راجح غلاب ، مرجع سابق ، ص 363.

[2]- Compagnie national des experts de justice en information et techniques Associées, lapreuve numérique à l'épreuve du litige, les acteurs du litige face à la preuve numérique(l'information numérique fait la preuve), Colloque du 13 avril 2010 à la première chambre de: la cour d'appel de paris ; p.28. أنظر الرابط الإلكتروني

http://www.cnejita.org/dac/collague 20100513 Actes.PDF

[3]– ومثال من اشتراك الخطأ بين الخبراء والمجني عليه، ما وقع في إحدى جرائم المعلوماتية حيث قام أحد الأشخاص في إحدى الشركات بوضع قنبلة منطقية بنظام الحاسب الآلي، وقد تم التأكد أن الشركة قبل إبلاغ السلطات المختصة قامت باستدعاء خبير للتحقق من صحة وجود القنبلة وإبطالها، وقد اكتشف الخبير القنبلة وقام بإزالة البرنامج الموضوع لها، وعندما تولت الشرطة التحقيق وجدت أن إزالة القنبلة أدى إلى إتلاف أدلة وجودها، راجع فايز محمد راجح .غلاب، مرجع سابق، ص . 363.

[4]–عمر محمد أبو بكر بن يونس ، مرجع سابق ، ص 103.

3-2 الجهات التعليمية: يمكن مواجهة الجريمة المعلوماتية عن طريق المؤسسات التعليمية والتي تهدف بدورها إلى تطوير العلم والقضاء على المشكلات التي تواجه الإنسانية، حيث يتم تدعيمها ماديا ومعنويا حتى تكون أفضل سبيل للمواجهة، وأنشأت العديد من المؤسسات التعليمية منها دراسات الكمبيوتر في جامعة ستافرورد ومعهد التكنولوجيا في ماساشوستس والذي وَفر خبراء على درجة عالية من التفوق [1].

3-3 جهات الضبط القضائي: قامت بعض الدول وأهمها الولايات المتحدة الأمريكية بإعداد أجهزة متخصصة للخبرة في إجراء الخبرة على الانترنت، العابر نشاطها الإطار الدولي في هذا المجال المتمثل في منظمة الأنتربول.

حيث أن آخر نشاط مؤسسي في هذا الإطار هو الفرع الجديد الذي تأسس في المباحث الفيدراليةFBI أطلق عليه المعمل الإقليمي الشرعي للحاسوب، وأصبح مقر خبرة عامة متعددة النواحي الأمريكية القضائية هدفه مكافحة التصعيد الخطير في الجرائم المعلوماتية من خلال التصنيف والتحليل للدليل الرقمي، وأهم دور يقوم به هذا المعمل هو التقاء العديد من منظمات الضبط القضائي من أجل التعاون فيما بينها [2].

4 الوسائل الإجرائية: من بين الوسائل الإجرائية نجد ما يلي:

أ-**اختفاء الأثر**، إن المسجلات التي يتم نشرها في المواقع الخاصة بالمخترقين تشير دائما بنصائح مختلفة من بينها قم بمسح آثاركCover your trachs وفي حالة عدم مسح المخترق لأثاره يقبض عليه، حيث يتقصى على الأثر بطرق عديدة سواء بواسطة البريد الإلكتروني الذي تم استقباله أو بتتبع أثر الجهاز الذي تم استخدامه للقيام بالاختراق، وحتى لو تمت عملية الاختراق بشكل صحيح وسليم إلا أنه يمكن القبض عليه كونه لم يقم بمسح أثاره.

---

[1]-خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ، مرجع سابق ، ص 299.

[2]-عمر محمد أبو بكر بن يونس، مرجع سابق ن ص 1037-1038.

ب- الإطلاع على عمليات التنظيم المعلوماتي وأسلوب حمايته، من المفروض على المحقق في حالة إجرائه للتحقيق في جريمة معلوماتية ما، أن يقوم بالإطلاع على النظام المعلوماتي ومكوناته من شبكات وبرامح، وعملياته كقاعدة المعطيات وإدارتها ومعرفة النظام والمستفيدين والإجراءات منها إجراء أمن العاملين، وكذلك عليه الإطلاع على أسلوب النسخ الاحتياطي والاستعانة ببرامج الحماية كمراقبة المستفيدين والبرامج وتسجيل الوقائع.

ج-الاستعانة بالذكاء الصناعي، من الممكن الاستعانة بالذكاء الصناعي في جمع الحقائق والأسباب والفرضيات، التي يستخلص منها النتائج عن طريق معاملات حسابية يتم تحليلها بالحاسب الآلي وفقا لبرامج صممت لأجل ذلك، حيث أن تقنيات الحاسب الآلي أثبتت نجاحها وتمكنها من جمع أدلة جنائية وتحليلها واستنتاج الحقائق منها [1].

ثالثا: مدى كفاية النصوص التقليدية في معالجة المسائل المتعلقة بالخبرة المعلوماتية

باعتبار أن القاضي قد يستخدم خبير استشاري بشكل غير رسمي في المجال الرقمي، ذلك ماقد يشكل صعوبة ويعيق إجراءات التحقيق وأكثر من ذلك قد تكون وجها من أوجه البطلان، كون أبعض القوانين تخول للمتهم دون سلطة التحقيق أو الاتهام الاستعانة بخبير استشاري، لأنه قد لا يجد القاضي خبيرا في مجال تكنولوجيا المعلومات ضمن قائمة جدول الخبراء، هذا ما يستدعي من المشرع التدخل من خلال تضمين نصوص قانونية التي تسمح بالاستعانة بالخبرة الاستشارية من طرف جهة التحقيق والاتهام في المجال المعلوماتي دون التقيد بخبراء الجدول المعتمدين [2].

[1]-خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص 308.

[2]-عمر أبو بكر بن يونس ، مرجع سابق ، ص 392.

ولقد نظم قانون الإجراءات الجزائية الجزائري نصوص خاصة بالأحكام المتعلقة بالخبرة بالنسبة، للجريمة التقليدية من المادة (**143**) إلى المادة (**156**)[1].

ورغم عدم تضمين نصوص خاصة تتعلق بالخبرة الرقمية، وكذلك نقص الخبرة في مجال تكنولوجيا المعلومات، إلا أنه هناك إمكانية تطبيق الأحكام المتعلقة بالخبرة في الجرائم الناشئة عن الحاسب الآلي، فبات الأمر على القاضي أن يكون ملما بالأمور الفنية، باعتباره يشرف ويراقب أعمال الخبرة، كما أنه يحدد المواضيع التي تتطلب الاستعانة بالخبرة، غير أن هذا الأمر غير متوفر في الدول النامية، وبالتالي تدريب كوادر الأجهزة الضبطية والقضاة في مجال الخبرة الرقمية تكاد تكون ضرورة لا غنى عنها[2].

