جامعة عبد الرحمن ميرة – بجاية
كلية الحقوق والعلوم السياسية
قسم قانون الجنائي

جرائم إختراق الأمن السيبراني في التشريع الجنائي المقارن

مذكرة لنيل شهادة الماستر في الحقوق
تخصص القانون الجنائي والعلوم الجنائية

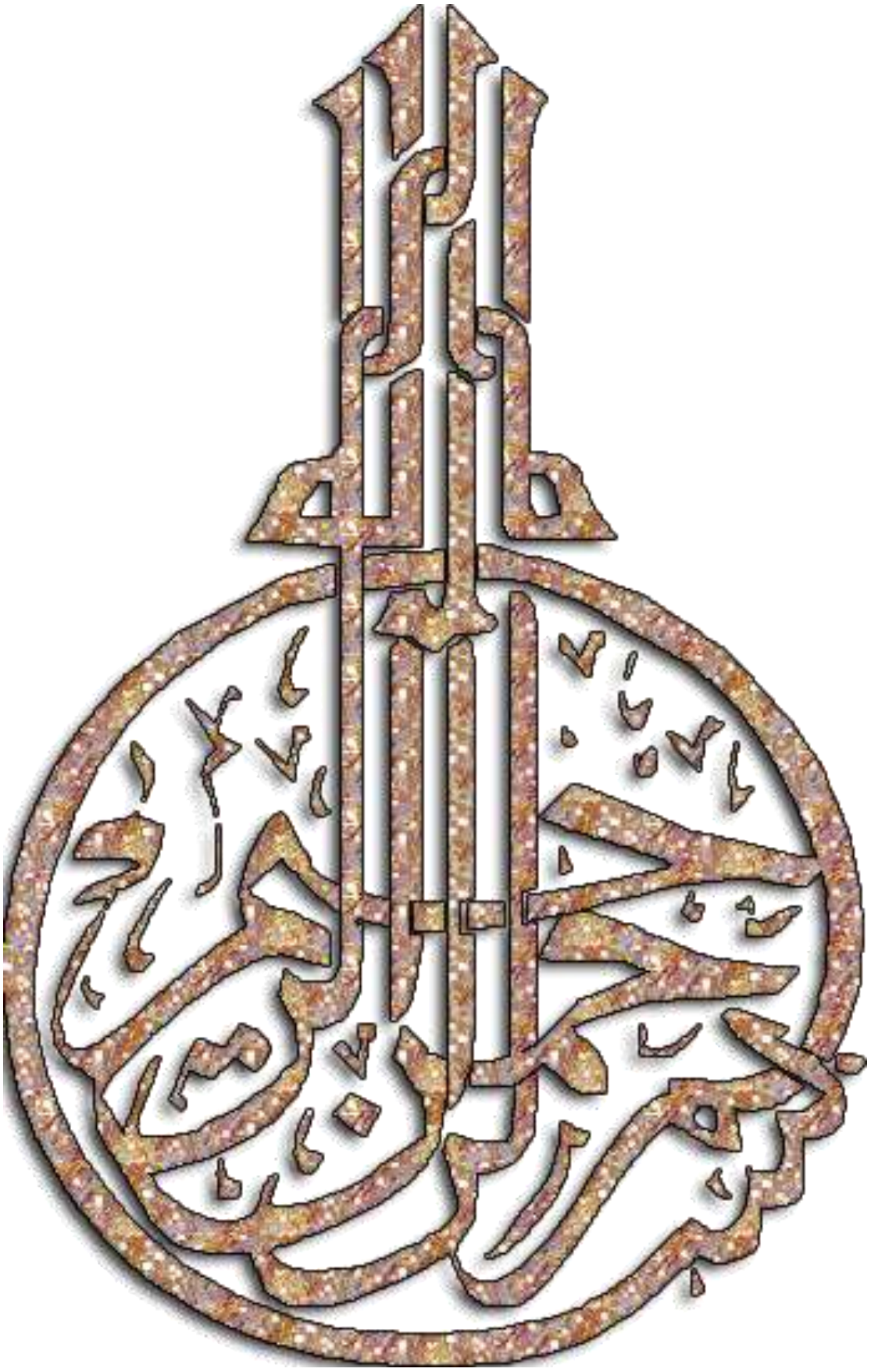
من إعداد الطالبة:
مجة حفصة

تحت إشراف الأستاذ:
أ.د. خلفي عبد الرحمن

لجنة المناقشة:

الأستاذ: مدوري زايدي	أستاذ جامعة بجاية	رئيسا
الأستاذ: خلفي عبد الرحمن	أستاذ جامعة بجاية	مشرفا ومقررا
الأستاذ: جبيري نجمة	أستاذ جامعة بجاية	ممتحنا

السنة الجامعية: 2022/2021



شكر وتقدير

قال رسول الله - ﷺ

من لا يشكر الناس لا يشكر الله

شكر الله دائما وأبدا

أتقدم بجزيل شكري إلى أستاذي المشرف "الدكتور خلفي عبد الرحمن " الذي كان نعم السند، بسعة صدره وجميل صبره، وقدرته على التحفيز.

كما لا أنسى بالذكر طاقم قسم الحقوق ممن درسنا على أيديهم ولا يمكنني أن أنكر فضلهم في تكويني.

وأخص بالشكر أساتذتي الكرام أعضاء لجنة المناقشة لما سيولونه من جهد ووقت للتدقيق والتمحيص في شأن هذه المذكرة.

الحمد لله الذي هدانا إلى الصلح...الحمد لله الذي أذاقني ثمرة النجاح...الحمد لله الذي أنعم علي نعمته بكل ارتياح...إلى قائدي وقرة عيني وقدرتي...

إلى الحبيب المصطفى محمد صلى الله عليه وسلم

أهدي ثمرة عملي إلى سندي ومن كان سبب في إكمال هذا المشوار

أبي رحمه الله

إلى التي أنارت لي طريق العلم ودروب الحياة، هي أحق الناس بحسن صحبتي، هي التي جعل الله الجنة تحت أقدامها: أمي الغالية، الحنونة طيبة القلب.

إلى أخواتي اللاتي وقفنا بجانبي طيلة مسيرتي الدراسية وشجعنني على الوصول إلى أعلى المراتب

إلى كل الأقارب وكل صديقاتي.

حفصة

قائمة المختصرات:

م.ج: مجلد

ط: طبعة

ق.إ.ج: قانون الإجراءات الجزائية

ق.ع: قانون العقوبات

ص: صفحة

ج.ر.ج.ج.ع: الجريدة الرسمية للجمهورية الجزائرية عدد

ع: عدد

المقدمة

إن تنامي التوجه نحو التحول الرقمي، وتبني التكنولوجيات العالمية الحديثة عاد بالكثير من الفائدة على الدول و كذا شعوبها، ولكن في المقابل نشأ عنه شق إجرامي يسعى إلى خلق عالم رقمي يستنزف العديد من ايجابيات التكنولوجيا الحديثة الخيرة، و تتميز شبكة الأنترنت عن غيرها من وسائل تقديم المعلومات والخدمات العالمية بجملة من المميزات التي من أهمها الكم الهائل من المعلومات التي يتم تداولها بسهولة ودقة، وكذا سرعة التفاعل بين تلك التقنية والمستخدم وسرعة الإدمان عليها كذلك، ونظرا للتطور الرهيب في تكنولوجيات الاعلام والاتصال والدور الكبير لشبكات الكمبيوتر والذي اصبح يعرف بتسمية "الفضاء السيبراني" أصبحنا نعيش في العصر الرقمي فزادت معه تنامي المخاطر كالتهديدات السيبرانية الرامية إلى إرتكاب جرائم سيبرانية، وهي حديثة تقف عائق أمام تطور المجتمع في كافة الميادين. ولقد بدت النصوص الجزائية التقليدية قاصرة عن ملاحقة هذا النوع من الجرائم، ذلك أن التشريع وليد الحاجة.

هاته الجرائم التي انتشرت وتعددت صورها وازداد حجمها وتسارعت وتيرتها وسهل ارتكابها رغم اختلاف تسمياتها، فأصبحت تقاس مدة ارتكابها بالثواني، والأدهى أنها قد ترتكب في حضور المجني عليه دون علمه بحدوثها؛ فلم تعد الحدود الجغرافية ولا الحواجز الإدارية، ولا بعد المسافات واختلاف اللغات عائقاً أمام مرتكبيها، وباتت مخاطرها تهدد أمن المجتمعات وقيمها، وشكل وجود جرائم إلكترونية بشكل مستمر ومتسارع تحديات كثيرة أمام النظم القانونية، لذا أصبح أمن الفضاء السيبراني يدخل ضمن أولويات للعديد من الدول، ودفعت التهديدات المتزايدة لأمن الفضاء السيبراني العديد من الدول للعمل على بذل جهود مضنية لاستحداث قوانين لمكافحة الجريمة السيبرانية، لذا قامت العديد من الدول باعتماد استراتيجيات من شأنها دعم الجانب العسكري في الفضاء السيبراني ليس فقط ضد الهجمات التي قد يقوم بها الأفراد والقراصنة بل أيضا ضد احتمال استخدامها من طرف بعض الدول في صراعاتها.

بدأ المجتمع الدولي في تنظيم تشريعات لمواجهة هذا النوع الجديد من الجرائم الذي ظهر مصاحبا لاستخدام الحاسب الآلي، والبحث عن آليات مكافحة تكون قادرة على مجابهة هذه الظاهرة الإجرامية واحتوائها ومراعاة طبيعتها وخصوصيتها.

وهو الأمر الذي دفع العديد من الدول والمنظمات والهيئات إلى رفع التحديات لمواكبة التطورات العالمية المتلاحقة، محاولةً اعتماد سياسات رامية إلى تطوير استراتيجيات عملها وجعلها تقدمية، وإعادة صياغة دورها من اجل توثيق أواصر التعاون والعمل المشترك فيما بينها، وتبادل الخبرات بما يساعدها على إيجاد آليات لمكافحة مختلف أنواع الجرائم الإلكترونية التي لم يسلم منها أي ميدان من ميادين الحياة.

غير أن المشرع الجزائري تصدى لهذه الجريمة من خلال سن وتعديل نصوص قانونية وقائية وردعية تجرم الأفعال الماسة بالأنظمة المعلوماتية، أبرزها القانون 04/09 المتعلق بالوقاية من جرائم تكنولوجيات الاعلام والاتصال ومكافحتها الذي كان أحد تلك القوانين التي وضعت آليات وضوابط تتيح ضبط و كشف الجريمة المعلوماتية.

وتكمن اهمية بحثنا في كونه من اكثر المواضيع حداثة أي يكاد يشمل جميع ميادين الحياة بالإضافة الى ظهور انماط اجرامية مستحدثة بشأن الاعتداء على المعلومات. ومن جانب اخر هذا الموضوع يتعلق بالتطور التكنولوجي مما جعل هذه الجريمة مستجدة وتختلف في ميكانيزماتها عن الجريمة التقليدية.

حيث أن اختيار موضوع" جرائم اختراق الامن السيبراني" كان بناء على عدة اعتبارات من اهمها:

* الشغف بكل ماهو جديد في عالم التقنية كتكنولوجيات الإعلام والاتصال، خصوصا ما تعلق بذلك الدمج بين الاعلام والاتصال والقانون.

*الرغبة الذاتية واندراج الموضوع ضمن اهتماماتي كوني طالبة لتعميق معارفي حوله.

*ان الجريمة السيبرانية اصبحت محور الساعة لانتشارها بكثرة ومساسها بحرمة الحياة الخاصة.

*محاولة الوصول الى انجع السبل لمكافحة هذه الجريمة وذلك من خلال دراستنا لها.

ومن الصعوبات التي اعترت طريقي في انجاز هذا الموضوع كونه كما سبق ذكره موضوع مستجد بالرغم من أن المجالات والمقالات تطرقوا له، اضافة الى قلة المراجع المتخصصة في الساحة القانونية الجزائرية، فضلا عن صعوبة اخرى لا تقل عن سابقيها والتي تكمن في كثرة المادة العلمية وهو الامر الذي احدث نوعا من الضغط وعدم التحكم في الافكار يسمح بطريقة عرضها بسلاسة.

إن الغاية المرجوة من هذه الدراسة تتمثل أساسا في تحديد مفهوم الجريمة السيبرانية ومعرفة موقف التشريعات الدولية والوطنية منها، ليس هذا فقط بل محاولة تسليط الضوء على الافعال المجرمة من طرف المشرع الجزائري وموقفه منها، دون اغفال سبل مكافحة هذه الظاهرة العالمية.

ومن اجل المضي قدما في هذه الدراسة وبناء على ما سبق نطرح الاشكالية الجوهرية في السؤال التالي:

ما مدى فعالية السياسة الجنائية لمواجهة الجرائم السيبرانية وحماية امن المعلومات في التشريع الجزائري والتشريعات المقارنة؟

وعلى هذا الأساس اعتمدت المنهج الوصفي لعرض الافكار والمفاهيم وكذلك المنهج المقارن لإبراز الفرق بين مواقف الشريعات الدولية والوطنية من هذه الجريمة.

وحتى اتمكن من معالجة الإشكالية المطروحة إرتأيت ان اقسم الخطة الى فصلين معتمدة التقسيم الثنائي:

الفصل الاول: الجوانب الموضوعية للأمن السيبراني

الفصل الثاني: الاليات القانونية لمجابهة الجريمة السيبرانية

الفصل الأول

الجوانب الموضوعية

للأمن السيبراني

تعتبر مسألة أمن وحماية المعلومات من أهم قضايا العصر-عصر الثورة الصناعية الرابعة - حيث أصبح نجاح أي مؤسسة يعتمد بشكل كبير علي ما تمتلكه من معلومات ؛ حيث اصبحت في الوقت الراهن معظم الدول والمنظمات والشركات الكبرى تركز بشكل كبير على الفضاء السيبراني، لتحقيق أهدافهم ومصالحهم، وأصبحت المواقع الإلكترونية والبرامج عبر الانترنت خاصة تلك البرامج المتعلقة بالبنى التحتية للدول وسيلة وأداة وهدف تسعى إلى امتلاكهم واستغلالها هذه الدولة أو تلك لمصلحتها الخاصة. ولابد من الإشارة إلى خصوصية الفضاء السيبراني في عدم وجود دولة بإمكانها فرض سيطرتها وسيادتها الأحادية عليه، مما أدى ذلك لاستخدامه بشكل يضر الإنسانية فظهرت الهجمات السيبرانية التي لم تكن معروفة إلا في وقت قريب وأصبحت من الأمور الرئيسية التي يتحتم على الدول مواجهتها في العصر الراهن بسبب ما يمكن أن تسببه من دمار شامل يمكن أن يمس الأمن القومي للدولة، حيث يهدف الأمن السيبراني إلى تعزيز الحماية الأنظمة الإلكترونية وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية وجميع مكوناتها المحيطة بالمجتمع من أجهزة وبرمجيات ومعدات وجميع ما يؤثر على تقدم هذه الخدمات.

للجريمة السيبرانية مسميات كثيرة؛ فالبعض يطلق عيها اسم جرائم الحاسب الآلي والبعض الأخر الجرائم المستحدثة أو جرائم الكمبيوتر أو الجرائم الإلكترونية وهذا نظرا لطبيعتها المتغيرة والواسعة فهي على غير الجرائم العادية لأنها لا تترك أثرا ماديا بل وحتى تهدد اقتصاد الدول وأمنها، فقد تتعدد أشكال هذه الجريمة فمنها ما تقع على الاشخاص وتهدد سلامتهم والاخرى تمس بأموالهم وشرفهم واعتبارهم فتهدد بذلك حياتهم الخاصة، واخرى تهدد اقتصاد الدول وأمنها

تصدت الجريمة السيبيرانية عدة تشريعات في قوانينها حيث جرمت أفعالا تدخل في نطاق النظام المعلوماتي توصف بالتعدي، فالمشرع الجزائري مثلا جرمها تحت عنوان المساس بنظام المعالجة الالية للمعطيات وخصص لها باب كاملا وهذا للحد من الجريمة السيبرانية (المبحث الأول).

لم يستقر الفقهاء على معيار واحد لتقسيم الجريمة الالكترونية، وذلك لتشعب هذه الجرائم وسرعة تطورها، فمنهم من يصنفها بالرجوع إلى وسيلة ارتكاب الجريمة أو دافع المجرم، أو على أساس محل الجريمة، وهناك من قسمها الى جرائم واقعة على الاموال وأخرى على الاشخاص وهادفة الى المساس بأمن الدول.(المبحث الثاني)

المبحث الأول

ماهية الامن السيبراني

يعتبر الفضاء السيبراني منبرا هاما تطل من خلاله الجماعات الإرهابية سواء لإدارة عمليات في أماكن مختلفة، أو من أجل الترويع والتحريض والحشد وبث ثقافة أو فكر إيديولوجي معين، ونلاحظ أن الوجود الإرهابي على شبكة الإنترنت ككل أصبح يشكل خطرا على الاستخدام السلبي لوسائل الاتصال، مما استوجب على الدول اللجوء الى منظومة الأمن ووضع استراتيجية أمنية شاملة من أجل ضمان "**الأمن السيبراني**" لأن أمن المعلومات يدخل ضمن الأمن الوطني الشامل.

تعدّ الجرائم السيبرانية من الجرائم المستحدثة، واتجهت الدول إلى ذكر عدة أنواع منها، نظرًا لخطورتها وتأثيرها الكبير على الواقع العملي وحياة الافراد الخاصة، حيث تفاقمت الاعتداءات على المعطيات الآلية خاصة مع ضعف الحماية الفنية، و نتيجة للتطور الحاصل في الوسائل الالكترونية مما يستلزم معرفة مدلولها (مطلب اول).

