جامعة عبد الرحمان ميرة-بجاية-
كلية الحقوق والعلوم السياسية
قسم القانون الخاص

الاختلاس في البيئة الرقمية في القانون الجزائري

مذكرة مقدمة لنيل شهادة الماستر في الحقوق

تخصص القانون الجنائي والعلوم الجنائية

من إعداد الطالبة

لعلاوي صبرينة

تحت إشراف الأستاذة

تواتي نصيرة

أعضاء لجنة المناقشة

الأستاذة هارون نورة أستاذة محاضرة قسم أ، جامعة بجاية ---------- رئيسا

الأستاذة: تواتي نصيرة أستاذة التعليم العالي، جامعة بجاية ---------- مشرفة ومقررة

الأستاذ بن سليمان محمد الأمين أستاذ محاضر قسم ب، جامعة بجاية ---------- ممتحنا

السنة الجامعية : 2022-2023

La cybercriminalité est la troisième grande menace pour les grandes puissances, après les armes chimique, bactériologique et nucléaires

مقدمة

سهلت تقنيات التكنولوجيا سبل الحياة والتواصل وانتقال المعلومات بين الشعوب، فالعالم كما قيل أصبح قرية صغيرة إلا أنَّ هذا التطور السريع والمذهل لا يخلو من عيوب، حيث اصبحت المجتمعات في الآونة الأخيرة تعاني من ظاهرة إجرامية مستجدة تعرف

بالجريمة المعلوماتية، حيث تنتهك الخصوصية المعلوماتية للأفراد والمؤسسات وتمس بأمن والاستقرار الدولي مما تتجاوز الحدود الإقليمية.

حيث خلق الفضاء الالكتروني فرص جديدة للمجرمين بتفحص الانترنت لارتكاب جرائم عديدة كالقرصنة المعلوماتية، الاحتيال بواسطة البطاقات الائتمانية، اختراق المواقع الالكترونية وأنظمة الحواسيب، كما أنَّ هذه الجريمة يختلف مرتكبوها عن مجرمي الجرائم المادية، فالمجرم المعلوماتي فائق الذكاء المسمى بـ محترف جرائم المعلومات والاتصالات يرتكب جرائمه بمنأى عن المراقبة والمتابعة.

حاول المشرع الجزائري على غيره من التشريعات المقارنة في التصدي على الجرائم المعلوماتية من خلال سن وتعديل نصوص قانون العقوبات بإدخال قواعد تجريمية جديدة يتم على تعقب الأفعال الجنائية المرتبطة بأنظمة المعلوماتية بينما أنشئ القطب الجزائي بغية الفصل في القضايا ذات الصلة بتكنولوجيا المعلومات والاتصال. فالجزائر من الدول التي عرفت في السنوات الأخيرة بارتفاع مؤشر هذه الجرائم على نطاق ملموس.

الإجرام المعلوماتي لم يتخذ في الدولة الجزائرية والوطن العربي بعدًا كالذي اعتاده الدول المتقدمة التي تحظى على اهتمام متزايد من حكومات الدول إلا أن ذلك لا ينفي ضرورة التصدي لبوادر تلك الآفة مادام أمامنا عصر العولمة الرقمية والجزائر ليست بعيدة عن ذاك النوع من الإجرام الذي تجاوز النطاق الإقليمي على الدولة على هذا الأساس قامت بسن القوانين الجنائية لمحاربة المعلوماتية.

تتجلى أهمية البحث المستمر في الجرائم المعلوماتية على ذاك النوع المستجد مرتبط بالتقنية العالية المتمثلة في الحاسب الآلي وشبكة الانترنت التي باتت في تطور دائم، مما يفرض على المشرع الجنائي مواكبة الظاهرة مع إيجاد الحلول التشريعية لمكافحتها مع الاكتفاء على القواعد التقليدية التي مازالت قاصرة من الناحية الموضوعية باعتبار الاجرام المعلوماتي يطال حقوقًا غير مادية بينما الناحية الاجرائية ما تثير من عقبات تتمحور على الاثبات الجنائي، حتمية التعاون الدولي القضائي لاسيَّما تنازع الاختصاص، بينما تدارك المشرع على الثغرات القانونية إلى غاية 2004 الذي صدر فيها القانون 04ـ 15 المتعلق بتعديل قانون العقوبات بغية تفعيل الحماية الجزائية على الأنظمة المعلوماتية من القراصنة الذي تم تعزيزه بمقتضى القانون 09ـ 04 على الرغم من اصدار تلك القوانين فلا ينبغي القول باكتمال البنية التشريعية في مجال المكافحة.

من المؤكد على البحث في المجال المعلوماتي قد يعترض على عقبات تحول من الطابع القانوني إلى التقني التي تتبين في الإلمام على المصطلحات التقنية الدالة بالأجهزة الحوسبية مع تأثير الفيروسات من تخريب النظم المعلوماتية ضف إلى الخطوات المتبعة لإثبات الجريمة تحتم على الباحث للاختيار بعناية فائقة مصدر المعلومات التقنية القانونية، أما بالنسبة إلى دور التشريعات الجنائية الوطنية الدولية في الحد من الجريمة المعلوماتية ذات بعد دولي عائقًا أمام السلطات القانونية في تكثيف بوادر مأمولة من خلال اتباع الوسائل الأمنية مع التدابير الوقائية دون المساس بالحريات الفردية عند تبادل المعلومات عبر الشبكة الآلية.

من خلال الدراسة المعالجة قد توصلنا إلى طرح إشكالية البحث التالية: ما مدى فعالية السياسة الجنائية في تكريس الحماية الجنائية على الاختلاس؟

ارتأينا ان نعالج الإشكالية وفق المنهج التحليلي النقدي المقارن حتى يتسنى علينا إجراء دراسة هادفة إلى نتائج تقييمية جادة بغية انتقاء حلول قانونية وقائية على مجال المكافحة بينما الميدان العملي لابد من تشجيع البحث في تطوير الآليات الممارسة التقنية من تطويق الإجرام.

بناءً على ذلك نستهل دراستنا على خطة منهجية متبعة إلى قسمين الذي قد تناولنا في الفصل على الإطار التقني القانوني للنظام المعلوماتي بينما أشارنا إلى الفصل الثاني على الإطار الإجرائي التطبيقي في البيئة الرقمية.

الفصل الأول
الإطار التقني القانوني للنظام المعلوماتي

النظام المعلوماتي قاطرة العبور للمعاملات المالية، الصفقات الاقتصادية، المستَّندات الشخصية التي تتجلى بالمرونة والثقة أثناء الاستخدام دون استغلالها لأهداف غير مشروعة، حيث تُمثل كتلة ضخمة من البيانات المخزَّنة التي يتم استقبالها من إدارة المعلومات في هيئة أُتوماتيكية متكاملة تحت تعليمات نظام تشغيل الحاسب الآلي.

إذ يُستهل علينا الولوج للطبيعة التقنية الذي طالما يبدو بعيدًا عن لغة القانون، مما يقتصر الاستعانة بالخبراء المؤهلين في ميدان التكنولوجيا الرقمية حتى يتسنى لنا الدراية بالبرهنة دون تفحص خوارزميات الشبكة العنكبوتية في الإطار الفني بل يكفي تِبْيان الباحث مهمة الكشف والتعقيب عن الآليات التي تطال على مؤشرات الإجرام من حيث الغموض الذي يحتوي بذاته، فلا تترك أيُّ بصمات مرئية الناتجة عن حوافز هاتيه التقنية المتسارعة سواء ماديًا أو معنويًا، لكي لا تظل الرؤية ضبابية للإفصاح عنها والتي اصطبغت على تسمية الإجرام المعلوماتي، بينما يتعذَّر الإثبات عن ملابساتها كون التعامل مع ملفات الكمبيوتر تجتاز من عدة عمليات تحويليَّة لنظام التشغيل الحاسب الآلي التي تسري على حدود دولية عابرة مما يقتضي التعرض إلى خصوصية النظام الآلي من أجل الفهم والإتقان بمنأى دقيق عن التركيبات النموذجية لممارسة هذه الأساليب المبتكرة.