وهذه الحتمية أدت بالدولة الجزائرية بالعمل على استفادة الشرطة والدرك الوطني وغيرها من الأجهزة القائمة على تحقيق العدالة، إلى تلقي التدريب والتعليم في فرنسا، بلجيكا وكندا، وقد تم تكوين مركز وقاية ومكافحة الإجرام المعلوماتي ببوشاوي من طرف قيادة الدرك، ويتم إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي بموجب المرسوم الرئاسي رقم (04-432) المؤرخ في 20 ديسمبر 2004 [3]، ويشمل هذا المعهد على المصالح والأقسام والمخابر بموجب قرار مشترك مؤرخ في 14 أبريل 2007 ، ومن بين مصالحه مصلحة الخبرات الخاصة بالدلائل التكنولوجيا، بحيث تضمنت المديرية العامة للأمني الوطن ومصالحها في بعض الولايات قسم خاص بالخبرة الرقمية، ويتكون من خبراء مختصين في تحليل و استعادة البيانات المحدوفة و تتبع عنوان IP ، و معالجة الصور و مطابقاتها ومعرفة الصور التي تم تركيبها، وكذلك الخبرة المتعلقة برسائل الهاتف النقال [4]، وكما وضع المشرع نصوص خاصة

---

[1]-راجع المواد من 143-156 من ق.إ.ج،ج.

[2]-فايز محمد راجح غلاب ، مرجع سابق ، ص 369.

[3]-مرجه نفسه ، ص 370.

[4]- القرار الوزاري المؤرخ في 14 ابريل 2007 يتعلق بتنظيم الأقسام و المصالح و المخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي ، ج ،ر ، ع 36 ، الصادرة في 03 يونيو 2007.

لها علاقة بالخبرة الرقمية، ومن ذلك إمكانية السلطات المكلفة بالتفتيش الاستعانة بكل شخص له دراية بعمل المنظومة المعلوماتية من أجل مساعدتها في إنجاز مهمتها محل البحث[1]، وكما قام بإنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والتي تكون مهمتها إنجاز الخبرات القضائية التي تطلبها السلطات والشرطة القضائية[2].

وعليه في الأخير يمكن القول أن الجرائم المعلوماتية هي جرائم ذو طبيعة غير مادية، هذا ما أدى بإجراءات التحقيق الجنائي فيها لا تزال محل خلاف فقهي وقضائي، وبالأخص إجراءات التفتيش والضبط عن بعد، والمعاينة وكذا غياب وجود الخبير المعلوماتي المتخصص في المجال الرقمي وغيرها من إجراءات التي تثير العديد من المشكلات التي تعيق التحقيق، باعتبار أن الدليل المراد استنباطه يكون خفيا غير مرئي وأكثر من ذلك فقدان الدليل لأثاره سواء بالتلاعب أو التغيير أو الحذف، لكون الجريمة المعلوماتية مجهولة لا تصل إلى علم سلطات التحقيق والاستدلال، وهذا راجع إلى عدم اكتساب المهارة والمعرفة وعدم الخضوع للتدريبات التي تسمح للقضاة وضباط الشرطة القضائية بمواجهة تقنيات الحاسب الإلكتروني المتطورة، وكذا عدم استعانتهم بخبراء مختصين في مجال التحقيق، وهذا ما ينعكس سلبا على نفسية المحقق والمجتمع وإيجابا على نفسية الجاني، كونه على ثقة بأن السلطات التحقيق المختصة غير قادرة على إيجاد الدليل ضده وهذا ما يشجعه أكثر على ارتكاب جرائم كثيرة وخطيرة، لذا فإن متابعة إجراءات التحقيق في مجال الجريمة المعلوماتية، تحتاج إلى الأمن المعلوماتي ولرجال الضبط القضائي والقضاة المتمكنون في الأمور الفنية، والتي لن يتسنى تحقيقها إلا عن طريق التدريب والتأهيل في المجال التقني المعلوماتي.

وكل هذه الأمور لا تؤدي إلى الكشف عن الحقيقة إلا بالحصول على الدليل الإلكتروني الرقمي، الذي يقوم عليه الإثبات الجنائي في الجرائم المعلوماتية للوصول إلى الحقيقة المطلقة،

---

[1]– الفقرة الأخيرة من المادة 05 من القانون رقم (09-04).

[2]– الفقرة (ب) من المادة 13 من قانون رقم (09-04).

وبالتالي من المهم جدا التعرض إلى الدليل الرقمي والذي لنَا الحديث عنه في الفصل الثاني كما سيأتي.

الفرع الخامس :الشهادة:

لقد أورد المشرع الجزائري الشهادة في الفصل الأول من الباب الأول من الكتاب الثاني تحت عنوان في طرق الإثبات المواد 212-238 . ما يميز الإثبات في المواد الجزائية هو مبدأ حرية الإثبات إذ يعطي هادا الأخير حرية شاملة و واسعة للقاضي الجزائي في استعمال كافة الوسائل و دلك لإثبات أو نفي الجريمة و ترك للقاضي مسألة تقدير الشهادة كأحد وسائل الإثبات الجنائية المعروفة. فله أن يأخذ به كما له أن يستبعده إذا لم يقتنع به فهي ضرورة من ضرورات العدالة .

فالشهادة كما يسميها الدكتور محمد عيد غريب " أنها تقرير يصدر من شخص لما يكون قد رآه أو سمعه بنفسه أو أدركه على وجه العموم بحواسه في شأن واقعة إجرمية " [1]

كما يعرفه الأستاد إدوار غالي " تعني الإدلاء بمعلومات معينة عن الغير أمام سلطة التحقيق تتعلق بالجريمة" [2]

و منه نري التركيز على الشهادة في حيث أن الشاهد يجب أن يكون قد حضر الواقعة بأحد حواسه و عاينها حتى تقبل منه و إلا أصبحت كاذبة و تسمى شهادة الزور و هي جريمة معاقب عليها حسب القانون .

و يجوز طبقا للمادة 88 من ق إ ج لقاضي التحقيق سماع كل شخص يرى ضرورة سمعاه كإجراء من إجراءات التحقيق من اجل كشف القضية إما لإثباتها أو نفيها و بالتالي يعتبر الشاهد هنا إما شاهد نفي أو شاهد إثبات و يدلي شهادة بعد اليمين بقول الحقيقة و لا شيئ غير الحقيقة و يصرح بما رأه و سمعه و عاينه بنفسه فلا يقبل الشهادة عن طريق التسامع .

---

[1]- محمد عيد غريب حرية القاضي الجنائي في الإقتناع اليقيني و أثره في تسبيب الأحكام الجنائية، د ط . دار الثقافة للنشر و التوزيع,عمان 2006 ص 86 .