وأمام هذه الوضعية استدعى تدخلا تشريعيا صريحا؛ حيث كفل المشرع الجزائري حماية قانونية لمعطيات الحاسب الالي من خلال تجريم افعال في قانون العقوبات واستحداث نظم قانونية جديدة سعيا منه لمواجهة التحديات التكنولوجية المعاصرة وتدارك الفراغ التشريعي الحاصل نظرا لعدم مواكبة هذه الجرائم للتشريعات التقليدية (مطلب ثان).

المطلب الأول

مدلول الأمن السيبراني والجريمة السيبرانية

الأمن السيبراني ليس مجرد مجموعة من المبادئ التوجيهية والإجراءات التي تهدف إلى منع الجريمة السيبرانية. بل هو في النهاية حماية للحكومة وشبكات الشركات من الاختراقات والهجمات السيبرانية التي تتعرض لها؛ ويسعى إلى جعل المتسللين يجدون صعوبة في العثور على نقاط الضعف واستغلالها، لهذا نحاول اعطاء مفهوم للأمن السيبراني (الفرع الاول).

إن الإجرام السيبراني هو أحد النتائج السلبية التي خلفها التطور التكنولوجي لوسائل الاتصال، وقد أخذت هذه الظاهرة الإجرامية التي فرضت نفسها على المجتمع حيزا كبيرا من الدراسات القانونية من أجل تحديد مفهومها.(الفرع الثاني)

الفرع الأول

تعريفات الأمن السيبراني

يقصد بالأمن السيبراني حماية الأشياء من خلال تكنولوجيا المعلومات مثل الأجهزة والبرمجيات وذلك اختصارا لمصطلح ICT[1]

يقسم الأمن السيبراني لغويا إلى لفظتين "الأمن" و "السيبراني"

الأمن: هو نقيض الخوف أي بمعنى السلامة، والأمن مصدر الفعل أمن أي إطمئنان النفس[2]

السيبراني: وهي مأخوذة من كلمة (سيبر) وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي، فالسيبرانية تعني (فضاء الأنترنت)، وهي كلمة مشتقة

[1] information and communication technologies"

[2] ايهاب خليفة، الأمن السيبراني الماهية والإشكاليات، مركز مستقبل الأبحاث والدراسات المتقدمة، أبو ظبي، ص14.

من الكلمة اليونانية التي وردت بداية في مؤلفات الخيال العلمي، وكان يقصد بها قيادة ربان السفينة.[1]

الأمن السيبراني اصطلاحا: هناك العديد من التعاريفات التي قدمت لمفهوم الأمن السيبراني، حيث يعرف بأنه مجوعة من الإجراءات المتخذة في مجال الدفاع ضد الهجمات السيبرانية ونتائجها التي تشمل تدابير المضادة المطلوبة.[2]

بينما عرفه "ادوارد امورسو" على انه: "وسائل من شانها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل والأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفه..."

يعرف "ريتشاد كمرر" الأمن السيبراني بأنه "عبارة عن وسائل دفاعية من شانها كشف وإحباط المحاولات التي يقوم بها القراصنة "[3]

بالنسبة للاكاديميين، يعرف كل من Martti Lehto,Pekka Neittaanmäkiالامن السيبراني على أنه "مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكمبيوتر تنفيذ التدابير المضادة المطلوبة"[4]

أما المعهد الوطني للمعايير والتقنية الأمريكي عرف الأمن السيبراني بأنه "الحماية من الأضرار واستعادة أنظمة الحاسب وأنظمة الاتصالات الالكترونية وخدمات الاتصالات الالكترونية والاتصالات السلكية بما في ذلك المعلومات الواردة فيها لضمان توافرها وسلامتها والمصادقة والسرية وعدم الانتهاك.

---

[1] سليمان قطاف، عبد الحليم بوقرين، مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية، جامعة عمار ثليجي، الاغواط، مج 5، ع4،2022، ص 62.

[2] إيهاب خليفة، مرجع سابق،ص4

[3] لامية طالة، التهديدات والجرائم السيبرانية وتأثيرها على الأمن القومي للدول و استراتيجيات مكافحتها، مجلة معالم للدراسات القانونية و السياسية،مجلد4،عدد 01،2020،ص60

[4] Martti Lehto,Pekka Neittaanmäki, "Cyber Security: Analytics, Technology and Automation, edition springer (USA), 30.05.2015

كما عرفت هيئة الاتصالات و تقنية المعلومات الأمن السيبراني بأنه: "هو حماية الشبكات و أنظمة تقنية المعلومات و أنظمة التقنيات التشغيلية و مكوناتها من أجهزة وبرمجيات و ما تقدمه من خدمات، وما تحتويه من بيانات من لأي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع".

من خلال ما ورد من تعريفات يمكن القول بالأمن السيبراني هو عبارة عن مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرار عمل نظم المعلومات وتعزيز حماية سرية البيانات الشخصية وخصوصيته[1]

الفرع الثاني

مدلول الجريمة السيبرانية

نجد أن العديد من الأعمال الأكاديمية حاولت وضع تعريف للجريمة المرتكبة عبر الأنترنت، حيث اختلف الفقهاء في وضع تعريف لها اذ هناك من يعرفها تبعا لوسيلة ارتكاب الجريمة(أولا)، او على اساس موضوع الجريمة(ثانيا)،او مدى معرفة المجرم بالتقنيات الحديثة للحاسوب(ثالثا).

أولا: تعريفها على أساس وسيلة ارتكاب الجريمة

اختلف الباحثون حول وضع تعريف موحد للجرائم السيبرانية؛ فمنهم من ينظر إلى موضوع الجريمة و منهم من ينظر الى الوسيلة المستعملة لارتكابها [2]،و تبدو الحقيقة أنه من الصعوبة بمكان وضع تعريف لهذه الظاهرة الإجرامية و ذلك خشية حصرها في مجال ضيق في ظل التطور المعلوماتي الحاصل على مستوى العالم[3] و تعرف بأنها:

---

[1] HTTPS.//atta.sa-libray.19.58 - ساعة الدخول

[2] مهدي رضا: الجرائم السيبرانية واليات مكافحتها في التشريع الجزائري، مجلة ايليزا للبحوث والدراسات، مجلد06،العدد02، 2021،ص113

[3] محمد علي العريان، الجرائم المعلوماتية، كلية الحقوق ،دار الجامعة الجديدة، الإسكندرية، د.ط، 2011،ص 54

تعتمد هذه التعريفات على وسيلة ارتكاب الجريمة وهو الحاسوب أو إحدى الوسائل التقنية الحديثة المرتبطة به فتعتبر من جرائم الانترنت، ومن ذلك تعريف مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها: "الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا"[1]

حيث عرفها بعض الفقه بأنها: "جرائم الانترنت تعني جرائم الشبكة العالمية التي يستخدم الحاسب وشبكاته العالمية كوسيلة مساعدة لارتكاب جريمة مثل استخدامه في النصب والاحتيال وغسل الأموال وتشويه السمعة والسب" [2]

عرفها الفقيه تايدمان:"كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب بأستخدام الحاسب الآلي"[3].

ثانيا: على أساس موضوع الجريمة

حيث ذهب فريق آخر من الفقه إلى تعريف الجريمة السيبرانية استنادا لموضوعها وبالتالي فهي: "الجرائم التي ترتكب ضد الأنظمة الالكترونية والشبكات المعلوماتية" بعبارة أخرى "هي نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الالكتروني أو التي تحول عن طريقه"[4]

عرفها اتجاه آخر بأنها: "الجريمة المرتكبة عبر الانترنت هي الجريمة الناتجة عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام المحركات إضافة إلى أفعال أخر يتشكل جرائم أكثر تعقيدا من الناحية التقنية مثل تعديل الكمبيوتر"

---

[1] سامى على حامد عياد، الجريمة المعلوماتية واجرام الانترنت، دار الفكر الجامعي، الاسكندرية، د.ط،2007، ص38

[2]مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، ط 1، مطابع الشرطة، القاهرة، 2009، ،ص 112.

[3]وردة لقديم: الجريمة الالكترونية في التشريع الجزائري، مذكرة مكملة من مقتضيات نيل شهادة الماستر في الحقوق، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف، 2017،ص 7.

[4]ذبيح عماد، سمية بهلول، الآليات العقابية لمكافحة الجريمة الالكترونية في التشريع الجزائري ،مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، عدد 13، 2020،ص140.

ثالثا: على أساس مستوى معرفة المجرم بالتقنيات الحديثة للحاسوب

تعتمد هذه التعاريف على أساس توافر المعرفة الفنية بتقنية المعلومات لدى الجاني في الجريمة الالكترونية، حيث عرفها الأستاذ دافيد طومسون بأنها "أية جريمة يكون متطلبا لاقترافها أن يتوافر لدى فاعلها معرفة بتقنية الحاسب"

اعتمد هذا الاتجاه في تعريفه للجريمة الالكترونية على معيار شخصي وهو مدى معرفة الجاني بتقنية المعلومات والإلمام بها، وحيث أن قصور هذه التعاريف واضحة لأن شخصية الجاني لا تكفي لوحدها لتعريف الجريمة الالكترونية حيث يمكن لشخص عادي غير مؤهل بتقنيات الحاسب الآلي ارتكاب جريمة الغش المعلوماتي أو السرقة المعلوماتية[1]

المطلب الثاني

موقف المشرع الجزائري من الجريمة السيبرانية

تدارك المشرع الجزائري مؤخرا ولو نسبيا الفراغ القانوني في مجال الجرائم المعلوماتية وذلك باستحداث نصوص تجريمية لقمع الاعتداءات الواردة على المعلوماتية بموجب القانون رقم: 04 ـ 15 مؤرخ في: 10 نوفمبر سنة 2004 المتضمن تعديل قانون العقوبات[2] و ذلك في القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات حيث نصت المواد 394 مكرر، و399 مكرر 1، 394 مكرر2، 394 مكرر 3، والمادة 394 مكرر4، والمادة 394 مكرر 5، والمادة 394 مكرر 6، والمادة 394 مكرر7 [3]

---

[1] رحيمة نمديلي، الطبيعة القانونية للجريمة السيبرانية في القانون الجزائري والقوانين المقارنة, كلية الحقوق والعلوم السياسية جامعة سطيف 2، ص ص06،07

[2] قانون رقم 04 ـ 15 مؤرخ في 10 نوفمبر سنة 2004 المعدل و المتمم للأمر رقم 66 ـ 156 مؤرخ في 8 يونيو سنة 1966 المتضمن قانون العقوبات (ج. ر. ج. ج ع 71)

[3] رحيمة نمديلي، مرجع سابق، ص 13

وصدر القانون رقم 09-04 مؤرخ في 5 غشت سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[1]، و عليه سوف أتناول نظام المعالجة الالية للمعطيات في (الفرع الأول), والجرائم المتصلة بتكنولوجيا الاعلام و الاتصال في (الفرع الثاني)

الفرع الأول

نظام المعالجة الالية للمعطيات في قانون العقوبات

المشرع الجزائري على غرار المشرع الفرنسي لم يعرف نظام المعالجة الالية للمعطيات بل تركه للفقه وحسنا ما عمله المشرع بعدم تعريفه له وذلك نظرا للتطورات الحاصلة في التكنولوجيا، وقد قدمت الاتفاقية الدولية للإجرام المعلوماتي تعريفا للنظام المعلوماتي في مادتها الثانية[2]:

Système informatique désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données[3]

بالإضافة الى تعريف مجلس الامة الفرنسي بأنه:" هو كل مجموعة مؤلفة من وحدة أو عدة وحدات لمعالجة المعلومات أو اختزانها أو إعداد البرامج والمعطيات وكل ما يؤدي إلى إدخال واسترجاع المعلومات"[4]. و استنادا على ما سبق سوف اتطرق الى الأفعال المجرمة من قبل المشرع في قانون العقوبات وهي كالتالي:

أولا: جريمة الدخول أو البقاء الغير المصرح به داخل نظام معلوماتي:

حيث نص عليها المشرع في المادة 394 مكرر من ق.ع.ج " **كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.**

---

[1] منال لبيض, الحماية الجزائية و المدنية من الجريمة المعلوماتية في التشريع الجزائري ,مذكرة لنيل شهادة الماستر, قانون أعمال, كلية الحقوق و العلوم السياسية, جامعة سطيف, 2015, ص 14

[2] أمال قارة: الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، 2006، ص101

[3] الاتفاقية الدولية حول الاجرام المعلوماتي المصادق عليها بتاريخ:2001/11/08 من طرف المجلس الأوروبي.

[4] رامي حليم، القانون الجنائي و التكنولوجيا الحديثة، محاضرات موجهة لطلبة الدكتوراه، ص08

وتضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة أو ترتب عن الأفعال المذكورة تخريب نظام اشتغال المنظومة".

وهو الركن المادي لجريمة الاعتداء على نظام المعالجة الالية للمعطيات. و يتمثل في الولوج الى النظام المعلوماتي الغير المفتوح للجمهور ضد رغبة المسؤول عن هذا النظام, و يقصد بفعل الدخول أي الدخول المعنوي للنظام باستعمال الوسائل الفنية و التقنية, و لا يشترط ان تكون هناك صفة للجاني لكي تقوم الجريمة بل تقوم مهما كانت صفة الانسان[1]

ونلاحظ ان المشرع قد جرم حتى مجرد الدخول للنظام المعلوماتي بأكمله او جزء منه فقط لكن اشترط ان يكون مقصودا وبدون ترخيص أي لا يكون عن طريق الخطأ او الصدفة اما فعل البقاء الغير المصرح به داخل نظام معلوماتي فقد يعني استمرارية التواجد داخل النظام دون اذن صاحبه رغم علمه بأن البقاء فيه غير مشروع و سواء كان بالصدفة او عن طريق الخطأ،[2] فاذا تم الدخول صدفة أو عن طريق الخطأ يجب أن يقتطع وجوده داخل النظام و الانسحاب منه، و اذا بقي فيعاقب على جريمة البقاء الغير المشروع داخل النظام[3].

و قد أورد المشرع الجزائري ظروف التشديد في هاتين الجريمتين، فاذا نتج عن الدخول أو البقاء محو أو تعديل في البيانات التي يحتويها النظام تشدد العقوبة، و أذا ترتب عن ذلك تخريب نظام اشتغال المنظومة و اعاقته عن أداء وظيفته يتحقق الظرف الثاني، كما عاقب على الشروع وهذا من خلال قوله" او يحاول"[4]

غير ان المشرع الفرنسي عاقب على جريمة الدخول او البقاء الغير المشروع داخل النظام المعلوماتي بنص المادة 1/323 من قانون العقوبات الفرنسي المعدل في سنة 1994

---

[1] رجاء أمدور: خصوصية التحقيق في مواجهة الجريمة المعلوماتية، أطروحة لنيل شهادة دكتوراه، قانون خاص، كلية الحقوق والعلوم السياسية، جامعة البشير الابراهيمي، برج بوعريريج، 2020، ص22

[2] عبد الرؤوف زيوش، الجريمة المعلوماتية في التشريع الجزائري، مجلة العلوم القانونية و الاجتماعية، جامعة. زيان عاشور الجلفة، عدد03، 2019، ص134

[3] **انظر** حمزة بن عقون، السلوك الاجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجيستير في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة باتنة، 2011، ص184

[4] المادة 394 مكرر من القانون 15/04 المتضمن قانون العقوبات الجزائري

حيث تمثلت العقوبة في الحبس لمدة سنة و غرامة لا تزيد عن 15 الف يورو، أما اذا وقع تعديل او اتلاف للبرامج فتشدد العقوبة لتصل الى سنتين حبس وغرامة تصل الى 30 ألف يورو.[1]

ثانيا: جريمة التلاعب في معطيات النظام المعلوماتي:

لقد جرم المشرع الجزائري أي اعتداء يقع على المعطيات الداخلية لنظام المعالجة حيث نصت المادة 394 مكرر1 من قانون العقوبات الجزائري على:" **يعاقب بالحبس من 6 أشهر الى 3 سنوات و بغرامة من 500.000 دج الى 2.000.000 دج، كل من ادخل بطريق الغش معطيات في نظام المعالجة الالية او أزال او عدل بطريق الغش المعطيات التي يتضمنها**"[2]

ثالثا: جريمة الاعتداء العمدي على المعطيات الداخلية للنظام المعلوماتي

و تكون الجريمة قائمة بفعل الادخال و الذي يعني إضافة معطيات جديدة في نظام المعالجة تكون غير صحيحة او خيالية و يتحقق كذلك عند ادخال برامج الفيروسات ، أو بفعل المحو و يقصد به إزالة معطيات مسجلة على دعامة موجودة داخل نظام المعالجة الالية أو تحطيمها أو نقل جزء من المنطقة الخاصة بالذاكرة، أما التعديل فنعني به تغيير المعطيات و استبدالها بأخرى.[3]

و نلاحظ أن المشرع الجزائري قد حصر في هذه المادة صور الاعتداء على المعطيات الداخلية في الادخال و المحو و التعديل، و هذا يعني ان أي اعتداء يقع خارج نطاق هذه الصور يكون مستبعدا، و كذلك نجده انه لم يشترط اجتماع هذه الصور لقيام الجريمة بل تكفي وقوع واحدة منهم.[4]

---

[1] سعاد عاطف عبد المطلب حسنين، الحماية الجنائية للمصنفات الرقمية، ط.1،دار الفكر الجامعي، 2018.ص 320،321

[2] رجاء أمدور، مرجع سابق، ص 22

[3] رزيقة بونار ،الجريمة المعلوماتية في التشريع الجنائي الجزائري ،مذكرة لنيل شهادة الماستر ،قانون عام ، كلية الحقوق والعلوم السياسية ،قسم الحقوق، جامعة بن يحي محمد الصديق ،جيجل ،2020،ص25

[4] عبد الرؤوف زيوش ،مرجع سابق ،ص135

وقد يتحقق ايضا بإدخال بيانات ومعلومات وهمية بقصد التشويش على صحة البيانات او عن طريق التدخل في الكيان المنطقي للكمبيوتر مثلا القيام يتعديل البرنامج او خلق برامج جديدة.[1]

رابعا: جريمة الاعتداء على المعطيات الخارجية للنظام المعلومات

جرمت المادة 394 مكرر2 مجموعة من السلوكات حيث نصت على ما يلي:" يعاقب بالحبس من شهرين الى 3 سنوات و بغرامة من 1000.00 دج الى 5000.000 دج كل من يقوم عمدا و بطريق الغش ب:

_تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة او معالجة او مرسلة عن طريق منظومة معلوماتية يمكن ان ترتكب بها الجرائم المنصوص عليها في هذا القسم

_حيازة او افشاء او نشر او استعمال لأي غرض كان المعطيات المتحصل عليها من احدى الجرائم المنصوص عليها في هدا القسم"

أي أن محل الجريمة هنا هو المعطيات المخزنة أو المرسلة عن طريق منظومة معلوماتية أي الصالحة لارتكاب الجريمة بدءا من تصميمها و بحثها و تجميعها وصولا الى توفيرها و الاتجار بها وهذا ما اقرته الفقرة الأولى من المادة، ليس هذا فقط بل جرم في الفقرة الثانية التعامل في معلومات متحصل عليها و هنا يتحقق الركن المادي فيها بالحيازة أو الافشاء او النشر أو الاستعمال[2].