حيث تُطرح إشكالات معقدة من إرسال، تخزين، حماية، معالجة، استعادة المعلومات لأجل تفكيك اللغز يرجع الأمر إلى أخصائي علم الحوسبة قادرين على إيجاد حلول سليمة راجحة، ثم يأتي دور القانون والقضاء بالوقوف على المسائل المثارة من خلال دراسة متأنية لأنماط تلك الجرائم مع استعراض دوافع التلاعب أو السطو على الأنظمة المعلوماتية.

بناءً على ضوء هذه المعطيات تم تقسيم الفصل إلى مبحثين الجانب الموضوعي للشبكة المعلوماتية الرقمية **(المبحث الأول)**، أشكال الاعتداء على النظام الآلي **(المبحث الثاني)**.

المبحث الأول
الجانب الموضوعي للشبكة المعلوماتية الرقمية

الإجرام المعلوماتي سلاح تقني هاجس قد يقرع إلى أجراس الخطر وتنويهًا على مجتمعاتنا من حجم الخسائر المتكبّدة بالخصوص هي جرائم لبيبة تـُولَّد في بيئة رقمية و تُقترف عادةً من محترفي شبكات النظم المعلوماتية، إذ يستحيل باعتباره شخصاً عادي بسيط أو جاهلاً للأليات التقنية الحديثة، مما يمتلكون أدوات صارمة على المعرفة التقنية العالية و اكتساب مواهب بحذاقة، كما يُستلهم كافة المستويات الاقتصادية، الاجتماعية، الثقافية، الأمنية من خلال اسهامات تسارع معدلات التكنولوجيا في مجال نظم المعلومات و الاتصال، فالإغراء عن تحديات جرائم الحاسبات الالكترونية يتطلب أولاً إعطاء وصفًا شاملاً لتحديد المفاهيم الأصلية على تقنية الحاسب الآلي ثم الولوج للناحية القانونية من أجل إبراز موضوعات الجريمة المعلوماتية سواء تعلق الامر بالطبيعة، الخصوصية، الدوافع، الانعكاسات.

حيث يتعذَّر الاتفاق على تعريف مشتَّرك ومتجانس من خلال تنافي الآراء الفقهيَّة، يرجع الأمر إلى سرعة وتيرة للتقنية وتفاوت الدور الذي تلعب على الانظمة المعلوماتية، لذلك قد تقع محلاً للجريمة تارة ووسيلة للارتكاب فكلما كان البحث منصبًا على جرائم النظام المعلوماتي بحد ذاته باتت محلاً للاعتداء ومن زاوية معاكسة إذا كان البحث عن دراسة الجرائم التي ترتكب باستخدام التقنية المعلوماتية استنَّد التعريف على الوسيلة آلة في دعم الإجرام

إذ يجدر بنا الحديث عن الطبيعة القانونية للجريمة المعلوماتية الذي يدار ضمن نطاق المعالجة الآلية للمعطيات المتصلة بشبكة المعلومات، ثم نعرج للدراسة عن المجرم المعلوماتي من خلال تنفيذ مساعي الجريمة بما في ذلك التغلب على تقنيات الحماية المؤمنة لأنظمة الكمبيوتر وعمليات اختراق البرامج المحصنة، مما يتسم بالخبرة وفائق الذكاء ذلك مفتاح للغوص في ثغرات الإجرام خلافًا عن المجرم العادي فلا يلجأ للعنف والاستفحال بل يتحدى القدرة الذاتية والمنافسة على الأنظمة الآلية داخل الفضاء الافتراضي لذا سنحاول الإلمام على فحوات الموضوع بالتحليل والإيجاز دون الاطناب مع الوقوف على المقاييس الركيزة للبحث.

للإحاطة على ذلك يتجلى لنا التطرق إلى التعريف التقني للحاسب الآلي **(المطلب الأول)**، ثم تحديد الطبيعة القانونية للجريمة المعلوماتية **(المطلب الثاني)**، بعد ذلك نخوض للحديث عن المجرم المعلوماتي **(المطلب الثالث)**.

المطلب الأول

التعريف التقني للحاسب الآلي

الحاسب الآلي حصيلة للاختراعات العلمية التقنية التي رصدت أبعاد لكافة أهداف الأنشطة الراهنة من الخدمات الطبية، الهندسية، التكنولوجية، بالإضافة إلى استجابة للاحتياجات الشخصية بلا استثناء الأمر الذي أدَّى بالدول للاعتماد عليه في المقام الأوَّلي نظرًا لما يحمل في طياتها من أهميَّة حقيقيَّة، ما يثبت ذلك السمات التي يمتَّاز بها من خلال سرعة في الإنجاز و سعة التخزين كذلك الدقة والموثوقيَّة، إذ يقتصر على الجهد والوقت و تقليص التكاليف الهائلة، مما بات شرايين يوافد كافة الأعمال ومعيارًا بناءً لا غنى عنه في الوقت الحاضر، حيث ندرك العلة في تواجد هذه الأجهزة عقبةً للتطوُّر التقني الملحوظ الذي نال تشجيعًا على الساحة الدولية، إذ يساعد على تنفيذ مهام متعدَّدة من خلالها حوَّلت العالم من فضاء مرئي إلى صفحة رقمية.

إذ أُطلقت على تسمية الحاسب الآلي سواء الحاسب الإلكتروني، المنظم الآلي، الحاسوب، ذلك باللغة العربية، أما كلمة(computer) باللغة الإنجليزية، بالمقابل كلمة (ordinateur) باللغة الفرنسية، حيث يرمز إليه بالعقل الإلكتروني وآلة تطبيقية ناجعة غير متناهيَّة.

يُعرف الحاسوب بما يلي: **"جهاز إلكتروني مصنوع من تركيبات محدَّدة يتم تأليفها وتوجيهها باستخدام أوامر خاصة من إدارة المعلومات، وذلك بتنفيذ ثلاث عمليات أساسيَّة هي: استقبال البيانات المدخلة (الحصول على الحقائق المجردة)، معالجة البيانات إلى معلومات (إجراء الحسابات ومعالجة المدخلات)، الحصول على النتائج."** [1]

لذا سنحاول خلال هذا المطلب تحديد المقصود بالحاسب الآلي **(الفرع الأول)** ثم نعرج إلى المقصود بالإجرام المعلوماتي **(الفرع الثاني)** بعد ذلك سنشير للتمييز بين الجريمة المعلوماتية عن الجريمة المادية **(الفرع الثالث).**

---

[1] - نعيم مغبغب، حماية برامج الكمبيوتر، (الأساليب والثغرات)، دراسة في القانون المقارن، منشورات الحلبي الحقوقية، بيروت،2006، ص 22.

ـــ تجدر الإشارة حول المفاهيم التقنية الدالة بالحقل المعلوماتي الواردة وفق القانون العربي النموذجي الموحد والتي تتجلى فيمايلي:

البيانات المعالجة آليا: عبارة عن مجموعة البيانات التي يتم إدخالها إلى ذاكرة الكمبيوتر وتحليلها وإجراء العمليات الحسابية المنطقية واستخلاص النتائج وقد يتم تخزينها بهدف الرجوع إليها".

تقنية المعلومات: أداة إلكترونية مغناطيسية كهروكيميائية والتي تستخدم في معالجة البيانات والوظائف التخزينية.