[2]- إدوارد غالي الذهبي، الإجراءات الجنائية في التشريع المصري,ط2 مكتبة غريب 1990 ص 434.

و الجريمة المعلوماتية أو جريمة النصب المعلوماتية محل الدراسة و لو ان لها مميزات خاصة إلا أنها في مجال الشهادة لا تختلف عن الشهادة التقليدية , إذ أن الشاهد ملزم بقول كل ما يعرفه من معلومات تخص الجريمة محل المتابعة .

أولا: الشاهد المعلوماتي :

سمي الشاهد المعلوماتي و هاذ لتمييزه عن الشاهد التقليدي , لقاضي التحقيق او من كان على رأس التحقيق أن يسمع الشهود ممن عاينوا الجريمة بأنفسهم و بحواسهم او الأشخاص الخبراء الدين يستطيعون عن طريق تقنيات معلوماتية كشف الجريمة . فهو بالتالي شخص متخصص في المعلوماتية و الوسائل المعلوماتية التي تتيح الولوج إلى نظام المعالجة الآلية للمعطيات و يسمى "شاهدا معلوماتيا " .

ثانيا كشف الأسرار : كون أن هادا الشاهد المعلوماتي شخص دو خبرة في مجال المعلومات فهل واجب عليه ان يكشف عن الأسرار و خاصة منها كلمات التشفير و المرور في الجرائم أم أنه ملزم فقط بقوم ما شاهده . و انقسم الفقه في هادا الشأن في حين أن التشريع يقرر صراحة حماية حرمة الحياة الخاصة التى لا يجب الاعتداء عليها تحت أي شكل .

فالقسم الأول يرى ان من واجب الشاهد فتح الملفات و تهكيرها عن اقتضى الأمر من أجل ضرورات التحقيق و يرى قسم ثان من الفقه بعدم جواز تهكيرها الاكتفاء بالشهادة [1]

الفرع السادس: الاعتراف : هو إقرار المتهم على نفسه بصدور الواقعة الإجرامية منه و يتضح من دلك أن الاعتراف تقرير أو إعلان و ان مضمونه هو الواقع .

فلا يعقل أن يعترف الشخص ضد نفسه بواقعة لم يفعلها و هادا من اجل أن يخلص شخصا أخرا لأي سبب و هادا خلافا للقاعدة المغلوطة التي لا أساس لها " أن الاعتراف سيد الأدلة " إذ أن الاعتراف كغيره من أدلة الإثبات يخضع للسلطة التقديرية للقاضي .

و أيضا من شروط صحة الاعتراف أن يكون صادرا عن المتهم نفسه . و أن يكون مخيرا و حرا في الاعتراف و دون أي إكراه كما يجب أن يكون الاعتراف محددا و واضحا لا يحتمل أي تأويل .

[1] – محمد طارق عبد الرؤوف الحق, مرجع سابق ص 307 .

في حالة الجريمة المعلوماتية المعترف كما سبق الذكر هو شخص محترف و يمتلك مهارات تقنية عالية تسمح له بإرتكاب الجريمة المعلوماتية بصفة عامة و باتالي يكون اعترافه مبني على أساس منطقى و مقبول بحيث يكشف طريقته الاحتيالية التي نصب بها على الضحايا أو يتم الإستعانة بخبير لقييم هاذا الاعتراف[1].

الفرع السابع :القرائن: هي عبارة عن علاقة منطقية بين واقعة معلومة و أخرى مجهولة يريد إثباتها , فالقاضي هو مصدر هذه القرينة و تسمى كدلك بالقرينة الفعلية أو الإقناعية لأن القاضي يصل إليها من خلال إقتناعه الشخصي أو الموضوعي.

و من خصائصها أنها دليل استنتاجي و دليل إثبات غير مباشر كما أنها قرينة موضوعية او شخصية كما أن من اهم ما يميز القرائن فهي لا يمكن حصرها و دلك لطبيعتها الذاتية و الموضوعية.

وبالتالي لا يمكن الأخذ بها لوحدها و إنما تكون مكملا لدليل أخر لأنها متوقفة على استنتاج و قد يحمل الخطأ [2].

في مجال الإجرام المعلوماتي يبقى نفس الحكم قائما بشأنها فالدليل الرقمي هو الأخر يعود تقديره للقاضي , على سبيل المثال عندما يعلم adresse ip الخاص بالحاسوب . هنا في هذه الحالة لا يكشف الفاعل مباشرة و إنما الحاسوب الذي ارتكبت منه الجريمة على عكس الدليل العلمي .

المطلب الثاني: ماهية الدليل المعلوماتي " الرقمي" كدليل إثبات في المواد الجنائية

ترتكز عملية الإثبات الجنائي للجرائم المعلوماتية على الدليل الجنائي الرقمي ، ذلك أن الوسيلة الوحيدة و الأساسية لإثبات هذا النوع من الجرائم ، و هو محور اهتمام بحثنا لذا ستناول في هذا المبحث مفهوم الدليل الرقمي في المطلب الأول ، بينما في المطلب الثاني

---

[1]– حسنى محمود نجيب , شرح قانون الإجراءات الجنائية , دار النهضة العربية القاهرة 1982 ص 472 .

[2]– عبد الحميد الشواربي القرائن القانونية و القضائية في المواد المدنية و الجنائية و الأحوال الشخصية ,د ط , الإسكندرية منشأة المعارف ص20 .

نتطرق لموقف المشرع الجزائري من الدليل الرقمي و نحدد أنظمة الإثبات الجنائي في الأنظمة القانونية.

الفرع الأول :مفهوم الدليل الرقمي

بإعتبار أن الدليل الرقمي ذو أهمية بالغة في مجال الإثبات الجنائي للجرائم المعلوماتية ، فإنه يجب التعرض عليه بتحديد مفهومه من خلال تعريفه و تعداد تقسيماته و خصائصه ، و أنواع و أمثلة عنه فيما يلي :

الفرع الأول :تعريف الدليل الرقمي و تقسيماته: لقد تنوعت و اختلفت تعريفات و تقسيمات الدليل الرقمي كما سنراه:

أولا: تعريف الدليل الرقمي:

يعرف البعض الدليل الرقمي، على أنه " **الدليل المأخوذ من أجهزة الحاسب الآلي و يكون شكل مجالات أو نبضات مغناطيسية أو كهربائية، ممكن تجميعها و تحليلها باستخدام برامج و تطبيقات و تكنولوجيا خاصة، و يتم تقديمها في شكل دليل يمكن اعتباره أمام القضاء.**

وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات و الأشكال و الرسوم ، و ذلك من أجل الربط بين الجريمة و المجرم و المجني عليه و بشكل قانوني يمكن الأخذ به أمام أجهزة إنفاذ و تطبيق القانون " [1].