---

[1] محمد أمين الشوابكة، جرائم الحاسوب والانترنت (الجريمة المعلوماتية)، د.ط، دار الثقافة والنشر والتوزيع،2001، ص ص 235،237

[2] عزيزة رابحي ،الاسرار المعلوماتية و حمايتها الجزائية ،مذكرة لنيل شهادة الدكتوراه، تخصص قانون خاص ،كلية الحقوق والعلوم السياسية، جامعة ابو بكر بلقايد،تلمسان،2017،ص170

خامسا: القواعد المشتركة بين هذه الجرائم

_ **تشديد العقوبة**: حيث نصت المادة 394 مكرر 3 على ان تتضاعف العقوبات المقررة للجرائم المذكورة في هذا القسم اذا استهدفت الدفاع الوطني او الهيئات و المؤسسات الخاضعة للقانون العام ، دون الاخلال بتطبيق عقوبات اشد[1]

_**عقوبة الشخص المعنوي**: حيث اقرت المادة 394 مكرر4 انه اذا ارتكب هذه الجرائم يعاقب بغرامة تعادل 5 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.[2]

الاشتراك و الاتفاق الجنائي: نصت المادة 394 مكرر5 على أن كل من شارك في مجموعة او في اتفاق تألف بغرض الاعداد لجريمة او اكثر من الجرائم المنصوص عليها في هذا القسم و كان التحضير مجسدا بفعل او عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها[3]

العقوبات التكميلية: اقرت المادة 394 مكرر6 الحكم بمصادرة الأجهزة والبرامج والوسائل المستعملة في الجريمة واغلاق الموقع محل الجريمة خاصة اذا كانت بعلم مالكها.[4]

الشروع: نصت عليه المادة 394 مكرر7 وعاقب المشرع على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبة المقررة للجنحة ذاتها.[5]

---

[1] المادة 394مكرر3 من قانون العقوبات الجزائري..

[2] المادة 394مكرر4 من قانون العقوبات الجزائري.

[3] المادة394مكرر5 من قانون العقوبات الجزائري.

[4] المادة 394مكرر6 من قانون العقوبات الجزائري.

[5] رزيقة بونار، مرجع سابق ،ص39

فالشروع في الجريمة المعلوماتية هو إتيان أي عرقلة مادية مثل الدخول للقاعة بهدف ارتكاب الجريمة يعد شروعا و من الاعمال التحضيرية وشدد عقوبتها وذلك خشية استعمال النظام المعلوماتي كوسيلة لارتكاب الجريمة وتسهيلها.

الفرع الثاني:

الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال

لقد اصدر المشرع الجزائري قانون رقم 04/09 مؤرخ في 05 غشت 2009 و المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتهما، و الجدير بالذكر أن المشرع قد وسع من مفهوم الجرائم المعلوماتية بمقتضى هذا القانون حيث اعتبر أي جريمة ترتكب أو تسهل ارتكابها بواسطة منظومة معلوماتية أو نظام الاتصالات الالكترونية بالإضافة الى جرائم المساس بالأنظمة الالية للمعطيات المحددة في قانون العقوبات الجزائري تدخل في نطاق الجريمة المعلوماتية، و عليه نستنتج ان المشرع قد وسع من دائرة التجريم بإصداره لهذا القانون.[1]

المبحث الثاني:

صور عن جرائم اختراق الامن السيبراني

تستهدف الجرائم المرتكبة عبر الانترنت الكثير من القطاعات؛ مما جعل تصنيفها صعبا عكس الجرائم التقليدية التي يسهل تصنيفها وذلك بسبب الاختلاف في تسميتها، حيث استند كل اتجاه على معيار معين، وتجدر الإشارة أن تحليل صور الجريمة السيبرانية وبيان أصنافها ليس بالأمر البسيط.

حيث صاحب ظهور شبكة الإنترنت تطورات كبيرة في شتى المجالات، فقد أصبحت معظم المعاملات التجارية تتم من خلال هذه الشبكة، مثل البيع والشراء، مما إنجر عنه

[1] نبيلة هبة هروال .جرائم الانترنت، دراسة مقارنة، اطروحة لنيل شهادة الدكتوراه.، كلية الحقوق والعلوم السياسية. جامعة ابي بكر بلقايد، تلمسان.2013.ص73

تطور وسائل الدفع والوفاء وأضحت جزء لا يتجزأ من هذه المعاملات، وفي خضم هذا التداول المالي عبر الإنترنت انتهز بعض المجرمين من أجل السطو عليها بالإضافة إلى ذلك فإن المعلومات المتعلقة بالأفراد متداولة بكثرة عبرها، مما يجعلها عرضة للانتهاك والاستعمال من طرف هؤلاء المجرمين، وجعلت سمعة وشرف الأفراد مستباحة تماما (المطلب الاول).

أتاحت الإنترنت للكثير من الدول ممارسة التجسس على دول أخرى، وذلك بالاطلاع على مختلف الأسرار العسكرية والاقتصادية لهذه الأخيرة، خاصة فيما يتعلق بالدول التي يكون بينها نزاعات، ويبقى المساس بالأمن الفكري من بين أخطر الجرائم المرتكبة عبر الإنترنت، حيث تعطي الإنترنت فرصا للتأثير على معتقدات وتقاليد مجتمعات بأكملها مما يسهل خلق الفوضى، حيث توالت عبر الإنترنت الهجمات الثقافية، والحضارية التي قد تزعزع الأمن الفكري والعقدي للشعوب المغلوبة على أمرها، وتنشر عبرها القوى الغالبة فكرها، ولغتها، وقيمها، وقد ظهر في أدبيات بعض الباحثين مذ بدايات شبكة الإنترنت إشارات التحذير من الغزو الفكري المركز الذي يستقبله الجيل العربي.(المطلب الثاني) .

المطلب الأول:

الجرائم الواقعة على الأشخاص والأموال

تعتبر الغاية الأولى و الأسمى من وضع التشريعات و سن القوانين هي حماية سلامة الأشخاص وحياتهم وأموالهم وممتلكاتهم، فمع التطور السريع للأنترنت أصبحت سلاحا فتاكا في يد المجرمين؛ حيث يستخدم المجرمون أسلوب القذف والسب وتشويه السمعة وغيرها من الأفعال اللاأخلاقية، بغرض المساس بشرف الشخص أو النيل من كرامته (فرع اول) و كذلك من المعلوم أنه باتت الكثير من المعاملات المالية في وقتنا الحاضر تتم بواسطة الشبكات الإلكترونية، مما زاد من تطور وسائل الدفع الإلكتروني، الأمر الذي أدى إلى تطور الجريمة الإلكترونية بغاية الحصول على الأموال بأقل تكلفة ممكنة(فرع ثان).

الفرع الأول:

الجرائم الواقعة على الأشخاص

يقصد بجرائم الاعتداء على الأشخاص بصفة عامة:" تلك الجرائم التي تنال بالاعتداء او التهديد بالخطر حقوقا ذات طابع شخصي بحت"، أو هي:" مجموعة من الجرائم التي تقع اعتداء على الجوانب الشخصية و الإنسانية، فهي تستهدف المساس بحياة الشخص او سلامته البدنية أو عرضه" وعليه يتم التطرق الى الجرائم الماسة بالشرف و الاعتبار الواقعة عن طريق الانترنت (اولا)، ثم الجرائم التي تمس بالشرف الواقعة على القصر عبر الانترنت (ثانيا).

أولا: الجرائم الماسة بالشرف و الاعتبار الواقعة عن طريق الانترنت

سوف اتطرق الى جريمة القذف و السب و التشهير عبر الانترنت و أبين اركان و أساليب ارتكاب كل جريمة على حدى.

1-جريمة القذف عبر الانترنت:

لقد وردت جريمة القذف في م 296من ق .ع.ج في الفقرة 1 "كل ادعاء بواقعة من شانها المساس بشرف او الاعتبار الأشخاص او الهيئات المدعي عليها بها او استنادها اليهم او تلك الهيئة ..." وحدد المشرع الجزائري في الفقرة 2 من نفس المادة وسائل التي ترتكب بواسطتها مثل التهديد أو الصياح او الكتابة او المنشورات او اللافتات و يفهم من هذا النص المشرع ان المشرع لم ينص صراحة ان الانترنت تعتبر كوسيلة لارتكاب جريمة القذف[1]

غير انه بالرجوع الى المادة 144 مكرر ق.ع فقد نصت صراحة على القذف الموجه لرئيس الجمهورية او الهيئات العمومية بانه صورة او وسيلة معلوماتية اخرى.[2]

اما بالنسبة لطرق او وسائل ارتكابها فان المشرع من خلال نص م 296 من ق.ع قد اشترط توافر صفة العلانية، وقد تقوم ب ثلاث اساليب:

---

[1] نبيلة هبة هروال ،مرجع سابق ،ص73

[2] نسيم دردور، الجرائم المعلوماتية على ضوء القانون الجزائري و المقارن ،مذكرة من مقتضيات نيل شهادة الماجيستير، كلية الحقوق والعلوم السياسية، جامعة منتوري ، قسنطينة ،2012، ص ص110،111

*العلانية عن طريق القول أو الترديد او الصياح : ويتحقق في الاماكن العمومية كالحافلة او الطرق العامة و بالتالي تتحقق العلانية في الانترنت عن طريق غرف الدردشة و المجموعات الاخبارية التي تقوم على الصوت و الصورة.

*العلانية بطرق الكتابة او المنشورات او اللافتات: وهنا تقوم على توزيع المنشورات على الجمهور دون تمييز او وضعها في مكان يمكن الجميع من رؤيتها.[1]

*العلانية بوسائل اخرى: ومثالها اذا تمت بواسطة الية لبث الصوت او الصورة او اي وسيلة الكترونية.

وعاقب عليها المشرع الجزائري بنص المادة 1/289 من ق.ع بالحبس من 5 أيام الى 6 أشهر وبغرامة من 5000دج الى 50.000دج وهذا فيما يخص القذف الموجه ضد الأفراد العاديين

أما القذف الموجه لرئيس الجمهورية فيعاقب عليه بالحبس من 3 اشهر الى 12 شهر و غرامة من 50.000دج الى 250.000دج أو احدى هاتين العقوبتين و هذا عملا بنص المادة 144 مكرر[2]

و المادة 144 مكرر2 نصت على الحبس من 3سنوات الى 5 سنوات و بغرامة من 50.000دج الى 100.000 دج او بإحدى هاتين العقوبتين كل من اساء الى الرسول او بقية الانبياء او استهزأ بالمعلوم من الدين بالضرورة او بأية شعيرة من شعائر الاسلام سواء عن طريق الكتابة او الرسم او التصريح او اية وسيلة اخرى.[3]

2- جريمة السب عبر الانترنت:

اما المشرع الجزائري عرفها في المادة 297 ق.ع والتي نصت على مايلي:"يعد سبا كل تعبير مشين او عبارة تتضمن تحفيزا او قدحا ينطوي على اسناد اية واقعة"[4]

---

[1] نبيلة هبة هروال، مرجع سابق، ص 88

[2] المادة 144 مكرر من الامر 156/66 المتضمن قانون العقوبات الجزائري.

[3] المادة 144 مكرر 2 من الامر 156/66 المتضمن قانون العقوبات الجزائري

[4] المادة 297 من الامر 156/66 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات الجزائري المعدل والمتمم (ج.ر.ع 49).

اما الوسائل التي ترتكب بها فهي نفسها السالفة الذكر في جريمة القذف، وتجدر الاشارة الى ان المشرع قد فرق بين السب الواقع على الافراد والواقع على رئيس الجمهورية و الماس بشعائر الاسلام و رموز الدين و الانبياء حيث نصت المادة 299 من ق.ع على الحبس من 6 ايام الى 3 اشهر مع نفس الغرامة الموقعة على جريمة القذف في حالة السب الماس بالأفراد العاديين ،اما اذا كانت تمس بالرئيس الجمهورية و اشخاص ينتمون الى مجموعات عرفية فتشدد العقوبة و تبقى نفس عقوبة القذف و هذا بنص المادة 144 مكرر من ق.ع.[1]

و قد شدد المشرع العقوبة اذا كان السب موجها لرموز الدين لتصل العقوبة الى الحبس من 3 سنوات الى 5 سنوات و غرامة من 50.000دج الى 100.000دج

3- جريمة التشهير الالكتروني عن طريق الابتزاز و تشويه السمعة

في غالب الاحيان يلجأ ذوي النوايا السيئة الى وسائل من شانها المساس بحرمة الشخص و الاعتداء على شرفه و حريته من بينها التشهير و الذي يهدف للكشف على اسرار على خبايا حياة شخص ما دون رضاه. و تجدر بنا الاشارة الى ان التشهير قد يترافق مع الابتزاز الالكتروني خاصة عبر وسائل التواصل الاجتماعي اما بنشر الصور او فيديوهات بهدف الحصول على المال من الضحية او بهدف اجباره على القيام بأفعال

تمس بشرفه و سمعته،[2]وهذا يعد امرا محظورا في نظر المشرع الجزائري مما تصدى له بنص المادة 303 مكرر من قانون العقوبات: "يعاقب بالحبس من 6 اشهر الى 3سنوات و بغرامة من 50.000 دج الى 300.000 دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت"[3]

و قد تتلخص وقائع قضية وقعت في الجزائر العاصمة في عام 2017 و التي راح ضحيتها المدعوة "رانيا" "من قبل المتهم "باهي" حيث ان هذا الاخير قد ارسل اليها طلب صداقة عبر الفاسبوك وتم قبولها من طرف الضحية وتطورت العلاقة بينهما حيث اوهمها

---

[1] نبيلة هبة هروال، مرجع سابق، ص 89.

[2]https:// www.legal-advice.online

[3]انظر المادة 303مكرر من قانون العقوبات الجزائري

بنيته الحسنة اتجاهها، و مع مرور الزمن اصبح يطلب منها ارسال صورها الشخصية بحجة انه سوف يتقدم لخطبتها و لكنه راح يخطط لنهب اموالها حيث ابتزها و ارغمها على اعطاءه مبلغا ماليا مقابل عدم التشهير بها.[1]

4- جريمة المضايقة و المطاردة الالكترونية

عرفت جريمة المضايقة والترصد الالكتروني بأنها السلوك الذي يوجه الى شخص عبر استخدام وسائل تقنية المعلومات الحديثة بغية ازعاجه او تهديده او الضغط عليه[2]

يجب ان ننوه ان هذه الجريمة غالبا ما ترتكب بواسطة البريد الالكتروني او وسائل حوارات اخرى على الشبكة، حيث تتضمن وسائل مضايقة و تخويف للمجني عليه بهدف السيطرة عليه و التحكم فيه و هذه الجريمة لا تتطلب وجود اتصال مادي بين المجرم و الضحية و هذا لا يفسر انها لا تشكل خطورة كغيرها من الجرائم بل ان قدرة الجاني على اخفاء هويته تشجعه على التمادي اكثر مما قد تفضي به الى سلوكات عنف مادية، ولا يفوتنا القول بأن جريمة المضايقة هدف الجاني من ورائها خلق التذمر و الخوف في نفس المجني عليه مما يسوقه للخضوع لطلباته.[3]

ثانيا: الجرائم التي تمس بالشرف الواقعة على القصر عبر الانترنت

وهنا سوف اتناول في هذا المضمون جريمة تحريض قاصر على الفسق و الدعارة عبر الشبكة و كذلك جريمة نشر رسائل الكترونية مخلة بالأخلاق الحميدة عبر الانترنت .

1-جريمة تحريض قاصر على الفسق و الدعارة عبر شبكة الانترنت:

لقد نص المشرع الجزائري عليها في الفصل الثاني من قانون العقوبات الجزائري في الباب الثاني تحت عنوان الجنايات و الجنح ضد الاسرة و الآداب العامة في القسم السابع المعنون ب"تحريض القصر على الفسق و الدعارة"، حيث نصت المادة 342 من هذا القانون

---

[1] القناة الاعلامية الشروق حصة "الشروق تحقق"2017 ساعة الدخول00.30

[2] علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، دراسة مقارنة، دار النشر والتوزيع، منشورات زين الحقوقية، 2013.ص 277.