ـ الحاسوب ونظم المعلومات: عبارة عن معدات متصلة ببرامج المعلومات الذي يستطيع المعالجة التلقائية للبيانات إضافة للتخزين والتحويل والاسترجاع من خلال النظام الآلي.

انظر/ ذياب موسى البداينة، الجرائم الإلكترونية، (المفهوم والأسباب)، الملتقى العلمي حول الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية الدولية، كلية العلوم الاستراتيجية، عمان، الأردن، 2014، ص 6.

الفرع الأول
المقصود بالحاسب الآلي (تقنية المعلومات)

لا شك أنَّ الحاسب الآلي تقنية مستأثرة على ميدان الاعمال بالنظر لما تُحقق من صلابة هاشة في الوقت الراهن، رغم ذلك يكاد يرسم بؤرة فاجعة نتيجة إستغلال النظام المعلوماتي لأغراض غير مشروعة أيًّا كان أموالاً، معطيات، برامج، ما يُعرف بالإجرام المعلوماتي، مما بات مصدرًا للذعر داخل الفضاء السيبراني قد يفوق نحو اعتداءات ملوَّنة تلحق بالقيَّم المحمية، إذ غيَّرت المعلوميات العديد من المفاهيم القانونية لاسَّيما المنظومة الجنائية نظرًا إلى الطبيعة الحساسة محلها المعطيات التي يتم إفشائها دون حق قانوني تلقائيا، مالا تتوقع أن تُمنى عليها الملكية الفكرية بمثابة مصنفات رقمية، لذلك تتردد المصطلحات الدالة على الإجرام في البيئة الرقمية فيما يتعلق تقنية المعلومات ابتداء من إساءة استخدام الكمبيوتر، جرائم المعلوماتية، جرائم تقنية العالية، جرائم الهاكرز وصولاً إلى جرائم الأنترنت [2].

حيث اختار المشرع الجزائري تسمية الأنظمة الآلية للمعطيات الواردة في الفصل الثاني" **الجنايات والجنح ضد الأموال"** من القسم السابع مكرر **"المساس بأنظمة المعالجة الآلية للمعطيات"**، إذ تضم تقنية المعلومات البعد التقني القانوني الذي يتجزأ إلى فرعين الحوسبة والاتصال، فالأول قائم على استخدام وسائل التقنية لإدارة تنظيم معالجة البيانات وفق مهام معينة، أما الثاني قائم على نقل المعلومات، مادام أمامنا واقع تقني إلا قد برزت مصطلحات جديدة دالة على أفعال إجرامية ما يجرنا للتساؤل ما هي الحدود التي ينتهي عندها العبث وتلك التي تبدأ عندها المسؤولية لأفعال جنائية؟؟

لذا بادر المشرع بتأطير عصرنة نظم المعلومات الذي يؤسس مشروعية تفعيل الحاسب الآلي محلا لارتكاب الجرائم الواقعة على سرية المعلومات الماسة بقيمتها و دورها الناجم عن الاستعمال غير المشروع للمنظومة الرقمية فلا ينبئ عن جسامة كامنة بل تخطَّي انتصارات شخصية والإدراك باقتراف أفعال إجرامية قد تزعزع المتعاملين والترسانة القانونية، مما تعترض على غياب تشريعي و قصور قضائي قد تؤثر على أزمة السياسة العقابية التي تفتقر بالحاجة إلى مرجعية نصوص الحماية الجزائية، بالنظر لإفراز أنماط جديدة ترجع إلى سرعة التكنولوجيا بدوره تؤدي لاستنفار المجرم على استفحال

---

[2] ـــ محمود أحمد عبابنة، محمد معمر الرازقي، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005، ص ص 11-12.

الإجرام، مع ذلك تُجدر الدعوة إلى التحسيس في البحث والإثراء مقارنةً بالجريمة التقليدية و باعتباره مالًا يستوجب تقويمه مع استنباط تلك المسائل المثارة من خلال خصوصية التصدي على عرقلة تطور الجرائم وخضم تعدد التشريعات، فلا ننسى إلزامية سن الحماية و تسليط الضوء على الهيئات المستَّدة لمجابهة الإجرام المعلوماتي[3].

لذا سنحدد مكونات الحاسب الآلي **(أولا)**، ثم نعرج لمراحل تقنية المعالجة الآلية **(ثانيا)**.

أولا: مكونات الحاسب الآلي

يحتوي نظام الحاسب الآلي على نوعين هما المكونات المادية (Hard ware) والمنطقية (البرامجSoft ware) ذلك ما سنبين من الناحية التقنية بالتدقيق لأجل التمعن والبرهنة في الإطار القانوني لما لها صلة على محل الاعتداء للمعلوماتية والتي تتجلى فيما يلي :

1. المكونات المادية للحاسب الآلي (Hard ware)

عبارة عن هيكل مادي لنظام الحاسوب والتي تتفرع إلى وحدات فعليَّة شاملةً المعالجة المركزية، وحدات الإدخال والإخراج، وحدات النظام والتخزين، كما سنوضحها فيما بعد:

أ ــ وحدات الإدخال (Input Unit)

مسؤولة عن إدخال البيانات (المعطيات) أو البرامج المراد معالجتها داخل الوسط الكائن إلى ذاكرة الحاسب الآلي. [4]

---

[3] - يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء: "الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، قانون العقوبات، قانون الإجراءات الجزائية، (قوانين خاصة)"، كلية الحقوق العلوم السياسية، جامعة 8ماي 1945، قالمة، الجزائر، 2019، ص ص 36-77.

ــ أضفى المشرع الجزائري مسألة الحماية الجزائية على المصنفات الرقمية المنظمة في حقوق الملكية الفكرية الأدبية ذلك بمقتضى الأمر رقم 03-05 المعدل لقانون الخاص بحقوق المؤلف في المادة 44، كذلك القانون 16-01 المتضمن للتعديل الدستوري إعمالا على إقرار حماية شكلية موضوعية لبرامج الحاسوب وقواعد البيانات نحو المواكبة للتطورات العلمية التكنولوجية في مجال نظم المعلومات والاتصال، أما التشريع اللبناني المقارن قد أقرّ على الاعتراف بالحماية الممنوحة للحاسب الآلي بصورة جزئية ويتبين ذلك بموجب المادة 2 الفقرة 9 من خلال القانون المتعلق بحقوق المؤلف.

انظر/ نعيم مغبغب، مرجع سابق، ص 42.

(4) ـ الحفناوي فاروق، موسوعة قانون الكمبيوتر ونظم المعلومات، دار الكتب الحديث، مصر، 2001، ص ص30ـــ89.

ب ــ وحدات التخزين (Memory Unit):

تسمح للقيام بعمليات تخزين المعلومات الواردة في النظام الآلي أو تخزين النتائج التي تأتي من وحدة المعالجة المركزية، حيث تتكون من وحدات الذاكرة الرئيسية والمساعدة فالأولى تستخدم في تخزين المعطيات والبرامج المراد تنفيذه مع القدرة على استيعاب المعلومات بسرعة فائقة أما الثانية تدعم الحاسوب على حفظ البيانات والمعلومات بصفة دائمة.

د ــ وحدات الإخراج (Output unit):

حيث تبرز للمستخدم البيانات المعالجة، في حين تؤدي مهمة إيصال الحاسب الآلي بالوسط الخارجي مع القيام بنقل البيانات من وحدة المعالجة المركزية إلى الحيز المادي.