في حين عرفه الدكتور عمر محمد أبو بكر بن يونس على أنه: " الدليل الذي يجد له أساسا في العالم الإفتراضي و يقود إلى جريمة " ، فيعد الدليل الرقمي الدليل المستعان بتقنية

[1]– ممدوح عبد الحميد عبد المطلب ، البحث و التحقيق الجنائي الرقمي في جرائم الكمبيوتر و الأنترنت ، د،ط ، دار الكتب القانونية ، مصر ، 2006 ، ص 88.

المعالجة الآلية للبيانات ، و الذي يؤذي بقاضي الموضوع إلى اقتناعه بثبوت ارتكاب الجريمة من شخص ما [1].

و كذلك و ضع البعض الآخر تعريف للدليل الرقمي على أنه : "هو ذلك الدليل المشتق من أو بواسطة النظم البرامجية المعلوماتية الحاسوبية ، و أجهزة و معدات أدوات الحاسب الآلي، أو شبكات الاتصالات من خلال إجراءات قانونية و فنية لتقديمها للقضاء بعد تحليلها علميا أو تفسيرها في شكل نصوص مكتوبة ، أو رسومات أو صور أو أشكال أو أصوات ، لإثبات وقوع الجريمة و لتقرير البراءة أو الإدانة فيها "[2].

إن مقدمات التعامل مع الدليل الرقمي تشير بكونه يتجاوب مع التطور الحاصل بسرعة فائقة حيث انه بعدما كان الدليل الصامت و الثابت يقدم ما يمكن الحصول منه على نسخ عن طريق الطباعة .**Print out** و الذي يطلق عليه تسمية " مخرجات الحاسوب" مثل الوثائق **Document** ، و الصور ***Pics ..إلخ*** فإن التطور اقتضى أن يكون هناك مظهر جديد للدليل الرقمي ذاته و هو المظهر التقني المعلوماتي الذي يتميز بالحركية و الذكاء[3] .

ثانيا: تقسيمات الدليل الرقمي: للدليل الرقمي أشكال مختلفة ، و قد قسمها البعض إلى الأقسام الأساسية التالية :

- أدلة رقمية خاصة بأجهزة الحاسب الآلي و شبكاتها.

- أدلة رقمية خاصة بالشبكة الدولية للمعلومات "**الأنترنت**".

---

[1]-عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت رسالة دكتوراه, كلية الحقوق عين الشمس,2004 ، ص969.

[2]-عبد الناصر محمد محمود فرغلي و محمد عبيد سيف سعيد المسماري الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية و الفنية ,دراسة تطبيقية مقارنة,المؤتمر الربي الأول لعلوم الأدلة الجنائية و الطب الشرعي .جامعة نايف العربية الرياض 2007، ص 13.

[3]- عمر محمد أبو بكر بن يونس، مرجع سابق، ص 969.

– أدلة خاصة ببروتوكولات تبادل ونقل المعلومات بين أجهزة الشبكة العالمية للمعلومات.

بالتالي هذا التقسيم يتطابق مع تقسيم الجريمة عبر الحاسب الآلي[1] .

و قد قررت وزارة العدل الأمريكية لسنة 2002 أن الدليل الرقمي يمكن تقسيمه كالتالي :

1– السجلات المحفوظة في الحساب الآلي و تشمل الوثائق و الملفات معالجة مثل **Winword** ورسائل و غرف المحادثات عبر الأنترنت [2].

2– السجلات التي تم إنشاؤها و إعدادها بواسطة الحاسوب ، و هي تعد مخرجات الحاسوب، و التي لم يشارك الأشخاص فيها مثل سجلات الهاتف وفواتير أجهزة الحاسب الآلي **files**.[3]

3–السجلات التي حفظ جزء منها بالإدخال وجزء ثم إنشاؤه عن طريق الحاسب الآلي ، ومنها أوراق العمل المالية التي تحتوي عل مدخلات تم تلقيها مباشرة إلى برامج أوراق العمل ، و بعد ذلك تتم معالجتها من خلال البرنامج بإجراء العمليات الحسابية عليها تلقائيا مثل **Exel**.

الفرع الثاني: خصائص الدليل الرقمي يمتاز الدليل الرقمي عن غيره من الأدلة الجنائية بعدد من الخصائص التالية :

1– تتكون الأدلة الرقمية من بيانات ومعلومات إلكترونية غير مرئية و غير ملموسة ، بحيث يتطلب لإدراكها استخدام أجهزة و معدات الحاسب الآلي **Hardware** واستعمال نظم برمجيات الحاسوب **Software** [1].

---

[1]– ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 88.

[2]– عبد الناصر محمد محمود فرغلي ، محمد عبيد سيف سعيد المسماري ، مرجع سابق ، ص14.

[3]– خالد عياد الحلبي ، إجراءات التحري و التحقيق في جرائم الحاسوب و الإنترنت,دار الثقافةللنشر و التوزيع ,عمان الأردن2011 ، ص 234.

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، و هذا 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 و هذا 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 ، و هذا ما حذا به المشرع البلجيكي بمقتضى القانون الصادر في **28 نوفمبر 2000م** ، 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 [2]، و عليه ما يميز الدليل الرقمي على أنواع الأدلة الأخرى أنه يمكن أن يستخرج نسخ من الدليل الرقمي مماثلة و مطابقة الأصل و لها نفس القيمة العلمية و الثبوتية ، و هذا ما يكفل وجود ضمانة قوية وفعّالة للحفاظ على الدليل ضد الفقدان و التلف و التغيير من خلال وضع نسخ طبق الأصل من الدليل [3].

4- صعوبة التخلص من الدليل الرقمي ، و تعتبر هذه الخاصية من أهم مميزات الدليل الرقمي باعتبارها ميزة يتمتع بها الدليل الرقمي عن غيره من الأدلة ، بحيث يقتضي الأمر مقارنة بين الدليل الرقمي و الدليل الجيني الذي يطلق عليه الحمض النووي **DNA** ، ذلك لاتحاد كل منهما في هذه الخاصية التي تتمثل في صعوبة التخلص منها من جهة ، ومن جهة أخرى من الممكن إحداث تعديل في تعديل في تكوينهما معا ، و هذا ما يستوجب مقارنة الأدلة الرقمية بالأدلة التقليدية ، حيث أن هذه الأخيرة تستمد قوتها في حالة التسريع بالحصول عليها

---

[1]- عبد الناصر محمد محمود فرغلي ، محمد عبيد سيف سعيد المسماري ، مرجع سابق ، ص14.

[2] - عمر محمد أبو بكر بن يونس، مرجع سابق، ص 7.