[3] ناصر وقاص، سفيان بخدة، الطبيعة القانونية للجرائم المستحدثة و وسائل ارتكابها ،مجلة البحوث القانونية و السياسية، جامعة مولاي الطاهر سعيدة، مج3، ع16، 2021، ص ص136،135

على تحريض صغار السن على ممارسة الفسق و اعتبرها جريمة قائمة بذاتها فالفسق فهو كل سلوك جنسي مخالف للآداب العامة [1]

و لقيام هذه الجريمة يشترط توافر ركن مادي و المتمثل في وقوع فعل مادي من المتهم بالقول او بالفعل او التشجيع على ذلك او تسهيل ارتكابها او اي وسيلة اخرى، و هنا يفهم ان المشرع لم ينص صراحة على ارتكابها عن طريق الوسائل التقنية كالشبكة العنكبوتية و اشترط كذلك صغر السن اي يجب ان تقع على القصر الذين لم يكملوا 18 سنة [2]

أما المادة 343 من قانون العقوبات تضمنت ونصت على التحريض على الدعارة و يقصد بها دفع المجني عليه ألا و هو القاصر الى ارتكاب الرذيلة لدى الغير و اعتبرها جريمة قائمة بذاتها حتى لو لم تتحقق النتيجة و هي وقوع الدعارة، و يكون بالقول الذي يأتي عن طريق الاغراء او الهدية او وعد او مخادعة أو عن طريق التحريض بالفعل و الذي يتحقق اذا صدر عن الجاني اشارات تحمل دلالة مثلا على مسكن الدعارة او الاشارة الى المصاحبة...

غير ان هذه المادة عددت صور التحريض على الدعارة مثل الاستدراج او التغرير او المساعدة او المعاونة او العيش مع محترف دعارة او اعالة قاصر في ممارسة الدعارة او اغوائه على امتهانها و عاقبت بالحبس من سنتين الى خمس سنوات.[3]

و في هذا الصدد طرحت قضية في المحكمة العليا و تعود حيثياتها الى ان فتاة لم تكمل 17 سنة تم الاعتداء على عرضها من طرف حمى امها حيث ادى الى فض بكارتها نتيجة علاقة غرامية بكامل رضاها حيث نتج عنها طفل قامت بولادته وقتلته عمدا، هذا ان الجريمة كيفت على انها تحريض قاصر على الفسق و الدعارة ومن ثم جاء مايلي:

---

[1] HTTPS://droit7.blogspot.com

[2] HTTPS://droit7.blogspot.com

[3] HTTPS//www.tribunaldz.com

" يكفي لرد هذا التكييف و اثبات عدم وجود هذه الجريمة في القضية المطروحة امامنا، حيث انه يشترط ان يقوم المحرض بالفعل لغيره لا لنفسه و مادام الجاني في قضية الحال اشبع رغباته و برضى المجني عليها و عمرها لا يفوق 16 سنة فهي هنا قاصرة مميزة[1].

2- جريمة الاستغلال الجنسي للقصر عبر الانترنت

هو مصطلح يشير إلى ظهور الأطفال في صور أو أفلام أو مشاهد إباحية ذات مضمون جنسي بما فيها من مشاهد أو صور للاعتداء الجنسي على القصر. وعادة ما يظهرون بملابس خفيفة أو عراة تماماً كما يعني هذا المصطلح تصوير أي طفل بأية وسيلة كانت ، سواء كان يمارس ممارسة حقيقية أو محاكاة أنشطة جنسية صريحة ، أو أي تصوير للأعضاء الجنسية ، لإشباع الرغبة الجنسية أساساً ، ويعتبر معتدياً وإن بشكل غير مباشر أي شخص يطالع صوراً إباحية للأطفال أو يحتفظ به.[2]

و هنا يجب التنويه الى ان المشرع الجزائري صمت اتجاه هذه الجريمة الخطيرة و الواقعة على فئة حساسة من المجتمع، حيث لم يضمن او يستحدث اية مادة في هذا الشأن في قانون العقوبات الجزائري بالرغم من انتشارها في المجتمعات.

و عملا بنص المادة 394 مكرر 2 من ق.ع و التي نصت على ان يعاقب كل من قام عمدا او بطريق الغش بتصميم او بحث او تجميع او توفير او نشر او الاتجار او حيازة او استعمال لاي غرض كان المعطيات المخزنة او المعالجة او المرسلة عن طريق منظومة معلوماتية، فاذا كانت تحوز هذه المعطيات صورا اباحية فقد نكون بصدد جريمة جنسية.[3]

---

[1] قضية جنائي في المحكمة العليا 27 /1987/10 ملف رقم 43267

[2] https://www.antiextortion.com , ساعة الدخول 23:01

[3] نبيلة هبة هروال، مرجع سابق، ص17.

الفرع الثاني:

الجرائم السبيرانية الوقعة على الاموال

ان موضوع الاعتداء على الاموال في نطاق شبكة الانترنت ينصب على الحاسب الالي اذ يعتبر الوسيلة النافذة لجرائم الاعتداء على اموال الغير، و من هذا المنطلق سوف اتطرق الى جريمة الاحتيال المعلوماتي (اولا) ثم جريمة الاتلاف المعلوماتي (ثانيا) ثم جريمة التزوير المعلوماتي (ثالثا) .

أولا: جريمة الاحتيال المعلوماتي

عرفها بعض الفقهاء بانها" أي سلوك احتيالي ينتهج مناهج الحوسبة بنية الحصول على امتياز مالي".

وعرفها جانب اخر على انها" استخدام شبكة الأنترنت والأجهزة الحاسوبية للاستيلاء على اموال الغير بطرق احتيالية"[1]، و يتحقق الركن المادي لجريمة الاحتيال المعلوماتي اذا توافرت العناصر الثلاثة التالية:

*استخدام الجاني لوسيلة من وسائل التدليس

*النتيجة الاجرامية و المتمثلة في تسليم المجني عليه ماله للجاني.

*العلاقة السببية بين نشاط الجاني و النتيجة الاجرامية[2]

و نكون بصدد هذه الجريمة عندما تقع عن طريق المعلوماتية اذا استعمل الجاني احد الطرق الاحتيالية حيث يوهم المجني عليه بوجود مشروع وهمي كاذب، او يمنحه امل بالحصول على الربح فيسلم المجني عليه ماله بطريقة معلوماتية أو استعماله لصفة او اسم كاذب فيحول المجني عليه امواله له الكترونيا ، اضافة الى امكانية اتصال الجاني

---

[1] -سالم سمير المرعي، الجرائم المعلوماتية و جريمة الاحتيال عبر الشبكة، بحث مقدم لنيل لقب أستاذ في المحاماة، سوريا،2019، ص.ص22،21

[2]عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة دراسة في الظاهرة الاجرامية المعلوماتية ، طبعة اولى ، دار الفكر الجامعي، الاسكندرية،2010،ص160 .

بالمجني عليه عن طريق الشبكة او يتعامل مع الحاسب مباشرة فيدخل اسما كاذبا لإيهام الحاسب و الاحتيال على النظام[1].غير ان المشرع الجزائري لم ينص صراحة عليها بل يكتفي دائما بنصي المادة 394 مكرر 1 و 394 مكرر2 من ق.ع..

ثانيا: جريمة الاتلاف المعلوماتي

الاصل أن جريمة الاتلاف التقليدية تقوم على فعل الاتلاف الواقع على الاموال الثابتة و المنقولة اولا وعلى فعل الضرر ثانيا، وهنا يثور التساؤل حول مدى انطباق نص جريمة الإتلاف اذا وقعت عن طريق الانترنت؟

فقد تقع هذه الجريمة عن طريق الانترنت بإتلاف وظائف الكمبيوتر والتلاعب في البيانات والمعلومات المخزنة فيها بالمحو أو التعديل أو اعاقة سير النظام المعلوماتي، وقد قسمها المشرع الفرنسي الى اتلاف واقع على المكونات المادية و اتلاف واقع على المكونات المعنوية.

***الاتلاف الواقع على المكونات المادية:** و تتجلى وسائل الاتلاف هنا في احداث حريق مثلا او انفجار او تكسير او ادخال مواد معدنية داخل الجهاز، ويدخل في هذا النطاق الاقراص الممغنطة و الاسطوانات و الكابلات.[2]

***** الاتلاف الواقع على المكونات المعنوية (المنطقية):** ويطلق عليه الفقهاء "تدمير النظم المعلوماتية" حيث يقوم بإدخال فيروسات داخل النظام فتعطل سيره او تصيبه بالشلل التام اوت شغل الذاكرة بالكامل مما يؤدي الى توقفها و بالتالي تتلف المعلومات المتواجدة داخل النظام.[3]

---

[1] صغير يوسف: الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة ماجستير في القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو ،2013، ص45

[2] خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، طبعة 1 ،. دار الفكر الجامعي، الاسكندرية،، 2009، ص ص421،422.

[3] احمد خليفة الملط، الجرائم المعلوماتية، طبعة 2، دار الفكر الجامعي، الاسكندرية، 2006، ص538.

ثالثا: جريمة التزوير المعلوماتي

يمكننا القول بان اركان جريمة التزوير هنا لا تختلف عن الجريمة التقليدية لأنه يشترط لقيامها تغيير الحقيقة و حدوث الضرر كنتيجة ووجود طرق تسهل تغيير الحقيقة مثل وضع امضاءات او أختام مزورة او زيادة كلمات في المحررات او التقليد وهذا ما نصت عليه مادة 211 من ق.ع المصري و تعرف بالتزوير المادي.

كذلك هي من جرائم العمد لا تقوم الا بتوافر القصد العام وهو العلم بمكونات المحرر المزورونية استعمال المحرر فيما زور من اجله.[1]

اما التزوير المعنوي فيتمثل في تدوين معلومات و بيانات لم يدلي بها المتعاقدين او تضمين معلومة غير صحيحة لتحريف الحقيقة او اثبات واقعة كاذبة و جعلها صحيحة[2].

غير ان المشرع الجزائري كعادته اغفل هذه الجريمة و لم يخصها بنص خاص بل تناول فقط جريمة التزوير التقليدية، غير انه يفهم من نص المادة 394 مكرر1 بقولها "كل من ادخل بطريق الغش معطيات في نظام المعالجة الالية او ازال او عدل.." انها تستوعب هذه الجريمة.[3]

المطلب الثاني:
الجرائم الماسة بأمن الدولة و الماسة بالأمن الفكري

اصبحت الشبكة العنكبوتية تشكل خطرا كبيرا على حياة الاشخاص والشعوب، ليس هذا فقط بل تعدت حتى الى تهديد امن الدول واستقرارها؛ حيث أتاحت الانترنيت للكثير من المنظمات الارهابية الترويج لأفكارها ومعتقداتها، وأدت إلى ظهور جرائم جد خطيرة مثل جريمة التجسس الالكتروني على الدول بالإطلاع على مختلف اسرار الدول القائم بينها نزاعات واستخدامها كنقطة ضعف اما بهدف الغزو وشن هجومات عليها او معرفة استراتيجياتها الامنية في الجانب العسكري والاقتصادي كما تعطي الشبكة

---

[1] علي حسن طوالبة، الجرائم الالكترونية، ط1، مطبوعات جامعة العلوم التطبيقية ،2008، ص 152.

[2] مرجع نفسه، ص 468

[3] حمزة بن عقون، مرجع سابق، ص 174

العنكبوتية فرصا للتأثير على المعتقدات الدينية وتقاليد المجتمعات مما سهل خلق الفوضى داخل الدولة والمساس بأمنها الداخلي وبنظامها العام (فرع اول).

كما يعتبر النظام المعلوماتي وسيلة فعالة للاعتداء على حقوق الملكية الفكرية ومثال ذلك استخدام النظام المعلوماتي في السطو على بنوك المعلومات التي تتضمنها برامج نظام معلوماتي آخر (فرع ثان).

الفرع الاول:

الجرائم السبيرانية الماسة بأمن الدولة

ان الجرائم الواقعة على أمن الدولة من أخطر الجرائم التي قد تتعرض لها الدولة وأفرادها كونها تمس بشخصيتها وحقوقها ومصالحها الأساسية ومصالح افرادها، وتستقل هذه الجرائم بأحكام خاصة بها، تختلف عن الأحكام العامة التي يتم تطبيقها على الجرائم الواقعة على الأشخاص والجرائم الواقعة على الأموال وغيرها.

و من هذا المنطلق سوف اتناول جريمة الارهاب المعلوماتي (أولا)، ثم جريمة التجسس الالكتروني (ثانيا).

أولا: جريمة الارهاب المعلوماتي

يمكننا تعريف الإرهاب الإلكتروني بأنه: العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان، في دينه أو نفسه أو عرضه أو ماله بغير حق, باستخدام الموارد المعلوماتية والوسائل الإلكترونية.

و لعل ابرز الأساليب المنتهجة من طرف الارهابيين في نشر ثقافتهم و مخططاتهم هي كالاتي:

* **تبادل المعلومات الإرهابية ونشرها من خلال الشبكة المعلوماتية**: حيث اصبحت هذه الفئات الخطيرة تنشر وعيها من خلال الشبكة الالكترونية عن طريق استعمال الايميل الذي يعد اهم سبيل لنجاح مخططاتهم، من جمع المعلومات و الاجتماعات الالكترونية لأنه غالبا ما يتم مداهمة معسكراتهم و تفكيكها لذا لجؤا الى الانترنت، ليس هذا فقط بل

اصبحوا يحصلون على التمويل و الدعم الالكتروني الارهابي و يخططون لتنسيق و تطبيق المخططات الإرهابية بل حتى يستعملون الشبكة في التدريب الارهابي.

***انشاء المواقع الارهابية:** ان إنشاء مواقع خاصة بهم على الشبكة العالمية للمعلومات تساعدهم في تعليم و تجنيد اشخاص جدد و تلقينهم كيفية شن الهجومات الارهابية او طريقة صناعة القنابل و الاسلحة الفتاكة[1]

ثانيا: جريمة التجسس الالكتروني

يعرف التجسس الالكتروني بأنه " تجميع المعلومات السرية المخزنة داخل الحواسيب المربوطة بالأنترنت و الخاصة بسياسة الدولة و نظامها الاقتصادي و دفاعها و تسليمها لحكومة اجنبية اخرى".

و من هذا المنطلق يتبين لنا ان محل هذه الجريمة هو معلومات اقتصادية اي الهدف فيها من التجسس كشف اسرار السوق و ميزانية الدولة ، و كذلك تقع على المعلومات السياسية لأنها المرآة العاكسة لمدى قوة تلك الدولة و حكومتها.[2]

اما بالنسبة لموقف المشرع الجزائري من هذه الجريمة فقد اعترف بها في المادة 64 من قانون العقوبات و ذكر الافعال التي تدخل في نطاق التجسس في الفقرات 2و3و4 من المواد 61 و 62 و 63 من نفس القانون و سوف أعدد امثلة فقط على هذه الافعال:

-القيام بالتخابر مع دولة اجنبية او مع من يعملون لمصلحتها لمعاونتها في عملياتها الحربية للإضرار بالقوات الجزائرية و ذلك عن طريق تسريب معلومات سرية تمس بأمن الدولة.

-اتلاف اسرار الدفاع الوطني او الاقتصاد الوطني بقصد اعانة دولة اجنبية.

-تسهيل دخول القوات الاجنبية الى الارض الجزائرية او تقديم الوسائل اللازمة في ذلك.[1]

---

[1] عبدالله بن عبدالعزيز بن فهد العجلان، المؤتمر الدولي حول حماية امن المعلومات و الخصوصية في قانون الانترنت، القاهرة، 2008، ص 411 .

[2] نبيلة هبة هروال ، مرجع سابق، ص372،373.

اما عن جريمة التجسس عبر الانترنت فلم ينص عليها صراحة لكن تستشف من نص المادة 2/63 من ق.ع بقولها: " الاستحواذ بأية وسيلة كانت على مثل هذه المعلومات..." مثل استعمال الانترنت للولوج الى حواسيب الجيش الشعبي الوطني و الحصول على اسرار الدفاع.[2]

الفرع الثاني:

الجرائم السيبرانية الواقعة على حقوق الملكية الفكرية

فمن الجرائم التي انتشرت مؤخرا الاعتداء على حقوق الملكية الفكرية والذي يكون منصبا على البرامج والمعلومات،[3] فقد يكون النظام المعلوماتي وسيلة للاعتداء على حقوق الملكية الفكرية، و ذلك بالاعتداء على المعلومات التي يتضمنها نظام معلوماتي آخر، و تخزينها و استخدامها دون إذن صاحبها، حيث يعدّ اعتداء على الحقوق المعنوية و على قيمتها المادية و سوف اتطرق الى :

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 [4]

وقد يكون الهدف وراء قرصنتها تحقيق الربح المادي عن طرق فك شفرتها و تسويقها او نشرها عبر الشبكة لإلحاق الضرر بمصمم البرنامج.[5]

---

[1] الامر 156/66 مؤرخ في 8يونيو 1966، المعدل و المتمم و المتضمن قانون العقوبات الجزائري.

[2] نبيلة هبة هروال ، مرجع سابق، ص 38 .

[3] محمد عبد الله ابو بكر سلامة، جرائم الكمبيوتر والانترنت، د.ط، منشأة المعارف، الاسكندرية،2006، ص 194.

[4] سورية ديش، انواع الجرائم الالكترونية و اجراءات مكافحتها، مجلة العلوم السياسية و القانون، ع01، 2017

[5] ابراهيم ممدوح، مرجع سابق، ص 446

الفصل الثاني

الاليات القانونية لمواجهة الجريمة السيبرانية

يعد موضوع الآليات القانونية لمكافحة الجريمة السيبرانية أصبح هاجسا يؤرق القانونين بصفة خاصة، حيث باتت الجرائم السيبرانية نوع جديد من أنماط الجريمة وما تتميز به من خاصية عابرة للحدود الإقليمية للدول مما أدى إلى توجه المجتمع الدولي للتعاون من أجل ايجاد طرق ردعية لها ، إذا ما تركت على الأمن القومي للدول في جميع النواحي، لذلك سعت الدول إلى اتخاذ إجراءات مشتركة للتصدي لتلك الجرائم، وذلك من خلال إبرام اتفاقيات ومواثيق دولية لمواجهتها والعمل على محاربتها، واصبح من الضروري أن تتسع دائرة التعاون الوطني و الدولي وهذا ما دعى المنظمات الدولية للتحرك بغية سن قوانين تكافح مرتكبي تلك الجرائم.