2. المكونات المنطقية للحاسب الآلي (soft ware)

البرامج اللازمة بالتطبيقات العملية التي تجرى داخل الكيان المادي للحاسوب، حيث تُخزن على أقراص مدمجة رقمية يتم تحميلها إلى الذاكرة، إذ يصطلح على تسمية (Computer Soft ware) بمعنى برمجيات الحاسوب المتعلق بالوثائق والمستندات، أما البرامج يقصد بها الإرشادات والإيعازات التي تحدد عمليات التنفيذ التسلسلي للحاسوب، لذا هناك نوعان للبرامج هما البرامج التطبيقية وبرمجيات النظم والتي سنتناوله فيمايلي:

أ ـ البرامج التطبيقية (Application soft ware)

عبارة عن برامج مصممة تؤدي وظائف منتجة ومعدة من مبرمجي النظم لاسيَّما مجموعة (Microsoft office) وهي (Access،Power point، Word ، Excel).[5]

ب ـ برمجيات النظم (Operating System Soft ware)

عبارة عن برمجيات وظيفية إجرائية تتحكم في العمليات الأصلية للأداء الآلي للحاسوب، بالمقابل هناك برمجيات تخزن على الأقراص الممغنطة المكونة من نظام التشغيل المسؤولة في كافة مهام الحاسب الآلي، كذلك لغة البرمجة بمثابة وسيلة التخاطب بالإضافة إلى تدوين تعليمات النظام، مما تلحق فيروسات حقيقةً تدخل ضمن برامج الحاسوب، لكن التصميم بغرض إلحاق الضرر والتخريب نظراً لاتساع شبكات الاتصال مع توافق نظم التشغيل قد ساهمت في تناثر تلك الفيروسات والولوج إلى قرصنة البرامج.

ثانيا: مراحل تقنية المعالجة الآلية(البيانات)

الحاسب الإلكتروني آلة مبرمجة مركبة من عدة وحدات متناسقة ومتسلسلة في الوظائف الطبيعية لها، حيث تؤدي مهمة معالجة البيانات أو المعطيات، إذ تجتاز عملية

(5) ـ محمد الزعبي، سهير الزعبي، الحاسوب والبرمجيات الجاهزة، دار وائل للنشر والتوزيع، عمان، 2002، ص14.

المعالجة التي يؤديها الحاسب الآلي على ثلاث مراحل متفاوتة تمامًا، لما لها صلة بالإجرام حال وقوعها على نظام المعالجة الآلية فيما بعد التشغيل لذلك سنتعرض إلى تلك الحالات وفق المنوال الآتي:

1. الإدخال

هي عملية أولية للمعالجة، حيث يتم تغذية الحاسوب بالبيانات المراد معالجتها من خلال اتباع تعليمات البرنامج، فلا يستوعب الحاسوب تلك البيانات إلا إذا وردت في هيئة مبرمجة، بعد ذلك يتم إدخال البيانات عبر أجهزة التغذية للنظام الآلي، إذ تبقى مرحلة الإدخال حلقة وصل بين الوسط المادي الخارجي ووحدة المعالجة المركزية.

2. المعالجة

تتولى في إجراء العمليات الحسابية أو استنتاج البيانات المدخلة من خلال تصنيفها، ترتيبها، مقارنتها أو اتخاذ قرارات معينة حسب تعليمات البرنامج، كذلك يتم تخزين البيانات من أجل معالجتها إلكترونيًا.

3. الإخراج

تعبَّر عن المرحلة النهائية التي تمر عليها عملية المعالجة من خلال إبراز النتائج المتحصلة على ذلك، كما ترسل المعلومات من الوحدة المركزية إلى أجهزة إخراج النتائج عند إتمام العملية بدوره تصل إلى المستفيد [6].

حيث قد بيَّنت العناصر الرئيسية للحاسب الآلي بمثابة جهاز تقني فعَّال ومؤشر رقمي مع آفاق إفشاء الثورة المعلوماتية ووسائل الاتصال في شتى نواحي الطفرة الميدانية، إذ فتحت أبوابًا يسيرة للأشخاص ذوي المصالح الضيقة وأصحاب الغايات غير المشروعة، لكن ما يفيد في هذه الدراسة الدور الذي يؤديه على آلية النظم المعلوماتية مع الطبيعة التي يحتويها قد تندرج ضمن خصوصية الحماية التامة للبرامج والمعطيات باعتباره مالاً معنويًا، لذا تولت المنظومة الجنائية جاهدةً في استبعاد أيَّ اعتداءات مجابهة لتقنية المعلومات، فضلا عن التكنولوجيا المستمرة في مجال الرقمية قد تنال استحقاق على

---

[6] - محمد المرسى زهرة، "مراحل عملية معالجة البيانات في الحاسب الإلكتروني"، **"مجلة التكنولوجيا والعلوم التطبيقية"** بتاريخ 12 أكتوبر 2018، على: 10سا و57 د، في الموقع الإلكتروني التالي: https://www.aspdkw.com تم الاطلاع عليه يوم: 6 ماي 2023، على: 11سا و33 د.

ميدان الأعمال، مما ارتأينا لإعطاء رؤية سليمة على العملية التقنية وآلية ممارسته رغم الفجوات التي تعيق تطبيقيًا، بغية الإحاطة بالنواحي الفنية على المنظومة القانونية.

الفرع الثاني
المقصود بالإجرام المعلوماتي

لاحظت الأبحاث العلمية التقنية قفزة مستجدة للعولمة الرقمية، حيث تتيح على المعلومات باعتباره موردًا ذات مرجعيَّة ووعاء جوهري على ميدان الاعمال امام واقع تكنولوجي حثيث، في حين خففت من كاهل العبء وتقليص الجهود المضنية على الأسواق الدولية، مع ذلك غدت التكنولوجيا بحرًا هائجًا للمعاملات الالكترونية التي جسَّدت روابط متشابكة داخل الفضاء الافتراضي.

بالرغم من التشجيع و الحضور القوي على التقنيات الآلية أمام عصرنة تكنولوجيا المعلومات والاتصال، إلا قد يغطي على جناح من الرداءة فلا مآل نحو الأمان ولا سبيل لإنهاء تلك المعارض المؤثرة بالمصلحة المحمية، لاسيَّما المنظومة القانونية التي تفتقر على وسيلة مضادة نحو المكافحة و الحد، ما جدى بالباحثين على الدراسة والتحليل لتلك الإشكالات المترتبة، حيث يتجلى ذلك في اتساع خلايا الإجرام بدوره تتفرع داخل البيئة المظلمة مجهولة الأثر التي قد ترمى على اعتداءات صارمة غير مألوفة مسبقا والماسة بالأموال، ما يُعرف بالإجرام المعلوماتي نتيجة حتمية لأيَّ تقدُّم علمي تقني الذي شغل عوائده الاجرامية على الطاقة الهائلة للحاسب الآلي، إذ انطلق على النهج التقليدي من السرقة و النصب إلى غاية بروز سبل جديدة تؤدي نحو اختراق الشبكات والأنظمة المعلوماتية، التحويلات الإلكترونية، قرصنة المواقع، نشر الفيروسات والبرمجيات الخبيثة.