[3]- عبد الناصر محمد محمود فرغلي ، محمد عبيد سيف سعيد المسماري ، مرجع سابق ، ص15.

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 ، و كذلك يمكن التخلص من الأوراق و الأشرطة المسجلة إذا كانت تحتوي على ارتكاب أشخاص لجرائم ، و ذلك عن طريق حرقها أو تمزيقها ، و عليه فإن عملية التخلص من هذه الأدلة سهل جدا و من 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 الإستعانة بخصائص التخلص من المستندات في الحاسب الآلي و الشبكة الإلكترونية لا تعتبر من العوائق التي تحيل دون استرداد الملفات ، حيث أنه تتوافر برمجيات من ذات الطبيعة الرقمية يمكن من خلالها استرجاع كامل الملفات التي تم من قبل إلغاؤها أو محوها من الحاسب الآلي أو إظهارها ، و هذا ما يعني صعوبة إخفاء الجاني لجريمته [1].

5- إمكانية توظيف نشاط الجاني لمحو أو إزالة الدليل من الحاسب الآلي كدليل إدانة ضده ، لأن فعل الجاني بمحو الدليل يتم تسجيله في الحاسوب ، و الذي 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 و رصدها و تحليلها في الوقت نفسه ، لأن الدليل الرقمي يمكن أن يقوم بتسجيل تحركات الأفراد و سلوكاتهم و عاداتهم و

[1]- عمر محمد أبو بكر بن يونس ، مرجع سابق ، ص 7.

بعض الأمور الخاصة بهم لذلك فالبحث الجنائي عن الدليل الرقمي يكون بسهولة مقارنة مع الدليل المادي [1].

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

الفرع الثالث: أنواع و أمثلة الدليل الرقمي: للدليل الرقمي أنواع و أمثلة متعددة نذكر منها ما يأتي :

أولا : أنواع الدليل الرقمي : يمكن تقسيم الأدلة الرقمية إلى الأنواع الأساسية التالية :

1- الورق و مخرجات الطابعات :

غالبا ما تترك الجرائم الواقعة على الأموال أو على الأشخاص أثار من الأوراق و المستندات بالغة الأهمية إلي يتم حفظها في الحاسب الآلي ، فالكثير ممن يقومون بطباعة المعلومات بهدف المراجعة أو التأكد من الشكل العام أو صحة المستند موضوع الجريمة ، فالطابعات و أجهزة الحاسب الآلي ذات السرعة الفائقة تطبع الكثير من الأوراق في وقت يسير ، لذلك يعد الورق من الأدلـة الرقمية الـتي يتم من خلالها بحث و تفتيش مسرح الجـريمة ، و للورق أربعة أنواع هي [3] :

أ- المسودة التي يتم إعدادها بخط اليد مثل تصور للعملية التي يتم برمجيتها.

---

[1]- ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 88.

[2]- عمر محمد أبو بكر بن يونس ، مرجع سابق ، ص 980 ،

- Eagham (casey) ,digital evidence and forensic science , Computer and the internet , computer crime -&s ted .Academic press .USAUK

[3]- عبد الله حسين على محمود، سرقة المعلومات المخزنة في الحاسب الالى,ط2,دار النهضة العربية القاهرة 2001، ص 397.

ب- أوراق تالفة و التي تتم طباعتها للتأكد من برمجة العملية ، و من ثم إلقاؤها في سلة المهملات.

ج- الأوراق التي تتم طباعتها و الإحتفاظ بها لأغراض تفيد الجريمة.

د- الأوراق الأساسية و المحفوظة في الملفات العادية أو دفاتر الحسابات و خاصة التي يتم تزويرها من أجل تنفيذ الجريمة [1].

2- **الأجهزة الإلكترونية ، و منها :**

أ **– الحاسب الآلي و ملحقاته** : لتحديد الجريمة على أنها جريمة معلوماتية مرتبطة بالمكان أو بالشخص يفترض وجود حاسب آلي ، حيث بإمكان خبير الحاسب الآلي التعرف على جهاز وموصفاته مع تميزه عن غيره من أجهزة الحاسب الآلي الأخرى ، بالإضافة إلى كيفية تحديد أسلوب التعامل مع أثناء الضبط و التحريز[2] .

ب- الطابعات : تقوم الطابعات باستخراج ما تم تحضيره لطباعته ، و تختلف أنواعها من عادية و ليزرية ، ملونة وغير ملونة ، حيث غالبا تستخدم في مجال التقنية المعلوماتية .

ج- المووديم : هي الوسيلة التي يمكن من خلالها لأجهزة الحاسب الآلي من الإتصال ببعضها البعض عبر خطوط الهاتف ، كما يقوم ذلك بإرسال الفاكس و الرد على المكالمات الهاتفية ، و تبادل البيانات و تعديلها ،و يأخذ أشكال متنوعة مرتبطة بتطور تقنية المعلومات.

---

[1]- سيدي محمد لبشير ، دور الدليل الرقمي في إثبات الجرائم المعلوماتية, دراسة تحليلية تطبيقية رسالة ماجستير في العلوم الشرطية تخصص التحقيق و البحث الجنائي كلية الدراسات العليا جامعة نايف العربية للعلوم الامنية ,لرياض 2010، ص 71.

[2]- عبد الله حسين على محمود ، مرجع سابق ، ص 398.

د- الهاتف النقال: يعتبر جهاز الإلكتروني حجمه صغير يفيد التواصل بين الأشخاص عبر الهواء ، و قد تطـور في الآونة الأخيرة ، فأصبح يتمتع بأشكال و مميزات أحدث أجهزة الحاسب الآلي اليوم ، و أطلق عليه تسميات عدّة منها الجوال ، و المحمول و الخلوي و النقال ..إلخ [1].

3- وسائل التخزين : و منـها :

أ- القرص الثابت الداخل، يعد الوحدة الرئيسية التي يتم من خلالها تشغيل نظام الحاسب و البرامج و البيانات.

ب- الأقراص المدمجة **CD** هي وحدات تخزين منتقلة تحتوي على معلومات،و تقوم بتخزين هذه المعلومات عليها و إعادة تسجيلها.

ج- ذاكرة فلاش **USB**، و هي سهلة النقل و التبادل و حجمها صغير تعمل على تخزين و نقل البيانات و لها قدرات تخزين و أحجام مختلفة و متنوعة [2].

د- الأشرطة الممغنطة **Magnetic Tapes**، و هي وسيلة تستخدم غالبا في الحفظ الاحتياطي للبيانات و المعلومات و توضع في مكان بعيد و آمن ، و ما يقوم البعض بإيداعها لدى خزائن البنوك أو مراكز التوثيق الحكومية الأمنية.