كما تبرز أهمية هاته الدراسة في معرفة مدى كفاية النصوص القانونية الحالية لمنع الجريمة وردع مرتكبيها ومدى الحاجة إلى خلق اليات عقابية جديدة للحد من هذه الظاهرة، ومع تفشي جرائم المعلوماتية استحدث القانون رقم 09 /04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، فضلا عن الاساليب الاجرائية التي استحدثها المشرع في قانون الاجراءات الجزائية (المبحث الاول).

اما على الصعيد الدولي، فقد تواجدت العديد من الهيئات والمنظمات والمجالس الدولية التي تلعب دورا ملحوظا في إطار إبرام الاتفاقيات، محاولة منها ترسيخ وجوب التعاون الدولي لمواجهة الجرائم السيبرانية، وعلى رأس هذه المنظمات هيئة الأمم المتحدة، والمجلس الأوروبي وبعض الهيئات الأخرى، دون اغفال اتفاقية بودابست لمكافحة جرائم تقنية المعلومات باعتبارها خطوة رائدة على مستوى التعاطف بين الدول، وهي الوحيدة من حيث حجم الدول المنظمة اليها، وترتكز أهمية هذه الاتفاقية بفعاليتها على إقرارها إجراءات عملية هامة؛ بالإضافة الى انه قد اتخذت مبادرات من قبل العديد من المنظمات كالاتحاد الدولي للاتصالات و منظمة التعاون الاقتصادي والتنمية والمنظمة الدولية لتوحيد المقاييس، وبالرغم الجهود التي تبذلها المنظمات والهيئات الدولية في مكافحة الجرائم

السيبرانية إلا ان هناك عوائق وصعوبات تقف كعارض في نفاذ هذه الاتفاقيات الدولية والإقليمية (المبحث الثاني).

المبحث الاول:

الخصوصيات الاجرائية المتعلقة بمكافحة الجريمة السيبرانية

الوسائل الإجرائية المستحدثة لمكافحة الجريمة السيبرانية هي أساليب محددة بموجب التشريع، تهدف إلى إثبات وقوع الجريمة و الكشف عن شخصية مرتكبها، عن طريق استخدام اساليب وتقنيات إلكترونية مختلقة، وذلك تماشيا مع إرادة المشرع في القضاء على الجريمة المعلوماتية والتصدي لها؛ حيث استحدث المشرع اليات ووسائل لردعها وذلك من خلال قانون الاجراءات الجزائية وقانون رقم 04/09 (مطلب اول).

علاوة على ذلك، والى جانب الآليات الإجرائية ، لا بد من تعزيز تلك الآليات بأخرى مؤسساتية وطنية، وإقليمية فعالة تعمل كل منها في المحيط المخصص لها، مع إلزامية أن يكون بينها اتصال وتنسيق وتعاون للحصول على المعلومات التي تسمح بالقبض على مرتكبي الجرائم الإلكترونية وتسليمهم للمحاكمة؛ لأن التعاون المتبادل بين كل تلك الهيئات الوطنية سيساعد على احترام الحدود الإقليمية، وكذا السيادة الدولية التي تعد الجريمة الإلكترونية أكثر الجرائم انتهاكا لها(مطلب ثان).

المطلب الاول:

الوسائل المستحدثة في قانون الاجراءات الجزائية و قانون 04/09

من ضمن المقومات التشريعية التي أرساها المشرع الجزائري ضمن خطته في مكافحة الجريمة المعلوماتية، ما جاء به في قانون الاجراءات الجزائية؛ حيث وجب عليه تعديل القوانين الاجرائية القاصرة عن ردع المجرمين والكشف عن الجريمة وفق ما يتماشى مع حداثها ومستجداتها (الفرع الاول).

اما قانون رقم 04/09 المتعلق بالوقاية من جرائم تكنولوجيا الاعلام والاتصال ومكافحتها فقد جاء بإجراءات هامة و صارمة لوضع حد للجريمة ألا و هي اسلوب المراقبة الالكترونية بالإضافة الى اسلوب المساعدة القضائية الدولية (الفرع الثاني).

الفرع الاول:

الاساليب المستحدثة في قانون الاجراءات الجزائية

اعتبر المشرع الجزائري الجريمة المعلوماتية من بين الجرائم الاكثر تعقيدا؛ والتي يجب اللجوء فيها الى اساليب خاصة و اكثر دقة عن طريق جهاز الضبطية القضائية وهذا لطابعها الخطير، من خلال إجراءات بحث تتمثل في اسلوب التسرب (اولا)، و اسلوب اعتراض المراسلات (ثانيا).

اولا: اسلوب التسرب

لقد نظم المشرع هذا الإجراء في قانون الإجراءات الجزائية من المادة 65 مكرر 11 الى المادة 65 مكرر 18 تناول من خلالها تحديد مفهومه وشروطه و كيفية تطبيقه في الجرائم السيبرانية وسنحاول تفصيل ذلك من خلال ما يلي[1]:

1- مفهوم اجراء التسرب:

عرفت المادة 65 مكرر 12 من ق.إ.ج التسرب بأنه: " قيام ضابط عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص والمشتبه في ارتكابهم جناية أو جنحة، بإيهامهم أنه فاعل معهم أو شريك لهم خاف "، فالتسرب إذن هو تلك العملية المحضر لها مسبقا، تهدف إلى التوغل داخل خلية

[1]نعيم سعيداني ، مرجع سابق، ص174.

إجرامية ومعرفة نشاطاتها، والكشف عن الأشخاص المتورطين سواء كانوا فاعلين أصليين أم شركاء، وذلك بتوفير جميع الوسائل البشرية والتقنية اللازمة"[1].

2- الشروط المنظمة لإجراء التسرب:

ربط المشرع الجزائري اللجوء إلى عملية التسرب بجملة من الشروط الشكلية والموضوعية تضمنتها النصوص الواردة في قانون الإجراءات الجزائية وذلك بغرض إنجاح العملية وتسهيل مهمة الشخص القائم بها ،ومن أجل بلوغ الأهداف والنتائج المرجوة من وراء هذه العملية.[2]

أ-الشروط الشكلية:

*الزامية الحصول على الاذن:

فلا يمكن بأي حال من الأحوال أن يباشر ضابط الشرطة القضائية عملية التسرب بمفرده دون أن يكون متحصلا على إذن بذلك من قبل الجهات القضائية المختصة متضمنا هوية الفرد المتسرب و نوع الجريمة، وهذا ما نصت عليه المادة 65 مكرر11 من قانون الإجراءات الجزائية"يجوز لوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن..... حسب الحالة بمباشرة عملية التسرب[3]

غير انه يجب ان يكون مكتوبا قبل مباشرة العملية و تتم تلك العملية تحت رقابة وكيل الجمهورية أو قاضي التحقيق الذي أذن بها، والذي يصدر إذنه بناءً على تقرير يحرره ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب، مضمناً إياه كل العناصر

---

[1] انظر أسامة مهمل، الاجرام السيبراني، مذكرة لنيل شهادة الماستر اكاديمي، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، مسيلة،2017، ص48.

[2]أمينة معزيز، التسرب في قانون الاجراءات الجزائية الجزائري، كلية الحقوق والعلوم السياسية، جامعة مستغانم، ص 251.

[3]نعيم سعيداني ، مرجع سابق، ص 176

الضرورية لمعاينة الجريمة محل العملية في ظروف تؤمن عدم تعرض الضابط أو العون المتسرب للخطر، مع ذكر هويته وصفته.[1]

***تحديد المدة المطلوبة لعملية التسرب في جرائم الانترنت:**

تحديد مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة (4) أشهر، القابلة للتجديد حسب مقتضيات التحري أو التحقيق و ضمن الشروط الشكلية و الموضوعية، غير أنه يجوز للقاضي الذي رخص بإجرائها أن يأمر في أي وقت بوقفها قبل انقضاء المدة المحددة على أن تودع هذه الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب وهذا عملا بنص المادة 65 مكرر 15 الفقرة الاخيرة من ق.ا.ج.

***تحرير المحضر الخاص بإجراء التسرب:**

يقوم ضابط الشرطة القضائية بتحرير محضر عن مهمته ، و قد ذكر المشرع ذلك ان يتم هذا في شكل تقرير، و هو ما نصت عليه المادة 65 مكرر13 من ق.ا.ج، [2]ولا يودع الإذن المتعلق بالتسرب في ملف الإجراءات إلا بعد انتهاء العملية والحكمة من إيداعها بعد نهاية العملية وليس قبلها أو أثنائها كون عملية التسرب سرية لا يعلم بها إلا القاضي الذي رخص بها والضابط المشرف عليها والعون المتسرب [3]

ب- الشروط الموضوعية:

فرض المشرع الجزائري ضوابط موضوعية لنجاعة عملية التسرب الى جانب الشروط الشكلية و هي :

---

[1] خضرة شنيتر، الاليات القانونية لمكافحة الجريمة الالكترونية(دراسة مقارنة)، اطروحة لنيل شهادة الدكتوراه طور ثالث، تخصص جنائي، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، 2020، ص 135

[2] دلال ملياني، اشكالية الاثبات في جرائم الانترنت في التسريع الجزائري، اطروحة لنيل شهادة الدكتوراه تخصص قانون خاص، كلية الحقوق والعلوم السياسية، جامعة ابو بكر بلقايد، تلمسان، 2017، ص ص201،202

[3] أمينة معزيز، مرجع سابق، ص254.

***سبب التسرب (التسبيب):**

قرر المشرع في المادة 65 مكرر11 أنه لا يجوز لوكيل الجمهورية أو قاضي التحقيق اللجوء إليه إلا إذا دعت الضرورة الملحة للتحري والتحقيق ضمن الشروط المبينة في القانون .

وفي نطاق الجرائم المحددة حصرا في المادة 65 مكرر05 من قانون الإجراءات الجزائي الجنائية [1] يعني يجب على ضابط الشرطة القضائية تبيان العناصر التي أقنعت الجهات القضائي المختصة لمنح الإذن[2].

***نوعية الجرائم:**

اي يجب على ضابط الشرطة القضائية تحديد نوع الجريمة و يجب ان لا تخرج عن نطاق الجرائم المنصوص عليها في المادة 65 مكرر5 ، وهي جرائم المخدرات ،أو الجريمة المنظمة العابرة للحدود ،أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و جرائم تبييض الأموال أو الجرائم الإرهابية، أو جرائم المتعلقة بتشريع الصرف ،أو جرائم الفساد.[3]

3- كيفية القيام بعملية التسرب في الجرائم السيبرانية:

حيث إن عملية التسرب في نطاق الجريمة السيبرانية تتمثل في دخول ضابط أو عون الشرطة القضائية إلى العالم الرقمي، وذلك باختراقه لمواقع مختلفة والبحث عن ثغرات إلكترونية فيها وفتحها، أو اشتراكه في محادثات غرف الدردشة، وايهامهم انه شريك لهم و فاعل معهم في الجريمة، مستخدما أسماء أو صفات وهمية وذلك بهدف الحصول على معلومات تفيد في التحقيق[4].

---

[1] صالح شنين، التسرب في القانون الجزائري حماية للنظام العام والحريات ام حماية للنظام،المجلة الجزائرية للقانون المقارن، جامعة عبد الرحمان ميرة بجاية، ع 2،ص126.

[2] نعيم سعيداني، مرجع سابق ص176.

[3] المادة 65 مكرر5 من الامر 155/66 المؤرخ في 8 يونيو 1966 المعدل والمتمم المتضمن قانون الاجراءات الجزائية .

[4] ينظر أسامة مهمل، مرجع سابق، ص 49.

ثانيا: اعتراض المراسلات

فالأصل في الدستور الجزائري ان تكون المكالمات سرية لا يجب الاعتراض لها بطريقة غير شرعية ما لم ينص القانون على ذلك و هذا عملا بنص المادة 39 من الدستور تنص صراحة على أن :"لا يجوز انتهاك حرمة حياة المواطن الخاصة و حرمة شرفه و يحميها القانون ، سرية المراسلات و الاتصالات الخاصة بكل أشكالها مضمونة" [1]

1-تعريف اجراء اعتراض المراسلات

وهو القيام باعتراض كل المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، التي يقصد بها التنصت التليفوني، ولم يعرف المشرع الجزائري هذه التقنية شأنه في ذلك شأن المشرع الفرنسي غير أن القضاء الفرنسي عرفها على أنها:" تقنية يتم من خلالها الاعتراض عن طريق ربط خط هاتفي للمشتبه فيه مع اللجوء إلى تسجيل المكالمات في أشرطة مغنطيسية"[2]

و تجدر الاشارة الى ان هذا السلوب يخضع لنفس اجراءات التسرب الشكلية و الموضوعية وذلك في المواد من 65 مكرر 5 الى 65 مكرر10"

حيث أنه بالرجوع لنص المادة 65 مكرر 5 من ق.ا.ج و التي جاء فيه" إذا إقتضت ضرورات التحري في الجريمة المتلبس بها، أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بالمعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد، يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي:

- إعتراض المراسلات التي تتم عن طريق وسائل الإتصال السلكية واللاسلكية، وضع الترتيبات التقنية، دون موافقة المعنيين من أجل إلتقاط الصور وتثبيت وبث

[1] https://www.mohamah.net

[2] خضرة شنيتر، مرجع سابق، ص 123

وتسجيل الكلام المتفوه أو إلتقاط صور لشخص أو عدة أشخاص يتواجدون في أماكن خاصة أو عمومية أو إلتقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.."[1].

يتبين لنا ان المشرع الجزائري ركز على الجرائم الخطيرة فقط منها الماسة بالمعالجة الالية للمعطيات أي ما يعرف بالجريمة السيبرانية[2]

وتجدر الاشارة الى أن المشرع الجزائري لم يحدد الاماكن المسموح فيها باتخاذ هذا الاجراء بل اكتفى بقول اماكن عمومية في نص المادة 56 مكرر 05 ؛ خلافا للمشرع الفرنسي الذي حدد الاماكن التي يتخذ فيها الاجراء مثل المحلات ذات الطابع المهني للأطباء وسيارات المحامين وهذا بموجب المادة 706-96 من ق.ا.ج. الفرنسي[3]

2- كيفية تطبيق اعتراض المراسلات على الجريمة السيبرانية:

يجب التنويه الى ان عملية الإعتراض تنصب على البريد الالكتروني، ومن المعلوم أن كل رسالة إلكترونية يظهر فيها معلومات عامة مثل تاريخ إنشاء الرسالة وتاريخ تلقيها وكذا عنوان المرسل و المرسل اليه لكن هذه المعلومات غير كافية بل يجب الحصول على المزيد من المعلومات التي يمكن العثور عليها في حاشية رسائل البريد الإلكتروني والتي لا تظهر بصورة مباشرة وإنما يتطلب الأمر من المستخدم إجراء بعض الخطوات للحصول عليه[4]

الفرع الثاني:

الوسائل الاجرائية المستحدثة في قانون 04/09

الى جانب الاساليب المنصوص عليها في قانون الاجراءات الجزائية استحدث المشرع الجزائري اجرائين للتحري عن الجريمة السيبرانية بموجب قانون رقم 04/09 وهذا لقصور القوانين

---

[1] نص المادة 65 مكرر5 من الامر 155/66، مرجع سابق

[2] انظر اسامة مهمل، مرجع سابق، ص 46

[3] يزيد بوحليط، الجرائم الالكترونية والوقاية منها في القانون الجزائري، ط 1، دار الجامعة الجديدة، الجزائر، 2019،ص 365

[4] انظر نعيم سعيداني، مرجع سابق، ص 181، 182

الاجرائية الاخرى عن مكافحة الجريمة ألا وهما المراقبة الالكترونية (أولا)، وأسلوب المساعدة القضائية الدولية (ثانيا).

اولا: نظام المراقبة الالكترونية

1-تعريف نظام المراقبة الالكترونية:

المشّرع الجزائري لم يتصّد لضبط تعريف المراقبة الالكترونية لا في مواد قانون الإجراءات الجزائّية ولا في القانون المتعلق بالوقاية من جرائم تكنولوجيات الاعلام و الاتصال، بل ترك : "هذا الامر للفقه حيث عرفه **"اجراء تحقيق يباشر خلسة وينتهك سرية الأحاديث الخاصة، تأمر به السلطة القضائية في الشكل المحدد قانوناً بهدف الحصول على دليل غير مادي لجريمة تحقق وقوعها ويتضمن من ناحية استراق السمع ومن ناحية أخرى حفاظه على الأشرطة عن طريق أجهزة مخصصة لهذا الغرض"**[1] كما عرفها اخرون بأنها:" عمل أمني أساسي له نظام معلومات إلكتروني يقوم فيها للمراقب بمراقبة المراقب بواسطة الأجهزة الإلكترونية عبر شبكة الإنترنت، لتحقيق غرض محدد وافراغ النتيجة في ملف إلكتروني، وتحرير تقارير بالنتيجة" لكن رجوعا لذات القانون نجد أن المشرع الجزائري لم يعتبر هذا الإجراء طريقة من طرق الحصول على الأدلة الجنائية الرقمية فقط، بل أدرجه أيضا ضمن التدابير الوقائية من الجريمة السيبرانية حماية للنظام العام من التهديد، و هذا عملا بنص المادة 04 من هذا القانون حيث يطبق هذا الاسلوب في الجريمة الموصوفة بأعمال ارهابية و التي يظهر ان فيها اعتداء على منظومة معلوماتية على نحو يهدد النظام العام و الدفاع الوطني او مؤسسات الدولة [2]

---

[1] عبد الحليم بن بادة، "المراقبة الالكترونية كإجراء لاستخلاص الدليل الالكتروني" ،المجلة الأكاديمية للبحث القانوني، جامعة غرداية، مج 10، ع03، ص 7391

[2] اسامة مهمل، مرجع سابق، ص 49،50.