علاوة على ذلك قد تبيَّنت المصطلحات الدالة على الجريمة المعلوماتية متعددة، قابلة للتعديل حسب مواكبة سرعة التكنولوجيا مع تطور قاعدي للجرائم القائمة في بيئة افتراضية مجردة، مما تجدر الإشارة في استخدام الباحثين لمصطلحات غير دقيقة في سياق التعبير، فحسبما تتطلب فرضيات البحث سواء الواقعة على الحاسب الآلي أم شبكة الانترنت تنحصر في نطاق مفهوم الجريمة المعلوماتية ذلك ابتداءً من إساءة استخدام الكمبيوتر، مرورًا بالغش المعلوماتي، جرائم الحاسب الآلي، الجرائم المعلوماتية أو ما يعرف بـ" **cyber crime**"، الجرائم الإلكترونية، جرائم تقنية المعلومات، جرائم المتصلة بتكنولوجيا الإعلام والاتصال إلى جرائم المساس بالأنظمة المعالجة الآلية

للمعطيات، فالتوضيح عن الدلالة الراجحة التي تُدرأ لكافة الاعتداءات الواقعة على الفضاء الافتراضي بما في ذلك جرائم المعالجة الآلية للمعطيات التي تتحقق تناسبًا مع طبيعة التقنيات الحديثة لتكنولوجيا المعلومات بدوره يتحد على البعدين التقني القانوني

إذ نلاحظ أنَّ التشريع الجزائري قد سار على منوال صحيح لما يسمح باستيعاب كافة الجرائم المستحدثة والمتخذة بشتى الوسائل الإلكترونية المتنوعة مستقبلا [7].

و نظرًا لخصوصية الجريمة إلا قد تنازعت الآراء الفقهية حول استخلاص تعريفًا جامعا يؤدي لانسجام في تقارب وجهات النظر عن المسألة المثارة، لذا حاولنا دراسة الدعائم الفقهية التي أعطت فكرة نابعة للجريمة المعلوماتية، حيث هناك رأي يرجح ماهي إلا جريمة تقليدية ترتكب بأسلوب إلكتروني خلافًا للرأي الآخر الذي يناقض الأمر تمامًا باعتباره ينشأ نتيجة العوامل التكنولوجية اللامتناهية أمام واقع رقمي فلا تتشابه مع الجرائم المادية على الاطلاق سواء من حيث محل الاعتداء، الوسيلة المستعملة، سمات مرتكبيها، الدوافع المنشودة، وذلك في ظل غياب سياسة عقابية مكفولة للمجابهة مع تقلص دور القضاء نظرًا للتطور، الحداثة، التعقيد، مما نلتمس بالوقوف على المسألة لأجل إزالة اللبس عن الفراغ التشريعي مع التخفيف من حدة الجدال الفقهي من خلال مراعاة حلول ملموسة تدفع تلك القيود. [8]

---

[7] - صليحة بوجادي، "الإطار المفاهيمي للجريمة المعلوماتية"، **"مجلة الدراسات القانونية المقارنة"**، المجلد **7**، العدد **1**، كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بوعلي، الشلف، الجزائر، 2021، ص ص 2530-2531.

(8) – رستم هشام محمد فريد، "قانون العقوبات ومخاطر تقنية المعلومات"، بحث مقدم لمؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاملة المجرمين، **"مجلة الأمن العام"**، العدد 151، الأردن،2003، ص 24.

تجدر الإشارة إلى تحديد الفارق الحقيقي بين المعطيات، المعلومات، المعلوماتية التي تتجلى فيمايلي:

المعطيات هي المادة الخامة المستخلصة للمعلومة، إذ تكون في حالة تبلور بمثابة معطيات خلافًا في حالة كمون ترد على المعلومات بذاتها، ذلك ما يسمى بالدورة الاستدراجية، حيث يتم استخدام تلك المعطيات المتحصلة من عملية المعالجة بغرض الحصول على معلومات إضافية جديدة، في حين يقصد بالمعلوماتية علم المعالجة العقلية والآلية للمعلومات التي تنقسم إلى كلمتين (information المعلومات) (automatique الآلي) فالفارق الأصلي بين المعلوماتية والمعطيات الأولى عبارة عن علم يهتم بالمعارف المتصلة على المعطيات من حيث تجميعها، تنظيمها، تخزينها، استرجاعها، تحويلها أما الثانية عبارة عن رموز، حقائق، إحصاءات خامة، لذلك يؤكد الفقه لا جدوى للتمييز طالما أنَّ المعلومات هي المعنى المستخلص من المعطيات بعد معالجتها، بالمقابل المعلوماتية هي المعلومات المبرمجة أليًا قد تستخدم في تقنيات الحاسوب والأنظمة الآلية، أما البرامج بمثابة مستودع يتم فيها معالجة المعطيات، إذن العلاقة تصبح الجزء بالكل قد تسري على غاية حماية المعلومات مادام الكل يتمتع في اطار الحماية القانونية ضد الاجرام المعلوماتي داخل البيئة الرقمية.

انظر/ امينة حماشي، " ماهية الجريمة المعلوماتية"، **"مجلة دراسات وأبحاث"**، المجلد 1، العدد 1، كلية العلوم الإنسانية والاجتماعية، جامعة زيان عاشور، الجلفة، الجزائر، 2016، ص449.

حيث نستند إلى التعريف الفقهي حسب ما جاء في التشريعات المقارنة سواء اكانت معايير صائبة أم منافية للفكر القانوني والسياسة الجنائية، فالعلة قد تسري على انعدام حصر قاعدة التجريم في نطاق أفعال معينة مما يتعذَّر التصدي لها، إذ حاول الفقيه ماروي (Marewe) حصر تعريفًا ملائمًا للجريمة المعلوماتية بقوله: **"هي الأفعال غير القانونية المرتكبة بواسطة العمليات الإلكترونية والماسة بالنظام المعلوماتي أو المعطيات مهما صاب الهدف".** [9]

نستخلص من خلال استقراء التعريف قد يتخلله نوعًا من الفراغ فلا يستوعب لكافة أنماط الجريمة سواء الواقعة بواسطة النظام المعلوماتي او على النظام المعلوماتي ذاته، نتيجةً لسرعة التطورات التكنولوجية التي تؤدي الى تنوع أساليب الدافعة لارتكابها على المسرح الافتراضي مع احترافية المجرم بالتلاعب على الآلات التقنية دون آثر، إذ تم اللجوء الى توسيع من مدلول الجريمة المعلوماتيَة الذي يعبر عن الطابع الفني من خلال التعامل مع الاليات التقنية المستقبلية.

كما قد نضع تعريفًا متناسقًا حسب مدى احاطتي على استقراء مغزى البحث، إذ تُعرف الجريمة المعلوماتية ما يلي: **"كل اعتداء غير مشروع يتم باستخدام النظام المعلوماتي والتي ترتكب في بيئة إلكترونية من شأنها أن تصدر عن إرادة إجرامية محلها المعطيات وذلك معاقب عليه قانونا"**.

لذلك نستنتج من خلال التعريف للجريمة المعلوماتية أمرين هما:

. عندما تكون المعلوماتية موضوعًا للاعتداء وذلك حال وقوعها على المكونات المعنوية من معطيات، بيانات، برامج.

. عندما تكون المعلوماتية وسيلة للاعتداء وذلك حال استخدام الجاني للأجهزة الآلية في تنفيذ جريمته، باعتباره عنصرًا معنويًا إراديًا، فالألة التقنية ما هي إلا رابطة بين الفاعل والمعلومة بواسطته يلجأ الجاني باستخدام دوافع خارقة والرامية للجريمة من خلال تحقيق السلوك غير المشروع.

أما فيما يتعلق التعريف القانوني قد تم إدراك المشرع للفراغ التشريعي والذي يتضح من خلال تعديله لقانون العقوبات بمقتضى القانون رقم 04-15 فلا أثر على إيجاد تعريفًا

(9) -محمد على العريان، الجرائم المعلوماتية، الطبعة الرابعة، دار الجامعة الجديدة، الإسكندرية، 2004، ص 43.
(10) ـــ نشناش منية، مداخلة حول الركن المفترض في الجريمة المعلوماتية، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، 2016، ص ص2-3.