و- البطاقات الممغنطة و بطاقات الائتمان القديمة و المواد البلاستيكية المستخدمة في إنشاء تلك البطاقات ، قد يمكن أن تكون قرائن للإثبات في الجرائم المعلوماتية [3] .

4- البرامج، و منـها:

---

[1]- سيدي محمد لبشير، مرجع سابق، ص 71.

[2]- مرجع نفسه ، ص 72.

[3] -عبد الله حسين علي محمود، مرجع سابق، ص 399، 400.

أ- **برامج نظم التشغيل:** أعدت هذه البرامج المصممة لتحديد تشغيل نظم الحاسب الآلي، و التي تقوم باستقبال و إخراج المعلومات و البيانات و التحكم في الذاكرة و التخزين و إدارة التطبيقات.

ب- **برامج التطبيقات:** تعتبر برامج مصممة لتحديد تشغيل نظام الحاسب الآلي، و التي تقوم باستقبال و إخراج المعلومات و البيانات و التحكم في الذاكرة و التخزين و إدارة التطبيقات.

ب- برامج التطبيقات: تعتبر برامج مصممة أساسا لأداء وظيفة محددة كمعالجة النصوص، بالإضافة إلى إدارة قاعدة البيانات، و يتم تحميل مثل هذه البرامج في حالة الحاجة إليها [1].

الفرع الرابع: مصادر الحصول على الدليل الرقمي:

إن مصادر الحصول على الدليل الرقمي تكمن في البيئة الرقمية التي ارتكبت فيها الجريمة المعلوماتية، وتتمثل في أجهزة الحواسيب الخاصة بالجاني أو المجني عليه وكذا أجهزة مقدم الخدمة.

وهذه المصادر قد تكون على سبيل المثال لا الحصر إذ أن التطور العلمي والتقني قد يسفر عن أنواع جديدة من المصادر التقنية ، إذ المقصود هنا من أين يمكن لجهات التحقيق والتحري عن الجريمة المعلوماتية استخلاص الدليل الرقمي , إد أننا ركزنا على طريقة فحص جهاز الحاسوب الخاص بالجاني و الضحية و هنا فحص جهاز الحاسوب كونه أقرب طريقة منطقية من أجل الحصول على الدليل العلمي أو الرقمي من أجل إثبات أو نفي الجريمة و لكن قد تكون هناك طرق أخرى مثل التسرب و اعتراض المراسلات و حفظ المعطيات المتعلقة بحركة السير و غيرها الكثير من الطرق الأخرى.

- فحص جهاز الحاسوب الخاص بالجاني و المجني عليه:

[1]- سيدي محمد لبشير، مرجع سابق، ص 71.

إن فحص جهاز الحاسوب الخاص بالجاني يمكن من التحقق وبيان الطريقة التي قام بها هذا الأخير في ارتكاب جرائمه، ومما لا شك فيه أن الجاني عليه هو المصدر الكاشف والنتيجة التي يترتب عليها ما قام به الجاني من جرائم، وبالتالي فإن فحص جهاز الحاسوب الخاص به يمكن المحقق من معرفة الدخول وتتبع مصدره.

ويمكن الوصول إلى الدليل الرقمي المتعلق بالجرائم المعلوماتية من خلال أجهزة الحاسوب سواء الخاصة بالجاني أو الجاني عليه عن طريق البحث في المصدرين التاليين:

أولا :أنظمة الحاسوب وملحقاتها:تعد الحواسيب مصدرا غنيا بالأدلة الرقمية خاصة تلك الحواسيب الشخصية التي تعد بمثابة أرشفة سلوكية للأفراد، فهذه الحواسيب تحتوي على الكثير من المعلومات المتعلقة بنشاطات الأفراد و رغباتهم، وعملية حجز الحاسوب بقصد تفحصه تعد نقطة البداية في الكشف عن خفايا الجريمة المعلوماتية باعتبار أن هذا الجهاز هو وسيلة تنفيذها.والحاسب الآلي في ذاته يقوم في تركيبته على أمرين هما :القطع الصلبة (hardware) و القطع المرنة.

وهناك عنصر ثالث يتوزع بين البرمجيات (Soft Ware) والقطع الصلبة وهو عنصر البرمجيات المعلوماتية. لذلك فإن الأمر يستلزم أن يكون الفحص ماديا ومعنويا للارتباط القائم بشكل طبيعي بين مكونات الحاسوب ككل.

وقد تعتمد عملية الفحص على الحاسوب ذاته أي ما يسمى بالفحص الذاتي من خلال قيام الحاسوب ذاته بفحص مكوناته وتقديم تقرير كامل بذلك إلى طالب الفحص، ومثل هذه العملية تتطلب من القائم بها مهارة عالية أو قد يتم الفحص عن طريق الاستعانة بجهاز آخر أو أجهزة تقنية للبحث في جزئيات عبر جهاز الحاسوب.ويجب أن تشمل عملية الفحص على ما يلي:

1- فحص القرص الصلب :يحتوي القرص الصلب بداخله على مجموع البيانات الرقمية ذات الطابع الثنائي والتي تتميز بعدم تشابهها فيما بينها على الرغم من وحدة الرقم الثنائي (0.1) وتتم عملية فحص القرص الصلب أما كليا أو جزئيا، فالفحص الجزئي يؤدي إلى التعرف على محتوى البيانات والتي يؤدي التعامل معها إلى الكشف عن القيمة الإستردادية للبيانات المخزونة فيه سواء كانت محتويات مكتوبة، صور أو أصوات.....إلخ.

بالإضافة إلى إمكانية معرفة ما تم حذفه من بيانات وبرامج بالاستعانة ببرمجيات خاصة للقيام بذلك،والمثال المستخدم هنا هو حالة البحث في ملفات النسخ وهذه الأخيرة هي عبارة عن ملفات تأخذ نسخة احتياطية عن كل صفحة يتم الولوج إليها عبر الانترنت كما توجد ملفات خاصة بالتنزيل الآلي (Download file) مهمتها استقبال الملفات التي يتم تحميلها على جهاز الحاسب من خارجه وعبر الانترنت فهذه الملفات مركزها القرص الصلب.

وللتعرف على محتويات القرص الصلب فإن ذلك يتوقف على مسائل عديدة منها الكيفية التي يتم بها ضبط الحاسوب ومهارة الشخص القائم باستخلاص البيانات دون العبث بمحتوياتها لذلك فإنه عند ضبط جهاز الحاسب الآلي، على المحقق أن ينتزع القرص من الجهاز الخاص به ويحافظ عليه من الارتجاج أو الاصطدام بأي شيء، وعدم محاولة تفريغ أي بيانات متواجدة عليه وذلك تلافيا لفقد أي بيانات، وتسليمه إلى الفني الخبير المختص الذي يقوم بتحليل النسخ التي تصدر من القرص وبعرض ما توصل إليه على المحقق.