2 ضوابط القيام بالمراقبة الالكترونية:

لقد قيد المشرع الجزائري اللجوء الى اسلوب المراقبة الالكترونية بضوابط منها:

*اشترط الحصول المسبق على إذن مكتوب ومسّبب من الجهات القضائيّة المختصة و هو النائب العام لدى مجلس قضاء الجزائر، باعتبار انه الجهة المخولة قانونا لمنح الاذن لمباشرة هذا الاجراء في الجرائم المنصوص عليها في قانون رقم 04/09

*حدد الجرائم التي يشرع فيها اجراء المراقبة الالكترونية وهي الموصوفة بأعمال إرهابية والماسة بأمن الدولة وهذا عملا بالمادة 04 من هذا القانون.

*اما بخصوص المدة المخصصة للاذن الممنوح لضباط الشرطة القضائية فقد حددها بستة (6) أشهر قابلة للتجديد ولم يقيد عدد المرات التي يجوز فيها تجديد الاذن.

* و اشترط ان يكون ضباط الشرطة القضائية المكلفون بإجراء المراقبة منتمون للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها لكي يكون الاذن صادر عن مجلس قضاء الجزائر.

*يتم اللجوء اليها لمقتضيات التحّري والتحقيقات القضائّية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية. [1]

ثانيا: اجراء المساعدة القضائية الدولية

تعّرف المساعدة القضائية الدولية بأنها" كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم" ولقد نص المشرع الجزائري في القانون رقم 09 /04 على مبدأ المساعدة القضائية في المادة 16 منه معتبرا أنه في إطار التحريات والتحقيقات القضائية الجارية لمعاينة الجرائم المعلوماتية يمكن

[1] انظر عبد الحليم بن بادة، مرجع سابق، ص ص 397، 398.

للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني، وتتخذ عدة صور نذكر أهمها:

1-تبادل المعلومات:

حيث أنه يعتبر تبادل المعلومات وتبادل الخبرات من أهم العناصر المتعلقة بالوقاية من الجريمة إذ أن تقاسم المعلومات وسرعة الحصول عليها يعمل على تسهيل مهمة الأجهزة الوطنية في التحرك لمواجهة الجريمة، ويشمل تقديم المعلومات والبيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية عن الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم وقد يشمل التبادل السوابق القضائية للجناة[1].

حيث حرصت المادة 26 من اتفاقية بودابست على التأكيد على واجب الدولة التي تمتلك معلومات هامة مساعدة دولة أخرى في معرض التحقيقات أو تداول الدعاوى الجنائية في الحالات التي لا يدرك فيها الفريق الذي يجري التحقيقات أو الملاحقة وجود هذه المعلومات [2].

2-نقل الاجراءات:

يقصد بنقل الإجراءات قيام الدولة اليت ارتكبت فيها الجريمة الإلكترونية أو بعض عناصرها بنقل إجراءات البحث؛ التحري والتحقيق في الجريمة إلى دولة أخرى قد مست مصالحها أيضا وذلك بناء على اتفاقية دولية متى توافرت مجموعة من الشروط والتي من أهمها: التجريم المزدوج الذي يقصد به أن يكون الفعل المنسوب إلى الشخص جريمة في الدولة الطالبة والدولة المقدم إليها طلب نقل الإجراءات، إصافة إلى شرعية الإجراءات المطلوب اتخاذها.

---

[1] عزيزة رابحي، مرجع سابق، ص 309،310

[2] اتفاقية بودابست لمكافحة الجريمة المعلوماتية المصادق عليها في 23 نوفمبر 2001 في بودابست عاصمة المجر ووقعت عليها كندا واليابان.

3- الانابة القضائية:

يقصد بالانابة القضائية طلب الدولة المحققة في الجريمة الإلكترونية من الدولة المطلوب منها اتخاذ إجراء قضائي محدد من إجراءات التحري والتحقيق في الدعوى العمومية.

نظم المشرع الجزائري مسألة الإنابة القضائية في الباب الثاني من الكتاب السابع من قانون الإجراءات الجزائية حيث نصت المادة 72 منو على مايلي: "في حالة المتابعات الجزائية غَير السياسية في بلد أجنبي تسلم الإنابات القضائية التي تكون صادرة من بلد أجنبي عبر القنوات الدبلوماسية ويتم إرسالها إلى وزارة العدل، تنفذ الإنابات القضائية إذا كان لها محل وفقا للقانون الجزائري مع مراعاة مبدأ العاملة بالمثل"[1]

المطلب الثاني:

الهيئات الوطنية المكلفة بالوقاية من الجريمة السيبرانية

خصصت مختلف التشريعات الوطنية والدولية مؤسسات ومصالح من أجل مكافحة الجريمة الإلكترونية، فمثلا المشرع الجزائري خصص هيئات ووحدات لمكافحتها حتى يتمكن من تحقيق الاستراتيجية الوطنية في أمن أنظمة المعلومات التي تفرضها عمليات حماية تلك الأنظمة، والتي أصبحت تشكل في معظم الأحيان الاستعمالات اليومية للتكنولوجيا المعلوماتية و شبكات الانترنت. منها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها (الفرع الاول)، ومصالح موجودة في وحدات الامن الوطني المتخصصة في مكافحة الجريمة السيبرانية (الفرع الثاني)

الفرع الاول:

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال

فبموجب المادة الثالثة عشرة من القانون رقم 04/09 المتضمن القواعد الخاصة

---

[1] ليلى عصماني، المساعدة القضائية الدولية آلية للحصول على الدليل الالكتروني، مجلة القانون المجتمع والسلطة، جامعة وهران2، مج 09، ع02، 2020 ص21،23

للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها نص المشرع الجزائري على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال ومكافحتها حتى تضمن الحق الدستوري لكل مواطن في حرمة حياته ومراسلاته من المساس بها بداعي مكافحة الجرائم، حيث صدر المرسوم الرئاسي 19-172 المعدل والملغي للمرسوم 15-261 منظما كيفية سير ومهام هذه الهيئة وتشكيلتها، وسوف اتناول تشكيلة الهيئة (أولا)، ثم البعض من مهامها (ثانيا)[1].

اولا:تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال

لقد تضمن المرسوم الرئاسي 19-172 تعديلا في الهيكل التنظيمي للهيئة حيث اصبحت تضم مجلس التوجيه و المديرية العامة .

1-مجلس التوجيه:

يترأسه وزير الدفاع الوطني أو ممثله ويتشكل من وزارات الداخلية، وزارة العدل، وزارة المواصلات السلكية واللاسلكية يكلف بالتداول حول الاستراتيجية الوطنية للوقاية من الجرائم المحددة في المرسوم وكذا التداول حول مسائل التطوير والتعاون مع المؤسسات والهيئات الوطنية المعنية، ويجتمع مجلس التوجيه في دورة عادية مرتين في السنة بناء على استدعاء من رئيسه ويمكنه أن يجتمع في دورة غير عادية كلما كان ضروريا بناء على استدعاء أو بطلب من أحد أعضائه أومن المدير العام للهيئة[2]..

يتَّرأس هذا المجلس وزير الدفاع الوطني القائد الأعلى للقوات المسلحة أي رئيس الجمهورية ومن الناحية العملية فإن نائب وزير الدفاع هو من ينوبه في رئاسة المجلس وهو ما نصت عليه المادة 05 من المرسوم 19- **172**

[1] خضرة شنيتر،مرجع سابق، ص 156

[2] https://www.aps.dz/ar/algerie

2-المديرية العامة:

طبقا لنص المادة 09 من هذا المرسوم فإنه تنشأ مديرية عامة يترأسها مدير عام يعين طبقا لتنظيم المعمول به في وزارة الدفاع الوطني وهو ما نصت عليه المادة 19 من نفس المرسوم، كما ان هذه المديرية تضم من الناحية التنظيمية مديريتان وهذا تطبيقا لنص المادة 10 من المرسوم و هما المديرية التقنية والتي تتكلف بمراقبة الاتصالات الالكترونية من الجرائم الارهابية أو الاعتداءات على أمن الدولة، ومديرية الادارة والوسائل تكلف بمراقبة تسيير ميزانية الهيئة والتسيير المالي اليومي لمواردها البشرية.[1]

ثانيا: مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال

لقد فصل المسوم الرئاسي مهام كل هيئة غير ان المادة 14 من قانون 04/09 ذكرها باختصار.

1-مهام مجلس التوجيه:

يكلف المجلس على الخصوص بالتداول حول الاستراتيجية الوطنية للوقاية من الجرائم المعلوماتية وتكنولوجيا الاتصال ومكافحتها، وكذا يتداول ويناقش مسائل التطوير والتعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال، إجراء تقييم دوري لحالة التهديد في مجال الجرائم والاهداف المرجوة منها، كما يقترح أي نشاط يراه مناسبا يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المعلوماتية ومكافحتها[2].

---

[1] حكيمة بوكحيل، الهيئة الوطنية للوقاية من جرائم الإعلام وتكنولوجيا الاتصال ودورها في تفتيش نظم المعلوماتية، مجلة الدراسات القانونية المقارنة، جامعة سوق اهراس، مج 07، ع 01، 2020،ص 1545

[2] مراد مشوش، الجريمة المعلوماتية في ظل قانون العقوبات وقانون الوقاية من جرائم تكنولوجيات الاعلام والاتصال، مجلة القانون، جامعة غرداية، مج09،ع 01،2020، ص ص 126،127.

2-مهام المديرية العامة:

تسهر على تنسيق نشاطات الهيئة و تبادل المعلومات مع الهيئات الأجنبية في اطار التعاون الامني، بالإضافة الى مهامها الادارية مثل مراقبة ميزانية الهيئة وتحضير الاجتماعات لمجلس التوجيه لأنها تتولى الامانة العامة و هذا ما أقرت به المادة 05 من هذا المرسوم[1]

الفرع الثاني:

وحدات الأمن الوطني المتخصصة في مكافحة الجريمة السيبرانية

في اطار مكافحة الجريمة السيبرانية والقضاء على اثارها على المستوى الوطني خصصت الدولة الجزائرية عدة فرق متخصصة فمنها ما يتواجد بمراكز الشرطة (اولا)، و البعض الاخر في جهاز الدرك الوطني (ثانيا).

أولا: وحدات مكافحة الجريمة السيبرانية في جهاز الشرطة

حيث تتولى المديرية العامة للأمن الوطني التحقيق في الجرائم السيبرانية والسعي لمكافحتها وذلك عن طريق انشاء مخابر متخصصة و فرق كذلك وهذا لما تمثل من دور فعال في ردع الجريمة.

1-المخابر:

يوجد مخبر مركزي للشرطة العلمية بالجزائر العاصمة ومخبر جهوي في قسنطينة ووهران للشرطة العلمية كذلك، وحسب الاحصائيات المصرح بها من دائرة الادلة الرقمية والاثار التكنولوجية التابعة لمخبر قسنطينة فقد شهدت عدة قضايا في 2014 اشهرها واحدة تتعلق بالإنابة القضائية الدولية حيث اقدم شابين من قسنطينة على تعطيل النظام المعلوماتي الخاص بموقع وزارة الخارجية الكويتية

[1] انظر حكيمة بوكحيل، مرجع سابق، ص 1546

2-الفرق المختصة:

لقد خصص المشرع الجزائري فرقة على مستوى أمن كل ولاية، حيث تم انشاء المصلحة المركزية لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ثم تم انشاء خلية مكافحة الجرائم المعلوماتية ثم ترقت الى خلية بحد ذاتها.[1]

ثانيا: وحدات مكافحة الجريمة السيبرانية على مستوى جهاز الدرك الوطني

يضع الدرك الوطني لتنفيذ مهامه في مجال الحفاظ على الأمن والنظام العام وحدات متنوعة وعديدة على مستوى القيادة العامة، أو على مستوى القيادات الجهوية والمحلية نذكر منها :

1-المعهد الوطني للأدلة الجنائية وعلم الاجرام:

يتواجد ببوشاوي في العاصمة والتابع للقيادة العلمية للدرك الوطني قسم الإعلام ولإلكترونيك الذي يختص بالتحقيق في الجرائم الإلكترونية، حيث يقوم بتحليل الأدلة الخاصة بالجرائم الإلكترونية، وذلك بتحليل الدعامات الإلكترونية، وانجاز المقاربات الهاتفية، وتحسين التسجيلات الصوتية والفيديو والصورة وذلك لتسهيل استغلالها بالإضافة إلى مراكز الرقابة من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ببئر مراد رايس والتابع لمديرية الأمن العمومية للدرك الوطني[2] ويقوم المعهد بالمشاركة في الدراسات والتحاليل المتعلقة بالوقاية والتقليل من كل أشكال الإجرام، كما يتم على مستوى المعهد تصميم بنوك المعلومات كالبصمات الجينية وغيرها لتكون في متناول المحققين والقضاة بغرض وضع المقاربات واستخلاص الروابط المحتملة بين المجرمين وأساليب النشاط الإجرامي[3]

---

[1] رجاء اومدور، مرجع سابق، ص ص 103،104

محمد بوعمرة، جهاز التحقيق في الجريمة الالكترونية في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماستر في

[2] العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة محند اولحاج، البويرة،2019، ص34

[3] خضرة شنيتر، مرجع سابق، ص 202.

2- مركز الوقاية من جرائم الاعلام الالي والجرائم المعلوماتية للدرك الوطني:

ويعتبر الجهاز الوحيد المختص بهذا المجال في الجزائر، ويهدف أساسا إلى تأمين منظومة المعلومات لخدمة الامن العمومي واعتبر بمثابة مركز توثيق ومقره يوجد ببئر مراد رايس، هذا المركز يعمل على تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة، وتحديد هوية أصحابها سواء كانوا أفراد أو جماعات كما يهدف إلى مساعدة باقي الأجهزة الامنية الاخرى في أداء مهامها[1]

المبحث الثاني:

الجهود الدولية المبذولة للوقاية من الجرائم السيبرانية

إن التعاون الدولي في مجال مكافحة الجريمة السيبرانية قد يتخذ شكلان فالأول يتعلق بضرورة التعاون في تنفيذ القانون لمتابعة ومعاقبة المجرمين بعد ارتكاب الجريمة والتي تعبر اختصاصات قضائية متعددة ذات نظم قانونية مختلفة، والمتمثل في التعاون القضائي، و الثاني يتعلق بالسعي إلى اتخاذ الإجراءات والآليات ذات الطبيعة التقنية الفنية التي تكفل منع ارتكاب الجريمة في مرحلة التنفيذ، وإذا كان التعاون الدولي هو الطريقة الفعالة لمكافحة الإجرام السيبراني ، فإن هذا التعاون يقتضي التخفيف من الفوارق بين الأنظمة العقابية الداخلية لأن التباعد بين هذه الانظمة يجعل المجرم المعلوماتي يبحث عن الأنظمة الأكثر تساهلا .

لذلك أبرمت العديد من الاتفاقيات الدولية في مجال التعاون الدولي من أجل مكافحة الجريمة السيبرانية وتظهر معالم هذا التقارب في قبول حالات تفويض الاختصاص في اتخاذ اجراءات التحقيق و جمع الأدلة و تسليم والاعتراف بالأحكام الجنائية، بحيث أن

[1] جمال الدين دندن، الاستراتيجية الامنية للدولة الجزائرية في مكافحة الجرائم السيبرانية، مجلة صوت القانون، جامعة الجزائر1، مج 07،ع 02،2020،ص986

هذا القانون الدولي لا ينال من سيادة الدولة، بل بالعكس عدم التعاون يزيد من التباعد بين الأنظمة العقابية مما يساعد على ارتفاع نسبة هذه النوعية من الجرائم (مطلب اول).

ناهيك عن الجهود التي بذلتها الدول والمنظمات العربية لتتمكن من القضاء على هذه الجريمة المستجدة (مطلب ثان).

المطلب الاول:

جهود الدول الغربية المبذولة لمحاربة الجريمة السيبرانية

لقد لعبت الدول دور مهما في الحفاظ على الامن والاستقرار، وخاصة في مجال مواجهة الجريمة السيبرانية عبر اقرار العديد من الاتفاقيات وعقد المؤتمرات الدولية، حيث تعتبر الجهود الدولية داعمة للجهود التي تبذلها مختلف الدول في تشريعاتها الداخلية، فتعتبر بمثابة قوانين استرشاديه تأخذ بها الدول لمواجهة الجرائم المستحدثة بما فيها الجريمة الالكترونية او ما يعرف بالجريمة السيبرانية.

و لقد كان للهيئات والمنظمات والمجالس الدولية دور ملحوظ في إبرام الاتفاقيات كمحاولة لترسيخ التعاون الدولي للتصدي لها (فرع اول)، اضافة الى الهيئات الاقليمية التي برز دورها في ردع الجريمة (فرع ثان).

الفرع الأول:

المنظمات الدولية المساهمة في مكافحة الجريمة السيبرانية

لقد ساهمت المنظمات الدولية بشكل كبير في الوقاية من الجريمة المعلوماتية و هذا نظرا لطابعها المتعدي لحدود الدول، لاسيما المنظمة الدولية للشرطة الجنائية كجهاز لمكافحة الجريمة (اولا)، وكذلك الجهود المبذولة من طرف منظمة الامم المتحدة (ثانيا)، ومنظمة التعاون الاقتصادي والتنمية (ثالثا).