قانونيًا جامعًا لجرائم المعلوماتية إذ اكتفى بالنصوص العقابية الواردة في المواد **"394 مكرر إلى 394 مكرر 7** التي تبين الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات دون تحديد ماهي الجرائم التي تدخل في نطاقها بل تؤكد ايُّ جريمة قد ترتكب أو يسهل ارتكابها عن طريق المنظومة المعلوماتية، في حين جاء القانون 04/09 وسَّع من مفهوم الجريمة المعلوماتية التي قد يصبح السلوك الاجرامي محل للاعتداء او وسيلة الارتكاب. **(10)**

نستنتج في جوهر النصوص القانونية الواردة في المواد 394 مكرر إلى 394 مكرر 7 قد تنقسم الجرائم إلى ثلاثة أصناف وهي: **(جرائم المساس بأنظمة المعالجة الآلية للمعطيات، جرائم ارتكاب أو تسهيل ارتكابها عن طريق المنظومة القانونية، جرائم ترتكب أو يسهل ارتكابها عن طريق نظام الاتصال وتخزين المعطيات في شكل إلكتروني شاملةً أجهزة الحاسوب ووسائل الاتصال وشبكات الربط).** [11]

تطبيقًا على ما سبق يقتضي بنا الخوض لأهم خصائص الجريمة المعلوماتية **(أولاً)**، ثم نأتي لتحديد الدوافع الرامية إلى التجريم **(ثانيا)** بعد ذلك نبين الانعكاسات التي تؤثر على الجريمة المعلوماتية**(ثالثا).**

---

[11] - أشار المشرع الجزائري للتعريف بالجريمة المعلوماتية من خلال المادة الثانية في الفقرتين ب/ج من القانون 04/09 التي جاءت ما يلي:

تنص الفقرة "ب " فيما يلي: "المنظومة المعلوماتية نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض او المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين."

في حين تأتي الفقرة " ج " للتعريف بالمعطيات المعلوماتية من خلال اشتراط المشرع على ضرورة الترابط بين مكونات النظام، مما ركز على وظيفة المعالجة مؤَسعا المجال على المعطيات والأنظمة، إذ جاءت ما يلي: **"أيَّ عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية ...."**

ـ يتبين من خلال التعريف السالف أنَّ المشرع بصدد الإشارة لتعريف الجرائم الإلكترونية مما قد اصطدم بمبدأ قانوني للشرعية الجنائية نظرًا لاستيعاب ذلك النص بكافة الجرائم التي ترتكب في بيئة رقمية، فالعلة قد جاء في الصياغة العامة للنصوص القانونية.

ـ قانون رقم 09ـــ04 المؤرخ في 05 أوت 2009، يتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، ج. ر. ج. ج، عدد 47، الصادر في 16 أوت 2009.

ـ راجع المواد 394مكررإلى 394مكرر7 من القانون رقم 04ـــ15، المؤرخ في 10 نوفمبر 2004، ج. ر. ج. ج، عدد 71 الصادر في 7فيفري 2004، يعدل ويتمم الأمر رقم 66ـــ156 المؤرخ في 8 يونيو 1966، المتضمن لقانون العقوبات.

ـــ يتعين الإشارة الى المفاهيم القانونية الدالة على الاجرام المعلوماتي والتي تتجلى فيمايلي:

ـ الاختلاس المعلوماتي:" يرُّد صورة للسرقة المعلوماتية بصفة مكتملة مانعة، حيث يتم نقل الشيء او المال بغرض التملك والاعتداء غير المشروع سواء العبث، الاقتحام، الاتلاف، الغش، التجسس المعلوماتي معتمدًا أساليب تقنية مستحدثة، إذ توازي بين السرقة المادية من حيث النقل الفعلي للحيازة، حيث يتم إخراج المال من المجني و إدخاله في حيازة الجاني ما يحدث على تبديل الحيازة، خلافًا للاختلاس المعلوماتي قد تقع الحيازة على المعلومات أيًا كانت طبيعته والتي تحدث داخل البيئة الرقمية، إذ يتم الاعتداء عليها بشتى الوسائل التقنية الجديدة."

انظر/ إبراهيم السيد حسانين زايد، **"الاختلاس المعلوماتي"، "المجلة القانونية للدراسات والبحوث العلمية"**، المجلد 11، العدد 9، القاهرة، 2021، ص ص3964 -39947.

أولاً: خصائص الجريمة المعلوماتية

يكتسب الإجرام المعلوماتي طابعًا قانونيًا ناتج عن إفراز تقنية المعلومات ووصلها على سائر الوسائل الإلكترونية المتجددة، مما أضفى عليها جنبات نابغة ومتنافرة مقارنة بالجرائم المادية التقليدية لاستدراك هاتيه المواصفات التي تتخذ أهمية استثنائية ملموسة ذات أولوية على الحماية القانونية لتلك الأفعال الإجرامية دون إصابة الهيئات الدولية لأي شلل طالما هناك الانفعالية والتفاعل على المواجهة، إذ يمكن استخلاص هذه السمات على النحو الآتي:

➢ 1. جرائم صعبة الإثبات والاكتشاف:

تتم الجرائم المعلوماتية في نطاق ميتافيزيقي فلا صلة بالمستندات بل تطوف وراءه الذبذبات الإلكترونية المتصلة بشبكة الإنترنت والأجهزة الآلية، إذ ينتهز الجاني فرصة مغرية بالعبث على البيانات المقترنة بالنبضات الإلكترونية مع محو آثاره وإخفاء ملامح الجريمة في زمن قياسي حتمًا قبل الوصول إلى يد السلطات الأمنية لغرض الخوض في العمليات الفنية، مما يستوجب الاستعانة بأخصائي علوم الحوسبة حتى يتسنى إجراء التحقيق عن الأدلة نظرًا للتعامل الجاني مع التقنيات الآلية الذي بدوره يتحدى السلطات الأمنية للالتحاق من وراء اثر الجريمة، كذلك التسلل نحو طمس الأدلة مع التغلب على المشاريع الإجرامية، بطبيعة الحال قد يعول نفعًا لإثبات إدانته، مادام التعود على التحريات المادية قد بسطت للكشف عن الأدلة فإنَّ فعالية الجرائم المعلوماتية تتم بالمصادفة دون الإبلاغ نظرًا لاستحالة رؤيته باعتبارها مشفرَّة عن لغة الحاسوب و المسماة بالبرمجة، مما يتعذر قراءة الأدلة لدى الأجهزة الأمنية. (12)

حيث يتضح في التفكير بالتمرن على المجال التقني لغرض معرفة لمسات الإجرام واستدراك ملاحظة الأدلة وكيفية رفعه من موقع الجريمة، بالإضافة إلى توافر أجهزة الرقابة ذات نوعية جديرة حتمًا سيؤدي إلى وضوح الدليل الخفي بسهولة ، **لذا نؤسس فكرة على السلطات الأمنية في إطار تنظيمي دولي لإنشاء مساحات خاصة على الوسط الافتراضي المسماة بالميتافيرس بمعنى محاولة التمثيل بشخصيات ثلاثية الأبعاد لأداء أنشطة الأنترنت مستقبلاً**، بينما يستوجب التكفُّل بالمجني دون الإحجام عن الإبلاغ مما نوجه من سلطة الدولة القيام بالواجب دون التذرع لمتطلبات المالية مادام المسألة

(12) ـ نسرين محسن نعمة الحسيني، محمد حسن مرعي، الجرائم الواقعة على الأموال، (دراسة مقارنة)، دار الكتب والوثائق القومية، مصر، 2020، ص ص 30ـ 41.