وهنا لابد من مراعاة شرط سلامة جهاز الحاسب الآلي، الذي يعني صحة حركة القطع الصلبة فيه وذلك لتجنب الوقوع في مأزق رفض المحكمة الاعتداد بالدليل المنبثق عنه، فشرط سلامة الحاسوب مطعن رئيسي على كل دليل تم الحصول عليه بحيث يجب الكشف على حركة الحاسوب بداية والإقرار بسلامته.

و إن من الأشياء التي تظهر بعد عملية فحص أي قرص صلب لأي جهاز تلك البيانات التي كان يستخدمها الجاني، وكذا الصور المخزنة فيه ومخابئ صفحات الانترنت، ومن خلالها يمكن التوصل لصفحات وعناوين مواقع الانترنت وكذا رسائل البريد الإلكتروني بالإضافة إلى رؤوس الصفحات المرسلة و الملقاة ومجموعة البرامج الجاهزة المتخصصة التي استخدمها المشتبه فيه (ومنها يمكن تحديد أصدقاء) المشتبه فيه وكذا تحديد ما يتحاورون فيه.

2 فحص البرمجيات :يتطلب الأمر في مثل هذه الحالة أن نميز بين الفحص الداخلي للبرمجيات والفحص الخارجي لها .فالفحص الداخلي يتم من خلال البحث في البناء المنطقي للبرمجة بما يوحي من بأن هناك مجهودا تجديديا في إعداده للعمل حين إنزاله على جهاز الحاسب الآلي Installation خلال تتبع خطوات منطقية تعبر عن هذا الجهد، وأكثر ما يتم البحث عنه في إطار الفحص الداخلي هو البحث عن مصدر الملفات الموجودة في هذا الإطار، ذلك أن النسخ عبر الانترنت لا يشبه النسخ باستخدام برمجيات المعالجة فالأول نسخ عبر العالم الافتراضي والثاني يتم باستخدام مصنف متداول في العالم المادي.وتفيد وسيلة النسخ في ترتيب كيفية حدوث الجريمة.

أما في حالة الفحص الخارجي والذي يتم اللجوء فيه إلى النسخة الأصلية للمقارنة بينها وبين النسخة محل الاشتباه وذلك للدلالة على ثبوت ارتكاب الجريمة بدرجة مقنعة.

وفي كلتا الحالتين ينبغي التنبيه إلى خطورة البرمجيات المعيبة التي يمكن أن تؤثر في الحاسوب وتجعله محل شك تهتز معه قيمة الدليل، يكون لهذا القصور أثره في عملية تقييم الدليل المستمد من البرمجيات ذاتها.

3-فحص النظام المعلوماتي :إن المهمة الأساسية لكل نظام معلوماتي هو تحقيق فرضية تنفيذ الأوامر التي يمكن أن يقوم بها مستخدم الحاسوب، وتعني عملية فحص النظام المعلوماتي ضبط كافة ما يحتويه جهاز الحاسب الآلي من معلومات يمكن استرجاعها عبره

تكون مخزنة في ملفات على أي شاكلة يمكن أن تكون عليها الحركة الاسترادادية ما دام موضوعها يشكل جريمة.

والحقيقة أنه على حسب كثرة التعامل بالحاسب الآلي يتكاثر محتوى النظام المعلوماتي مما يزيد من صعوبة فحصه بالنظر إلى الحجم الضخم والكم الهائل من المعلومات المخزنة فيه.

بالإضافة إلى أن عملية تحزين البيانات لا تتخذ شكلا محددا وإنما تتنوع أساليبها، والتي يصل مداها إلى حد إمكانية تخزين البيانات بشكل آمن في الحاسوب بنظام التشغيل أو بنظام إخفاء البيانات المعلوماتي بحيث لا يظهر الملف حتى في حالة البحث الآلي للحاسب عنه والذي قد يحتوي على مواد إجرامية، وتفوت الفرصة بسبب هذه التقنية على المحققين من الوصول إليه.

الفرع الخامس: موقف المشرع الجزائري من الدليل الرقمي في مجال الإثبات الجزائي و أنظمة الإثبات الجنائي.

إن الإثبات في المواد الجنائية هو النتيجة التي تتحقق باستعمال وسائله وطرقه المختلفة للوصول إلى الدليل الذي يستعين به القاضي لاستخلاص حقيقة الوقائع المعروضة عليه و إعمال حكم القانون عليها، ويعني ذلك أن موضوع الإثبات هو الوقائع وليس القانون.

وبالتالي فإن الإثبات الجزائي هو كل ما يؤدي إلى كشف غموض الجريمة وإقامة الدليل على وقوعها والتأكد من أن المتهم هو مرتكب الجريمة بالفعل ووجود الدليل على ذلك، ويعتبر الدليل الوسيلة القانونية التي يستعين بها القاضي للوصول إلى الحقيقة وكشف غموض الجريمة ونسبتها إلى المتهم.

ولقد ذهب الفقه الإجرائي إلى وضع نظامين إجرائيين في مجال الإثبات الجزائي يختلفان فيما بينهما من حيث الأسس التي يقوم عليها كل واحد منهما وهذه الأنظمة هي:

نظام الإثبات القانوني أو المقيد وفيه يحدد القانون الأدلة التي يجوز الأخذ بها والاستناد عليها.

والثاني هو نظام الإثبات الحر أو المطلق وفيه لا يقيد القانون القاضي بأدلة معينة في إثبات الواقعة وله أن يقتنع بأي دليل يعرض عليه.

و من هاذا المنطلق أخد المشرع الجزائري بالنظام التوفيقي أو ما يسمى النظام المختلط حيث في عامة الجرائم أخد بالإثبات الحر أما في بعض الجرائم مثل جريمة الزنا أخد بالنظام القانوني أو المقيد,و بالتالي جريمة النصب التقليدية تقع ضمن الجرائم التى يجوز فيهاالإثبات بطريقة حرة و غير مقيدة.

فنصت المادة 212 من قانون الإجراءات الجزائية على أنه يجوز إثبات الجرائم بأي طريق من طرق الإثبات وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص "....كما نصت المادة 307 من قانون الإجراءات الجزائية أيضا أن القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم وأن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة للمتهم"....

ومن خلال هذين النصين القانونيين يتضح جليا أن المشرع الجزائري قد تبنى كقاعدة عامة نظام الاقتناع الشخصي للقاضي الجزائي، إلا واستثناء نجده أخذ أيضا بنظام الأدلة القانونية في إثبات بعض الجرائم أين اشترط لإثبات أدلة قانونية محددة مسبقا وعلى سبيل الحصر.وبتحليل المادة 212 من قانون الإجراءات الجزائية نجدها تكرس قاعدتين تكمل إحداهما الأخرى، قاعدة الاقتناع الحر للقاضي الجزائي من جهة وقاعدة حرية اختيار وسائل الإثبات الجزائي من جهة أخرى.