اولا: المنظمة الدولية للشرطة الجنائية كجهاز لمكافحة الجريمة السيبرانية (الانتربول)

هي أكبر منظمة شرطة دولية أنشئت عام 1923 مكونة من قوات الشرطة ل195 دولة حيث في عام 1923 عقد في العاصمة النمساوية "فينا" مؤتمرا لجمعية الدولية للقانون الجنائي، بمبادرة الدكتور (يوهانز شوبار) رئيس شرطة مدينة فينا، لمناقشة التعاون الدولي في المجال الجنائي، إلا أن عمل الجمعية توقف بسبب النزاعات المسلحة التي اندلعت في ذلك الوقت. وفي عام 1925 عقد اجتماع في مدينة برلين لإنشاء مركز للمعلومات، وقد تم تبني هذا الأمر بالفعل وأنشئ ذلك المركز عام 1927، لكن هذه المنظمة أنشأت عندما صدرت الجمعية العامة للأمم المتحدة في دورتها الخامسة والعشرين والتي عقدت في العاصمة النمساوية فينا للفترة من 7 – 13 / حزيران / 1956 ،قرارًا خاصًا باعتماد النظام الأساسي للمنظمة الدولية للشرطة الجنائية وأصبح هذا النظام نافذ المفعول ابتداء من 13/6/1956 فأصبحت المنظمة منذ ذلك التأريخ تعمل بشكل دائم ومستقر[1].

1-الهيكل التنظيمي للمنظمة:

لقد نصت المادة 05 من ميثاق المنظمة على أنها تتكون من:

***الجمعية العامة:** وهي اعلى سلطة في المنظمة تتكون من مندوبي الدول الأعضاء في المنظمة الذين تعينهم دولهم، و تسند لها القيام بتحديد المبادئ العامة لتحقيق اهداف المنظمة، كذلك اعتماد القرارات وتوجيه التوصيات إلى الأعضاء بشأن المسائل باختصاص المنظمة، اضافة الى دراسة برنامج عمل السنة الموالية وتقديمه للأمين العام للموافقة عليه

***اللجنة التنفيذية:** تتكون من 13 عضو من دول مختلفة و تجتمع مرة واحدة في السنة، يعهد اليها القيام بالإشراف على تنفيذ قرارات الجمعية العامة و اعداد جدول الأعمال لدوراتها، بالإضافة الى مراقبة ادارة الامين العام.

[1]https://pulpit.alwatanvoice.com/

*الامانة العامة: حيث نصت المادة (26) من النظام الأساسي على مهام الأمانة العامة والتي تتمثل في تطبيق قرارات الجمعية العامة واللجنة التنفيذية، و القيام بإدارة المنظمة العامة، اضافة الى تأمين الاتصال بالسلطات الوطنية والدولية لمعالجة مسائل التحريات الجنائية.

المستشارون: يتم تعيين المستشارين من قبل اللجنة التنفيذية، ولا يكتسب تعيينهم الصفة النهائية الا بعد المصادقة علية من قبل الجمعية العامة للمنظمة، وفترة تعيينهم تستمر لثلاث سنوات لدراسة المسائل العلمية والفنية، ويكون دورهم استشاري فقط أي غير ملزم.[1]

2-دور الانتربول في مكافحة الجريمة السيبرانية:

حيث تعتبر همزة وصل بين الشرطة عبر العالم والمنظمات والهيئات الاقليمية نظرا لموقعها الهام والمساعد على ردع الجريمة وتحديد هوية المجرمين، وكمثال عن المجهودات المبذولة من طرفها في نطاق مكافحة الجريمة نأخذ ما حصل في الجمهورية اللبنانية حين تلقت النيابة العامة برقية من انتربول ألمانيا حيث تم توقيف طالب جامعي متهم بإرسال صور اباحية لقاصر دون 10 سنوات من موقعه على الانترنت[2]

ثانيا: جهود منظمة الأمم المتحدة

بذلت منظمة الأمم المتحدة جهودا كبيرة في سبيل مكافحة جرائم الإنترنت، وذلك لما تسببه هذه الجرائم من أضرار بالغة وخسائر جسيمة بالإنسانية ، وايمانا منها بأن منع هذه الجرائم ومكافحتها يتطلبان استجابة دولية في ضوء الطابع والأبعاد الدولية لإساءة استخدام الكمبيوتر والجرائم المتعلقة به[3]

---

[1] https://www.mohamah.net/

[2] خضرة شنيتر، مرجع سابق، ص ص 212،213

[3]- يوسف صغير، مرجع سابق، ص93

وتوصلت منظمة الأمم المتحدة في مؤتمرها الثامن المنعقد بهافانا 1990 حول منع الجريمة و معاملة المجرمين إلى اصدار قانون خاص بالجرائم المتعلقة بالحاسوب ، و أشار القرار إلى أن الأجرام الدولي لمواجهة الجرائم المستحدثة يتطلب من الدول الأعضاء اتخاذ عدة إجراءات تتلخص فيما يلي:

* حماية مصالح الدولة وحقوق ضحايا جرائم السيبرانية

* رفع درجة الوعي لدى الجماهير و القضاة و الأجهزة العاملة على مكافحة هذا النوع من الجرائم

* التعاون مع المنظمات المهتمة بهذا الموضوع ، و وضع و تدريس الآداب المتخذة في استخدام الحاسوب في المناهج التعليمية[1]

*تحديث القوانين و أغراضها الجنائية بما في ذلك التدابير المتخذة من أجل ضمان تطبيق القوانين الجنائية الراهنة من تحقيق و قبول الأدلة على نحو ملائم و إدخال التعديلات إذا دعت الضرورة لذلك، ثم عقدت كذلك الأمم المتحدة المؤتمر الثاني عشر لمنع الجريمة و العدالة الجنائية بالبرازيل أيام 12 إلى 19 أفريل 2010 ، حيث ناقشت فيه الدول الأعضاء ببعض التعمق مختلف التطورات الأخير في استخدام التكنولوجيا من طرف المجرمين و السلطات المختصة في مكافحة الجريمة الحاسوبية[((((2))))]

وما قد سلف ذكره يعتبر نقطة صغيرة من بحر المجهودات التي بذلتها هذه المنظمة، ولا تزال تثير مجهودات كبيرة لكن لا يسعني الوقت لتعدادها، و تجدر الاشارة الى ان منظمة الامم المتحدة تبقى الهيئة الأمثل لمكافحة الاجرام السيبراني

[1] https://www.droitetentreprise.com

[2] يوسف صغير، مرجع سابق، ص 94

ثالثا: منظمة التعاون الاقتصادي والتنمية

بدأت هذه المنظمة الاهتمام بالجريمة السيبرانية منذ عام 1978 ، حيث وضعت مجموعة من الأدلة و قواعد إرشادية تتصل بتقنية المعلومات، و يعد الدليل المتعلق بحماية الخصوصية و قواعد نقل البيانات من أول الأدلة التي تم تبنيها من قبل مجلس المنظمة في عام 1980 مع التوصية للأعضاء بالالتزام بها، وفي سنة 1983 أصدرت تقريراً بعنوان الجرائم المرتبطة بالحاسوب و تحليل السياسة القانونية الجنائية، حيث تطرق التقرير الى السياسة الجنائية القائمة و المقترحات الخاصة في عدد من الدول الأعضاء ، وتضمن الحد الأدنى من أفعال سوء استخدام الحواسيب و التي على الدول تجريمها وكمثال عن هذه الافعال الدخول الى الحاسب بطريقة غير مصرح بها، أو الإفشاء الغير مصرح به للمعلومات المعالجة آلياً وإتلاف أو تخريب ما يحتويه من بيانات و برامج.

تعقد المنظمة سنويا عددا من الملتقيات المعمقة للقطاعات ذات العلاقة بهذا المجال تركز فيها على معايير الأمن ومستوياته، إضافة إلى معايير تنفيذ وتطبيق القانون وذلك بهدف مواكبة التطورات في مجال جرائم الإنترنت.[1]

الفرع الثاني

الهيئات الاقليمية الساعية لمكافحة الجريمة السيبرانية

وضعت عدة مؤسسات إقليمية لمكافحة الجريمة، كانت نتاج توحيد مجهودات دول جمع بينها في كثير من الأحيان الموقع الجغرافي والحدود السياسية، والتهديد المشترك الذي تفرضه الجرائم العابرة للحدود كما هو الحال في الجرائم السيبرانية منها الأفريبول كهيئة اقليمية لمكافحة الجريمة (أولا)، دون اغفال اتفاقية بودابست التي كان لها الفضل في مكافحة جرائم تقنية المعلومات(ثانيا)، ثم المجلس الاوروبي كهيئة مساهمة (ثالثا).

[1] مراد مشوش، مرجع سابق، ص 709

اولا: الأفريبول كهيئة اقليمية لمكافحة الجريمة

وتعرف بمنظمة الشرطة الجنائية الافريقية، تم انشاءها بمبادرة من الدولة الجزائرية وتضم قوات الشرطة ل 41 دولة، حيث يعتبر آلية أنشئت من أجل مضاعفة رصيد التعاون الشرطي في الدول الإفريقية على المستويات الاستراتيجية والعملياتية والتكتيكية بين مؤسسات الشرطة في إفريقيا ، ولمنع الجريمة العابرة للحدود الوطنية والجريمة السيبرانية والكشف عنها والتحقيق فيها بالتعاون مع مؤسسات الشرطة الإقليمية والدولية [1].

كما تعمل على اعادة تأهيل مختلف أجهزة الشرطة الافريقية وتعزيز قيم السلم والأمن في القارة. بالإضافة الى ايجاد الحلول للجرائم التي تواجهها افريقيا

ثانيا: اتفاقية بودابست لمكافحة جرائم تقنية المعلومات

وتعد الأولى في مجال مكافحة جرائم الانترنت وقد ابرمها المجلس الاوروبي في 2001/11/08 وشملت العديد من جرائم الانترنت منها: الإرهاب، تزوير بطاقات الائتمان، دعارة الأطفال وتعمد الاتفاقية إلى تنسيق القوانين الجديدة في دول عديدة، وجاءت نتيجة مشاورات طويلة بين الحكومات واجهزة الشرطة وقطاع الكمبيوتر وصاغ نصها عدد من الخبراء في مجلس أوروبا بمساعدة عدة دول منها الولايات المتحدة.

علاوة على ذلك، فقد حددت الجرائم التي يجب أن تتضمنها التشريعات الوطنية للدول الأعضاء وتتلخص هذه الجرائم في الجرائم المعلوماتية كما هو الشأن في الاختلاق والانتحال والنصب والاحتيال المعلوماتي، الجرائم المتعلقة بأمن الشبكات والمراقبة غير

---

[1] خضرة شنيتر، مرجع سابق، ص 244.

[2] جمال براهيمي، اليات التحقيق في الجريمة الالكترونية، اطروحة لنيل شهادة الدكتوراه في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2018، ص 30818 .

المشروعة والعدوان على الثقة في البيانات أو على النظام والإساءة إليه، كذلك جرائم الأخلاق مثل إنتاج أو بث أو حيازة ما يتعلق بدعارة الأطفال. [1]

ثالثا: المجلس الاوروبي كهيئة اقليمية

لقد ساهم المجلس الاوروبي بنسبة كبيرة في مكافحة الجريمة السيبرانية خاصة بعد تتويجه عند اصداره لاتفاقية بودابست لمكافحة الجرائم المعلوماتية، اضافة الى هذا فقد عمل على دعم و تعزيز عمل الجهات المختصة كأجهزة الشرطة المختصة والاجهزة القضائية وهذا ما أكدته ورشة عمل المجلس في 2010 حيث نصت على:

*دعم الطابع الدولي لاتفاقية بودابست.

*تكوين رجال قضاء مختصين في هذا المجال.

*تكثيف الجهود لردع جرائم استغلال القصر جنسيا عبر الشبكة[2]

المطلب الثاني

جهود الدول العربية لمكافحة الجرائم السيبرانية

لقد اعتبرت الجهود العربية في مجال دعم وترقية طرق التعاون فيما بينهم من اجل مكافحة الجرائم السيبرانية جهودا اقل من الجهود الاوروبية ، حيث أدى رواج المعلومات في كل الدول العربية إلى ظهور عدة ممارسات إجرامية في هذا النطاق مما حذا بهذه الدول إلى المحاولة لإيجاد سبل تشريعية ناجعة لمواجهة هذا النوع من الجرائم المستجدة، غير انه كانت في البداية تتمحور حول مواجهة الجرائم الماسة بحق المؤلف على اساس عدم انتشار هذه الجرائم بعد في القطر العربي. لكن بعد الانتشار الرهيب لهذه الظاهرة اتخذت التشريعات العربية عدة سبل لردعها فنجد مثل القانون العربي الاسترشادي لمكافحة الجريمة السيبرانية (الفرع الاول)، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات (الفرع الثاني).

---

[1] سليمان قطاف، مرجع سابق، ص ص 79،80.

[2] حسين ربيعي، اليات البحث والتحقيق في الجرائم المعلوماتية، اطروحة مقدمة لنيل الدكتوراه في العلوم القانونية، تخصص قانون العقوبات، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، 2015، ص 139.

الفرع الاول :

القانون العربي الاسترشادي لمكافحة الجريمة السيبرانية

صدر عن جامعة الدول العربية قانونا استرشاديا لمكافحة جرائم تقنية الفضاء السيبراني، حيث سعت الدول العربية لتجريم الأعمال الغير مشروعة المرتكبة من خلال استخدام الفضاء السيبراني بالتوقيع على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لتعزيز التعاون بين الدول العربية لمكافحة الجرائم السيبرانية لعام 2010 والحفاظ على أمنها وسلامتها[1].

وقد نتج هذا القانون كثمرة عمل مشترك بين مجلس وزراء الداخلية العرب ومجلس وزراء العدل العرب ، وقد تضمن القانون الاسترشادي الخاص بمكافحة هذه الجرائم مجموعة من المواد نصت على الزامية حماية حياة الاشخاص الخاصة من الاعتداءات التي تقع عليها الانظمة المعلوماتية وذلك في المواد 161-163، كما جرمت المادة 464 منه أفعال الدخول عن طريق الغش للنظام المعلوماتي وعرقلة سير نظام التشغيل بالإضافة الى تجريم تزوير وثائق المعالجة الالية وتغيير وتعديل المعلومات فيه.[2]

الفرع الثاني:

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

لقد ساهمت هذه الاتفاقية بشكل كبير في ردع جرائم تقنية المعلومات على المستوى العربي بمساهمة وموافقة عدة دول، مما استوجب الوقوف على تعريفها (اولا)، ثم الجرائم التي تناولتها الاتفاقية (ثانيا).

---

[1] سليمان قطاف، مرجع سابق، ص 81.

[2] عبد الرزاق منذر، مدى الحماية الجنائية للمعلومات عبر الحاسوب والانترنت (دراسة مقارنة)، اطروحة لاستكمال نيل الدكتوراه في فلسفة القانون، كلية القانون، جامعة عمان العربية، عمان، 2012، ص 135 .

اولا: تعريف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

عرفت اتفاقية فينا لقانون المعاهدات الاتفاقية بأنها عبارة عن "اتفاق دولي يعقد بين الدول في صيغة مكتوبة والذي ينظمه القانون الدولي، سواء تضمنته وثيقة واحدة أو وثيقتان متصلتان أو أكثر ومهما كانت تسميته الخاصة". مما سبق يمكن تعريف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بأنها الاتفاق الدولي الإقليمي المعقود بين الدول العربية في نطاق جامعة الدول العربية بصورة خطية في أكثر من وثيقة والذي وافق عليه مجلس وزراء الداخلية والعدل العرب في اجتماعهما المنعقد في مقر الأمانة العامة لجامعة الدول العربية في 2010 بالقاهرة وسمي "الاتفاقية العربية لمكافحة جرائم تقنية المعلومات" و تتكون من ديباجة و 43 مادة مقسمة في 5 فصول.[1]

ثانيا: الجرائم التي تناولتها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

لقد تناولت هذه الاتفاقية الجرائم التي تستهدف نظام ووسائل تقنية المعلومات و الجرائم التي ترتكب باستعمال تقنية المعلومات، و يتم تفصيلهما فيما يلي:

1- الجرائم التي تستهدف نظام ووسائل تقنية المعلومات

نصت الاتفاقية محل البحث عن الجرائم التي تستهدف تقنية المعلومات في المواد 06إلى 11منها حيث تطرقت في المادة 06 الى جريمة الدخول الغير المشروع للنظام دون رضا المسؤول عنه اما للاطلاع او التسلية و جعلها كهواية لاختراق الانظمة الحاسوبية.[2]

كما تضمنت المادة 08 منها جريمة الاعتداء على سلامة البيانات وتتحقق هذه الجريمة عند القيام بمحو البيانات والمعلومات كليا وتدميرها إلكترونيا او تشويه البيانات

---

[1] احمد حمي، زهيرة كيسي، صور جرائم تقنية المعلومات وفقا للاتفاقية العربية لسنة 2014، مجلة العلوم القانونية والسياسية، جامعة تامنغست، مج 10،ع1،2019 ص778

[2] محمد خليفة، (خصوصية الجريمة الإلكترونية وجهود المشرع الجزائري في مواجهتها)، دراسات وابحاث، جامعة زياني عاشور الجلفة ، ع01، مج01، ص 370

والمعلومات أو البرامج عن طريق إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدا وبدون وجه حق.

اما المادة 09 منها نصت على أن جريمة إساءة استخدام وسائل تقنية المعلومات تتحقق متى كان إنتاج أو بيع أو شراء أو استيراد أو توزيع أو توفير أدوات أو برامج مصممة أو مكيفة لغايات ارتكاب الجرائم السابقة او حيازتها بغرض ارتكاب هذه الجرائم.