متعلقة بالكيان الأمني وإلا ستفقد المنظومة القانونية مرجعها في السيطرة على الإجرام. **(13)**

➢ 2. وقوع الجريمة أثناء المعالجة الآلية

شرط مسبق على وقوع الجريمة خلال عملية المعالجة للبيانات المخزنة في النظام الآلي، إذ يتم أثناء تشغيل نظام المعالجة سواء في مرحلة الإدخال، المعالجة، الإخراج، ففي مرحلة الادخال يتم ترجمة المعلومات إلى لغة مبرمجة بإدخال بيانات جديدة، أما المعالجة قد يتم طرح تعديلات على البرنامج من خلال التلاعب، الاستبدال، المحو أم تشغيل برامج جديدة، في حين تأتي مرحلة الإخراج على إبراز النتائج بعد معالجتها، مما يقع الاعتداء على تلك النتائج بشأنها تؤدي لانعدام التوافق مع البيانات المخزنة في النظام.

➢ 3. أسلوب ارتكاب الجريمة المعلوماتية

ذاتية الجريمة المعلوماتية قد تتضح صراحةً في أسلوب الارتكاب مع استخدام الجناة أساليب ذات الطابع التقني داخل الواقع الافتراضي، مما تتطلب قدرًا عالي للذكاء والخبرة الملمَّة على المجرم في تنفيذ خططه الإجرامية، خلافًا عن الجريمة المادية يقتضي جهدًا عضلي في صورة ممارسة العنف والإيذاء بطبيعة الحال هي جرائم ناعمة هادئة جدًا بدوره يوظف أفعال غير مشروعة دون تدارك وقوعه، كما أنها من الجرائم التي نالت معدلاً ضخمًا على المنظمات الدولية القانونية، حيث تستدعي السياسة الجنائية بوضع نصوص مبادرة على المكافحة والحد أما عن خصوصية المجرم المعلوماتي باعتباره المسقط الأصلي نحو استنفار الإجرام، رغم ذلك تعد الجرائم المعلوماتية غامضة للكشف عن نواياه بالإضافة الى بواعث ارتكابه متنافرة تمامًا. **(14)**

---

(14) ـ تجدر الإشارة لإحدى القضايا الواقعية التي تتلخص فيمايلي:

" هناك شخص يدير مكتب الحسابات، حيث يتولى المراجعة والتدقيق لإحدى شركات الشحن، والتي تمت الجريمة باسمها على مدار خمس سنوات، نجحت حتما في إخفاء الدليل خلال تلك المدة، إذ لم تكشف إلا بالمصادفة لإحدى البنوك التي سبقت التعامل مع الجاني ولو أن شركة الشحن تكلَّفت عناء في تنشيط الرقابة الذاتية على أموالها وحساباتها لكن الأمر اكتشف مبكرًا، فالخطورة تحذو بالمتعاملين في المؤسسة الذين يسهلون على تغيير أنظمة الحماية المسمى بـ: حواجز البروكسي (نظام الرقيب)."

ـ يقول أدريان أورمان خبير المعلوماتية والذي جاء ما يلي: "الصعوبة تكمن على استطاعة برمجة الكمبيوتر من خلال البيانات التي قام بها وبالتالي التغلب للحصول على أية أدلة للإمساك بالمجرم معقدة."

Voir/ LUCAS DE LEYSSAC Marie Paul, Encyclopèdie juridique Dalloz, Paris, 2003, p17.

(14) ــ خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2009، ص ص 79-87.

ثانيا: دوافع الإجرام المعلوماتي

لا شك أنَّ فئات مرتكبي الجريمة المعلوماتية غير متطابقة تمامًا عن مرتكبي الجرائم المادية، لذا من الطبيعي إيجاد نفس التباين في العوامل التي تدفع لارتكاب أفعال غير مشروعة تبعًا لطبيعة شخصية المجرم ومدى خبرته بالمخاطرة والذهن المنتقد الذي يتخذ بناءً على موهبة خارقة في مجال البرمجة مع استخدام تقنيات الحاسب الآلي بوضعيات أوتوماتيكية مقابل الغاية المنشودة من وراء استعماله للأجهزة سواء بتشغيله أم يتعدى النشاط نحو عمليات خيالية غير متوقعة تمامًا، فضلاً عن ذلك قد تنحصر تلك الدوافع إلى قسمين فالأولى متعلقة بالغايات الشخصية التي تنبع عن الرغبة الذاتية للفاعل أما الثانية مرتبط بالعوامل البيئية المادية نظرًا للآثار الناجمة عن تصرفات المجرم نحو سبق الإجرام، حيث يتسنى لنا إدراج هاتيه الدوافع في النقاط الموالية ما يلي:

ـ تشير الاحصائيات المسجلة عن الإبلاغ بالجرائم المعلوماتية التي تتراوح بين 20%، 30% "، حيث ذكرت الدراسة أنَّ العديد من الشركات تم وقوعها تحت خط الإجرام ذلك حوالي الف شركة و هي بصدد إنجاز جهاز فورتن 500 بما يعادل 2% من جرائم الحاسوب التي قد تم إبلاغ عنها إلى مكاتب التحقيقات الفيدرالية، في حين بقي جزء هائل لم يتعين الكشف عنها نظرًا للمؤشرات السلبية التي قد تؤثر في السياسة، مما سعت لجنة خبراء مجلس أوروبا للتكفل بالمجني على الإبلاغ دون الإحجام بمساوئ الإجرام والتي تفرض التزام على موظفي جهة المجني للإحاطة بعلمهم في حدوث الجريمة، فلا يجوز إحلال المجني محل الجاني".

انظر د/ عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، (دراسة قانونية متعمقة في القانون المعلوماتي)، دار الفكر الجامعي، الإسكندرية، 2006، ص59.

La Cyber criminalité peut se définir : « c'est l'ensemble des infractions pénales commises sur le réseau d'internet. »

Disponible en ligne à l'adresse suivant: http://VSabourni.free.fr

➢ 1. التحدي على النظام المعلوماتي

إحداث عملية اختراق الأنظمة الإلكترونية من خلال كسر الحواجز الأمنية قد يتحسس الجاني بالدعابة تغطي أوقات فراغه بدافع المزاح والاستهتار، مما يتم القيام بالتصرفات ليست بذي قيمة في بناء القصد الجرمي الذي يؤدي لافتعال جرائم بالدرجة ولو بدايته جاءت عن استفزاز، فالتصرف بحقيقته قد يصيب تخريب متعمد لغرض المتعة بالإضافة إلى الفضول بدافع الانتقام والغرور على منافسة التقنيات الآلية، إذ يتملكون شعور البحث عن القوة دون التحسيس بالدنيوية التي تؤثر عن إثبات القدرة الذاتية، أما فيما يتعلق الغرور عن التفوق العلمي الأول يسعى للتفاخر أمام الغير بإثبات الموهبة و الثاني يسعى الى التحدي لانتصارات شخصية دون التفاخر، بينما قد يكون الباعث رغبة للانتقام ضد الأشخاص، المؤسسات الاقتصادية، الأنظمة السياسية للدول، لذا أُدخلت في التكوين القانوني ما يسمى بالقصد الجنائي الخاص عنصرا ملزمًا لإثبات النية الإجرامية كذا سببا للتشديد والتخفيف [(15)].

➢ 2. تحقيق الثراء غير المشروع

استقرت شبكة الانترنت على الصعيد الدولي، مما سهلت في إحداث جرائم نوعية جديدة في اختراق نظم المعلومات المرتكبة من قبل القراصنة الذين يقبعون أوساط غير مشكلة للخطر، فالغاية المثالية هنا قد تتجلى في حجم الأرباح من خلال الاستيلاء على الأنظمة الآلية للمؤسسات معتمدًا شبكات الاتصال الدولي فلا يطاق عن إثبات الذاتية بل الكسب المادي ولو بأقل معرفة بغض النظر لأسلوب ارتكاب الجريمة متعلق بالأنظمة الآلية، إذ اعترف دوغلاس بيرت أحد مسؤولي مركز الحماية من جرائم الحاسب الآلي التابع للشرطة الفيدرالية الأمريكية بقوله: **"تحديد الخطر أمر بالغ الصعوبة فلا يمكننا أن نتوقع كل شيء".**

---

(15) ــ بوهرين فتيحة، "الجريمة المعلوماتية في التشريع الجزائري"، **" مجلة الحقوق والعلوم الإنسانية"**، المجلد 14، العدد 4، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، 2021، ص55.