وإذا كان الدليل الرقمي ذو الأصالة العلمية هو الأوفر والأنسب في إثبات الجريمة المعلوماتية بصفة عامة و جريمة النصب المعلوماتي بصفة خاصة.

الخاتمة

كان لثورة المعلومات التي بزغ فجرها في أواخر القرن الماضي و ظهور الحاسوب و شبكة المعلومات بالغ الأثر في التطور الذي شهده العصر الحالي و العصر السابق .

بدليل أن مستوى العلم و المعرفة الذي بلغهما العالم ليسا إلا مظهرا من مظاهر التطور،إذ أن العالم حقيقة استفاد بشكل كبير من هاذ التطور الذي جعل العالم مريحا.

غير أن الاستعمال المشروع لأجهزة الحاسب و شبكة المعلومات عكر وجود هاده الأنظمة من خلال الإجرام ألمعلوماتي وعمليات الاحتيال الممارسة من قبلهم ضد من يلج هذه الأنظمة.

و بالتالي النصب المعلوماتي صورة من صور الإجرام ألمعلوماتي الذي يسخر فيه المجرم ألمعلوماتي جهاز الحاسوب و نظام المعالجة من اجل تنفيذ مخططاته الإجرامية , مستغلا في ذلك نقص و قصور القوانين في تنظيم هادا النوع من الإجرام , ناهيك عن براعتهم في استخدام الحاسب و الشبكة المعلوماتية.

التوصيات:

1- الإسراع في إنشاء مشروع الحكومة الإلكترونية و الذي من خلاله يتم السعي إلى استخدام تقنية المعلومات و الاتصالات الإلكترونية و لتوفير و تقديم خدمات المعلومات للمواطنين و الحكومة و بالتالي توفير حماية أكبر.

2- بموجب المادة 44 من ق إ ج و مادة 05 من الأمر 04/09 أقترح أن يضيف المشرع فقرة أخري تقيد التفتيش خاصة في أجهزة الحاسوب و المعلومات عند قيام ضابط الشرطة القضائية بتنفيذ أمر التفتيش.

3- لخطورة المجرم المعلوماتي و خاصة انه عادة لا يستعمل حاسوبه الخاص , أقترح أن يعاد تنظيم عمل مقاهي الإنترنت كأن يفرض عليها القيام بإعداد استمارات المعلومات لكل زبون يثبت فيها هويته و الحاسوب الذي استعمله و التوقيت.

4- تدريب و تكوين رجال الأمن و الدرك في مجال المعلوماتية من اجل حماية أوسع من الإجرام المعلوماتي , كما أدعو إلى تأسيس مدارس خاصة بضباط شرطة مختصين في نفس المجال .

5- العمل على تثقيف المواطنين و نشر ثقافة معلوماتية من أجل أن يكونوا أكثر حذار في التعامل مع أنظمة المعطيات و أيضا من اجل أن يقوموا بمراقبة ولوج أبنائهم إلى نفس المجال.

6- تطوير نظام المعلوماتية و نظام الحماية لأجهزة و مواقع الدولة الرسمية خاصة ما يتعلق ببنك المعلومات الخاص بالمواطنين و الإدارات.

7- العمل على تشريع قانون خاص جديد يحدد طبيعة كل الجرائم المرتبطة بالمعلوماتية و أيضا إرفاقه بقانون إجرائي خاص به من أجل متابعة المجرمين المعلوماتيين.

8- ضرورة القيام بمعاهدات دولية و الحرص على تطوير و تثمين التعاون الدولي في مجال الجريمة المعلوماتية بصفة عامة لما لها من خطورة تضر بمصالح الدول كافة.

9- عدم إهمال الجرائم المعلوماتية و خطورة المجرمين المعلوماتيين عند تحضير الدولة سياستها الجنائية.

10- تجريم بعض صور النصب المعلوماتي مثل التحويل الإلكتروني الغير مشروع للأموال.

11- ضرورة تكوين قضاة التحقيق و قضاة الموضوع في مجال المعلوماتية.

12- فيما يتعلق ببطاقات الائتمان أو بطاقات السحب , حرص المؤسسات المالية على إظهار الساحب بطاقة الهوية كإجراء سابق على السحب من أجل حماية الأفراد.

13- التركيز على العقوبات المالية ضد المجرمين المعلوماتيين و بالتالي نعاقب المجرم بالهدف الذي كان يسعى له من جهة و من جهة أخرى من اجل تفادي مساوئ الحبس.

14- الجريمة المعلوماتية أو جريمة النصب موضوع البحث من الجرائم الخطيرة التي يجوز تسليم المجرمين فيها و تفعيل إجراءات المساعدة و تبادل المعلومات بشأنها كونها تكتسى طابعا عالميا و عابرا للحدود.

15- تجريم فعل الاحتيال على الآلة مثل الاحتيال على عدادات الكهرباء و الغار بنصوص صريحة.

إهداء

شكر و عرفان

مـلخص المذكرة

تعتبر جريمة النصب من ضمن أكثر الجرائم تطورا و استخداما للذكاء و الدهاء و الحيلة كما أن البعض من هؤلاء المجرمين يعمل جاهدا من أجل الإيقاع بضحاياه دون حتى أن يكشف عن اسمه ، ويسعى في خلق حيل وطرق تتناسب مع التطورات والاحتياطات المبذولة، لأجل تمرير أعمالهم الإجرامية تحت غطاء يوهمون به الآخرين أن أعمالهم مشروعة و تحقق نتيجة تسعى الضحية لتحقيقها و الوصول إليها.

و في ضل غياب نصوص قانونية صريحة تجرم فعل النصب الإلكتروني اكتفى المشرع الجزائري بتجريم النصب و الاحتيال بصفة عامة من خلال المادة 372 من قانون العقوبات هادا من جهة, و من جهة أخرى غياب النصوص الإجرائية الخاصة بمتابعة هذه الجرائم المستحدثة على غرار نظام الإثبات الخاص بها و مآل الاختصاص القضائي بشأنها.

فتطبيقا لمبدأ الشرعية الجنائية التي تعتبر ضمانة أساسية للمحاكمة العادلة و النزيهة من جهة و ضرورة الفصل في القضايا المطروحة أمام القضاء وهنا يجد القضاة أنفسهم مجبرين على الفصل وإيجاد حلول لهذه الأخيرة.

الكلمات المفتاحية: نصب-احتيال-جريمة النصب-إلكترونية-معلوماتية-جريمة