اما بخصوص المادتين 10 و11 فقد نصتا على جريمتى التزوير والاحتيال، ففي التزوير اشترطت الاتفاقية ان يكون بغرض تغيير الحقيقة؛ أما الاحتيال فيتحقق بمحو البيانات او تعطيل الانظمة الالكترونية[1].

2- الجرائم التي ترتكب باستعمال تقنية المعلومات:

لقد تطرقت لها الاتفاقية في المواد من 12 الى 18 حيث نصت المادة 12 على الجريمة الاباحية بشتى انواعها من افلام وصور... وذلك الواقعة على القصر، وجريمة الاستغلال الجنسي جرمت بمقتضى المادة 13 منها والذي يكون نتيجة الاتجار بالنساء، اما المادة 14 فقد نصت على جريمة انتهاك حرمة الحياة الخاصة عند نشر صور الاشخاص او معلوماتهم، والمادة 15 جرمت الجرائم المتعلقة بالإرهاب عن طريق تقنية المعلومات مثل نشر أفكار ومبادئ جماعة إرهابية والدعوة لها او نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية او عن طريق نشر النعرات والفتن ولاعتداء على الاديان والمعتقدات[2].

اما المادة 16 فقد جرمت في فقراتها الاتجار بالأشخاص والاعضاء البشرية مثلما تناولها المشرع الجزائري في قانون العقوبات، والمادة 17 نصت على الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة مثل بيع او تصدير نسخ مقلدة، واخيرا جريمة الاستخدام غير

---

[1] احمد حمي، مرجع سابق، ص ص 783،784.

[2] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المبرمة بين الدول العربية في القاهرة بتاريخ 21 ديسمبر 2010، وصادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 14-252 مؤرخ في 08 سبتمبر سنة 2014 ، (ج.ر.ج.ج.ع57).

المشروع لأدوات الدفع الإلكترونية مثل البطاقات الذكية اما بالتزوير او اصطناع أو وضع أي اجهزة أو مواد تساعد على تزوير أو تقليد أي أداة من أدوات الدفع الإلكتروني بأي وسيلة كانت وهذا بنص المادة 18 من الاتفاقية.[1]

[1] انظر المواد 16،17، 18 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

خاتمة

وختاما لهذه الدراسة المعنونة تحت **"جرائم اختراق الامن السيبراني في التشريع الجنائي المقارن"** توصلت الى أن الجرائم السيبرانية او المعروفة بالجريمة المعلوماتية أنها من أكثر الجرائم التي عرفها العالم الحديث خطورة، وذلك لما تتسم به هذه الجريمة من اختلاف عن الجرائم المعروفة في العالم التقليدي، بالإضافة إلى التحديات التي فرضتها على الجهات الخاصة بوضع القوانين وانفاذها ؛ولقد واكب المشرع الجزائري ولو بقدر قليل الحركية التشريعية التي فرضت نفسها عالميا، خاصة مع دخول الإنترنت في مختلف مناحي حياة المواطن الجزائري، فبعد الفراغ التشريعي الذي كانت تعاني منه الجزائر في هذا المجال سعت لسده في بادئ الأمر بتعديل قانون العقوبات وذلك بالقانون رقم 15/04، ولعدم كفاية هذا المشرع الجزائري إلى إصدار قانون خاص والمتمثل في القانون رقم 04/09 والمتضمن القواعد الخاصة بالوقاية القانون دفع الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ولم يكن هذين القانونين الوحيدين في هذا المجال بل كانت هناك محاولات أخرى خاصة في قوانين الملكية الفكرية مثل قانون حماية حق المؤلف والحقوق المجاورة، غير أن بالرغم من هذه المحاولات يبقى المشرع الجزائري بعيدا كل البعد عن التطور القانوني على المستوى العالمي من جهة، وعن تطور أساليب ارتكاب الجريمة عبر الإنترنت مما يستلزم مراجعة وتطوير القوانين القائمة ،ومن جهة اخرى اصدار المزيد من القوانين لتقوية والترسانة القانونية في هذا المجال.

أما فيما يخص الجهود الإقليمية فتمثلت في جهود الاتحاد الأوربي الذي يعتبر الإطار الأنجع لمكافحة الجريمة المرتكبة عبر الإنترنت خاصة بعد إبرام اتفاقية بودابست في 2001 والتي كان لها الفضل في مكافحة الجرائم السيبرانية على المستوى الدولي، أما على المستوى العربي الوطني فبالرغم من قلة المجهودات التي بذلتها الدول العربية الا انها كانت ناجعة ورائدة تمكنت من ردع هذه الظاهرة الاجرامية الخطيرة..

التوصيات:

من خلال ما تقدم سابقا توصلت الى بعض التوصيات والتي قد تساهم بحد كبير في المساعدة على القضاء على الجريمة السيبرانية:

ضرورة تكوين قضاة التحقيق في مجال الجرائم المعلوماتية في معاهد متخصصة*

*ضرورة تنظيم حملات توعوية لمستعملي الوسائط المعلوماتية و تعريفهم بحجم الخطورة التي تترصدهم في حالة عدم اتخاذ الاحتياطات الوقائية اللازمة عند استعمالهم لها.

* وضع التعاون الدولي لمكافحة الجرائم الدولية هدفا أسمى وأرقى عن تحقيق مصالح شخصية للدول

* تفعيل العمل والعلاقات الدبلوماسية بشكل مكثف، ليعمل على توطيد أواصر التعاون بين البلدان، وتقريب وجهات النظر.

* ضرورة تدريب وتأهيل أفراد الضبطية القضائية على كيفية التعامل مع هذا النوع من الجرائم بعقد دورات تكوينية بشكل دائم

قائمة المصادر والمراجع

قائمة المراجع

➢ الكتب باللغة العربية :

1. احمد خليفة الملط، الجرائم المعلوماتية، طبعة 2، دار الفكر الجامعي، الاسكندرية،، 2006.

2. أمال قارة: الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر،2006.

3. خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، طبعة 1 ،. دار الفكر الجامعي، الاسكندرية،، 2009.

4. سعاد عاطف عبد المطلب حسنين، الحماية الجنائية للمصنفات الرقمية، طبعة اولى،دار الفكر الجامعي، 2018.

5. عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة دراسة في الظاهرة الاجرامية المعلوماتية ، طبعة اولى ، دار الفكر الجامعي، الاسكندرية،،2010.

6. علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، دراسة مقارنة، دار النشر والتوزيع، منشورات زين الحقوقية، 2013.

7. علي حسن طوالبة، الجرائم الالكترونية، ط1، مطبوعات جامعة العلوم التطبيقية ،2008.

8. محمد أمين الشوابكة، جرائم الحاسوب والانترنت (الجريمة المعلوماتية)، د.ط، دار الثقافة والنشر والتوزيع، 2001.

9. محمد عبد الله ابو بكر سلامة، جرائم الكمبيوتر والانترنت، د.ط، منشأة المعارف، الاسكندرية،2006.

10. محمد علي العريان، الجرائم المعلوماتية، د.ط، دار الجامعة الجديدة، الاسكندرية، مصر، 2011.

11. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة، القاهرة،،طبعة 1، 2009.

12. يزيد بوحليط، الجرائم الالكترونية والوقاية منها في القانون الجزائري، طبعة 1، دار الجامعة الجديدة، الجزائر، 2019.

➢ **الرسائل العلمية :**

1. أسامة مهمل، الاجرام السيبراني، مذكرة لنيل شهادة الماستر اكاديمي، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، مسيلة،2017

2. حسين ربيعي، اليات البحث والتحقيق في الجرائم المعلوماتية، اطروحة مقدمة لنيل الدكتوراه في العلوم القانونية، تخصص قانون العقوبات، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، 2015.

3. حمزة بن عقون، السلوك الاجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير ، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2011.

4. خضرة شنيتر، الاليات القانونية لمكافحة الجريمة الالكترونية(دراسة مقارنة)، اطروحة لنيل شهادة الدكتوراه طور ثالث، تخصص جنائي، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، 2020.

5. دلال ملياني، اشكالية الاثبات في جرائم الانترنت في التسريع الجزائري، اطروحة لنيل شهادة الدكتوراه تخصص قانون خاص، كلية الحقوق والعلوم السياسية، جامعة ابوبكر بلقايد، تلمسان، 2017.

6. رجاء أمدور: خصوصية التحقيق في مواجهة الجريمة المعلوماتية، أطروحة لنيل شهادة دكتوراه، قانون خاص،كلية الحقوق والعلوم السياسية، جامعة البشيرالابراهيمي، برج بوعريريج، 2020.

7. رزيقة بونار ،الجريمة المعلوماتية في التشريع الجنائي الجزائري ،مذكرة لنيل شهادة الماستر ،قانون عام ،قسم الحقوق، كلية الحقوق، جامعة بن يحي محمد الصديق ،جيجل ،2020.

8. صغير يوسف:الجريمة المرتكبة عبر الانترنت،مذكرة لنيل شهادة ماجستير في القانون الدولي للأعمال،كلية الحقوق والعلوم السياسية،جامعة مولود معمري،تيزي وزو ،2013،

9. عبد الرزاق منذر، مدى الحماية الجنائية للمعلومات عبر الحاسوب والانترنت (دراسة مقارنة)، اطروحة لاستكمال نيل الدكتوراه في فلسفة القانون، كلية القانون، جامعة عمان العربية، عمان.

10. عزيزة رابحي ،الاسرار المعلوماتية و حمايتها الجزائية ،مذكرة لنيل شهادة الدكتوراه،قانون خاص ،كلية الحقوق والعلوم السياسية، جامعة ابو بكر بلقايد،تلمسان،2017.

11. محمد بوعمرة، جهاز التحقيق في الجريمة الالكترونية في التشريع الجزائري،مذكرة تخرج لنيل شهادة الماستر في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة محند اولحاج، البويرة،2019

12. -منال لبيض, الحماية الجزائية و المدنية من الجريمة المعلوماتية في التشريع الجزائري ,مذكرة لنيل شهادة الماستر, قانون أعمال, كلية الحقوق و العلوم السياسية, جامعة سطيف, 2015,

13. نبيلة هبة هروال .جرائم الانترنت، دراسة مقارنة، اطروحة دكتوراه.، كلية الحقوق والعلوم السياسية. جامعة ابي بكر بلقايد، تلمسان.2013.

14. نسيم دردور،جرائم المعلوماتية على ضوء القانون الجزائري و المقارن ،مذكرة نيل شهادة الماجيستير، كلية الحقوق والعلوم السياسية ، جامعة منتوري ، قسنطينة ،2012،

15. وردة لقديم: الجريمة الالكترونية في التشريع الجزائري، مذكرة مكملة من مقتضيات نيل شهادة الماستر في الحقوق، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف، 2017

➢ المجلات العلمية والدراسات:

1. احمد حمي، زهيرة كيسي، صور جرائم تقنية المعلومات وفقا للاتفاقية العربية لسنة 2014، مجلة العلوم القانونية والسياسية، جامعة تامنغست، مج 10،ع1،2019

2. ايهاب خليفة ،الأمن السيبراني الماهية و الإشكاليات ، مركز مستقبل الأبحاث والدراسات المتقدمة ،أبو ظبي.

3. جمال الدين دندن، الاستراتيجية الامنية للدولة الجزائرية في مكافحة الجرائم السيبرانية، مجلة صوت القانون، جامعة الجزائر1، مجلة 07،ع 02،2020.

4. حكيمة بوكحيل، الهيئة الوطنية للوقاية من جرائم الإعلام وتكنولوجيا الاتصال ودورها في تفتيش نظم المعلوماتية،مجلة الدراسات القانونية المقارنة، جامعة سوق أهراس، مج 07، ع 01، 2020

5. ذبيح عماد، سمية بهلول،الآليات العقابية لمكافحة الجريمة الالكترونية في التشريع الجزائري مجلة الحقوق والعلوم السياسية، عدد 13، 2020.

6. سالم سمير المرعي، الجرائم المعلوماتية و جريمة الاحتيال عبر الشبكة، بحث مقدم لنيل لقب أستاذ في المحاماة، سوريا،2019.

7. سليمان قطاف، مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية، مج 05، ع 02،2022.

8. سورية ديش، انواع الجرائم الالكترونية و اجراءات مكافحتها، مجلة العلوم السياسية و القانون،عدد اول، 2017

9. صالح شنين، التسرب في القانون الجزائري حماية للنظام العام والحريات ام حماية للنظام، المجلة الجزائرية للقانون المقارن، جامعة عبد الرحمن ميرة بجاية، ع 2.

10. عبد الحليم بن بادة ، "المراقبة الالكترونية كإجراء لاستخلاص الدليل الالكتروني" بين الحق في الخصوصية ومشروعّية الدليل الالكتروني المجلة الأكاديمية للبحث القانوني، جامعة غرداية، مج 10، ع03.

11. عبد الرؤوف زيوش، الجريمة المعوماتية في التشريع الجزائري، مجلة العلوم القانونية و الاجتماعية، جامعة زيان عاشور الجلفة، عدد03، 2019.

12. عبدالله بن عبدالعزيز بن فهد العجلان، المؤتمر الدولي حول حماية امن المعلومات و الخصوصية في قانون الانترنت، القاهرة.

13. لامية طالة، التهديدات و الجرائم السيبرانية: تأثيرها على الأمن القومي للدول و استيراتيجيات مكافحتها، مجلة معالم للدراسات القانونية و السياسية،مجلد4،عدد 03، 2020.

14. محمد خليفة، (خصوصية الجريمة الإلكترونية وجهود المشرع الجزائري في مواجهتها)، دراسات وابحاث، جامعة زياني عاشور الجلفة ، ع01، مج01.

15. مراد مشوش، الجريمة المعلوماتية في ظل قانون العقوبات وقانون الوقاية من جرائم تكنولوجيات الاعلام والاتصال، مجلة القانون، جامعة غرداية، مج09،ع 01،2020

16. مهدي رضا: الجرائم السيبرانية واليات مكافحتها في التشريع الجزائري،مجلةايليزا للبحوث والدراسات، مجلد06،العدد02، 2021.

17. ناصر اوقاص،الطبيعة القانونية للجرائم المستحدثة و وسائل ارتكابها ،مجلة البحوث القانونية و السياسية ، مجلد3 عدد 16، 2020.

➢ المحاضرات:

1. أمينة معزيز،التسرب في قانون الاجراءات الجزائية الجزائري،كلية الحقوق والعلوم السياسية، جامعة مستغانم.

2. رامي حليم، محاضرات موجهة لطلبة الدكتوراه، مقياس القانون الجنائي و التكنولوجيا الحديثة.

3. رحيمة نمديلي، الطبيعة القانونية للجريمة السيبرانية في القانون الجزائري والقوانين المقارنة, كلية الحقوق والعلوم السياسية ، جامعة سطيف 2.

➢ تقارير والمواثيق الدولية

1. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المبرمة بين الدول العربية في القاهرة بتاريخ 21 ديسمبر 2010، وصادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 14-252 مؤرخ في 08 سبتمبر سنة 2014 ، (ج.ر.ج.ج.ع57).

2. الامر 156/66 المؤرخ في 8يونيو 1966 ، المعدل و المتمم و المتضمن قانون العقوبات (ج.ر ع 49).

3. الاتفاقية الدولية حول الاجرام المعلوماتي أبرمت بتاريخ:2001/11/08 من طرف المجلس الأوروبي

4. القانون 15/04 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم للأمر 156/66 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات. (ج.ر ع 71).

5. اتفاقية بودابست لمكافحة الجريمة المعلوماتية الموقعة في 23 نوفمبر 2001 مصادق عليها في بودابست عاصمة المجر

➢ المواقع الاكترونية :

1. HTTPS//:droit7.blogspot.com2
2. HTTPS//:droit7.blogspot.com
3. HTTPS//www.tribunaldz.com
4. https//www.antiextortion.com
5. https://www.mohamah.net
6. https://www.droitetentreprise.com
7. https://pulpit.alwatanvoice.com
8. https://www.mohamah.net/

فهرس

المحتويات

الفهرس

ملخص:

في ظل التطور المعلوماتي الذي شهده العالم بأكمله والذي انعكس على اشكال الجريمة وخلق للشعوب طريقا للتواصل فيما بينها يسمى بالفضاء السيبراني، فبهذا تعاظمت الهجمات السيبرانية داخل هذا الفضاء مما اصبح يهدد الامن القومي للدول و يستهدف نظامهم الاقتصادي والعسكري وحتى حياة شعوبهم الخاصة؛ مما استلزم تظافر الجهود الدولية للقضاء على هذه الجريمة. وحذا المشرع الجزائري حذو التشريعات الدولية لكن يبقى بعيدا عن دائرة الردع .

الكلمات المفتاحية: الفضاء السيبراني، الهجمات السيبرانية، الامن القومي، الردع.

Resumé:

À la lumière du développement de l'information dont a été témoin le monde entier, qui s'est reflété dans les formes de criminalité et a créé pour les peuples un moyen de communiquer entre eux appelé le cyberespace, ce qui a entraîné une augmentation des cyberattaques dans cet espace, ce qui menace la sécurité nationale. des pays et vise leur système économique et militaire et même la vie de leurs propres peuples ; Cela a nécessité des efforts internationaux concertés pour éradiquer ce crime. Le législateur algérien a suivi la législation internationale, mais reste loin du cercle dissuasif.

Mots Clés : Cyberespace, cyberattaques, sécurité nationale, dissuasion.

Abstract:

In light of the information development witnessed by the entire world, which was reflected in the forms of crime and created for peoples a way to communicate with each other called the cyberspace. With this, cyber attacks increased within this space, which threatens the national security of countries and targets their economic and military system and even the lives of their own peoples; This necessitated concerted international efforts to eradicate this crime. The Algerian legislator has followed the lead of international legislation, but remains far from the deterrent circle.

Mots clés : Cyberspace, cyber attacks, national security, deterrence.