تجدر الإشارة إلى تقرير صادر من السيد مكيو هيومان (Mikko Hypomane) مدير مركز البحوث للشركة(F.Secure) بشأن مجرمي المعلوماتية الذين يعمَّدون تبليغ رسائل إلكترونية إلى ضحاياهم مسبقًا مع إخبارهم بأمر اكتشاف ثغرات أمنية على أنظمتهم المعلوماتية، كما سيقومون بمحو بياناتهم وتدميره كليًا في حال عدم تحويل الأموال إلى حساباتهم. وبالفعل حدث لشركة Google ذلك في شهر ماي 2004، أين قام ميشيل برادلي (Michel Bradly) إرسال تهديدات للشركة مع إلزامية دفع 100.000 دولار وإلا سيطلق فيروسًا وبرنامج غامض قد يؤدي إلى تعطيل النظام المعلوماتي المتعلق بالتحصيل عائدات الإشهار للصفحات المدعمة، رغم ذلك ألقي القبض عليه في ولاية كاليفورنيا الأمريكية بتاريخ 17 ماي 2004. انظر/ ذياب موسى البداينة، الجرائم الإلكترونية (المفهوم، الأسباب)، المرجع سابق، ص93.

(17) - عبد الرحمان جميل محمود حسين، الحماية القانونية لبرامج الحاسب الآلي، (دراسة مقارنة)، رسالة لنيل شهادة الماجستير في القانون الخاص، كلية الدراسات العليا، جامعة النجاح الوطنية، فلسطين، 2008، ص 58.

علاوة على ذلك قد يجني الفاعل أرباحًا هائلة تشكل دافع محفز لأصحاب النوايا السيئة، **حيث أشارت الدراسات الإحصائية الصادرة عن مركز احتيال المعلومات الوطني في الولايات المتحدة الأمريكية(N.F.I.C) ما يقارب 34% حالات الغش المعلوماتي لأجل اختلاس الأموال، 23% سرقة المعلومات، 19% أفعال إتلاف، 15% سرقة وقت الألة لأجل تحقيق منافع شخصية،** في حين نلاحظ تحقيق المجرم للأرباح المادية وفق ما يرويه أحد محترفي المعلوماتية في سجن كاليفورنيا بقوله: **"لقد سرقت أكثر من نصف مليون دولار بفضل الأجهزة الحاسوبية المتعلقة بالضرائب في الولايات المتحدة الأمريكية كما بإمكاني تكرار ذلك في أي وقت، لقد كان شيئًا سهلاً فأنا أعرف أسلوب عمل جهاز الحاسوب لنظام الضرائب، إذ وجدت ثغرات كثيرة يمكن أن تمدني بمبالغ طائلة لو لم يكن لسوء الحظ قد صادفني".**[16]

إذ يُمثَّل دافع الكسب المادي في الحقيقة غاية الفاعل الأكثر رواجًا في اقتراف جرائم الكمبيوتر بما يطويه من ثراء مالي، فلا يمنعنا من إيجاد بواعث مصداقية لتلك الأفعال الإجرامية.

- **3. الدوافع النمطية الخارجية**

- التنافس السياسي الاقتصادي دافعًا للإجرام، مثال على ذلك **"قيام إحدى القراصنة على اختراق الأنظمة الآلية التابعة للحكومة الأمريكية مدة عام كاملة مما أدى إلى سرقة معلومات سرية تدخل ضمن الأجهزة الأمريكية ".**

- التسابق الفضائي العسكري بين الدول على سبيل المثال **"إغارة القراصنة على الشبكات المعلوماتية التابعة لوكالة فضاء ناسا مع موقع الأسلحة الذرية التابعة للحكومة الأمريكية".**

- مناهضة العولمة ذات تأثير احتمالي مطلق يدفع للإجرام على سبيل المثال **"اختراق النظام المعلوماتي الخاص بالمنتدى الاقتصادي العالمي في دافوس، حيث تمت عملية سرقة المعلومات السرية المتعلقة بالشخصيات المشهورة المشاركة في إحدى المؤتمرات الدولية والتي أرسلت بصددها لإحدى الصحف السويسرية.**

إذ يمكننا وضع التصور الرياضي الذي يثبت عن الدوافع المترددة في حقل الجرائم المعلوماتية:

-حروب المعلومات+ تعدد المنظمات الإجرامية = دوافع سياسية فكرية.

-انكار الخدمات التجارية+ التنافسية بأنشطة غير مشروعة = التحدي على النظام المعلوماتي

-الاحتيال على الأنترنت= الاستيلاء على المنافع المادية والثراء الشخصي.

-التجسس على المعلومات+ الابتزاز= تحقيق انتصارات تقنية مالية.[17]

فالملاحظ من خلال الدراسة لتلك الدوافع هناك فائدة مزدوجة الأولى تساعد في إيجاد الحلول المناسبة للمقاومة التغلب أما الثانية تحدد التكييف القانوني التي قد تضفي عليها، فلا ننسى الحماية القانونية الماسة بالمصالح المحمية الذي يبرر تجريمه، مما يقال عليه ليس هناك شعور حقيقي بالأمان ولا أخلاقية للأفعال المرتكبة مع قناعاتنا لتلك الأسباب باعتبارها موحدة سواء في جرائم ضد الأشخاص أو الأموال.

ثالثا: أثار الإجرام المعلوماتي

أدت مساوئ استخدام المعلوماتية إلى اقتناص فرصة تحقيق غايات غير قانونية، إذ تتفاقم تلك المخاطر نظرًا لتعدد أنماط الجرائم في البيئة الافتراضية بالإضافة الى احترافية مرتكبيه بالتعامل مع التقنيات الآلية المساهمة في تنفيذ الإجرام، مما يُجدر التنسيق بالتعاون الأمني الدولي مع طرح سبل وقائية للتخفيف من حدة استفحال الإجرام وفق استراتيجية صارمة على المجابهة.

لذا سنعرض عن تلك الانعكاسات التي قد تصطدم بالتهديد الأمني القانوني المبنية فيما يلي:

---

(18) ـ نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2008، ص 93.
ــ تجدر الإشارة إلى أمثلة نموذجية الواقعة لإحدى مستشاري البنوك العالمية والتي تتلخص فيمايلي:
"قيام مستشار لدى البنك والذي يسمى Stanley Rifkin في تحويل مبلغ 10مليون دولار إلى حساب بنكي مفتوح باسم شخصي في سويسرا طالما يتمتع بثقة مطلقة لدى البنك، إذ تسمح له بالولوج إلى مفتاحين إلكترونيين لأجل التحكم في التحويلات الالكترونية للأموال ذلك من بنك لأخر، مما تمكن بفضل معالجته الآلية للمعلومات وتألفه الشديد مع النظام الآلي لغرض الوصول إلى المفتاح الثالث."
انظر/ نبيل صقر، موسوعة الفكر القانوني، (جرائم الكمبيوتر والأنترنت في التشريع الجزائري)، دار الهدى، الجزائر، 2005، ص 118.

➢ 1. التأثيرات الاقتصادية

تلحق الجرائم المعلوماتية أضرارًا بالأنشطة الاقتصادية لاسيَّما المعاملات المالية في مجال تقنية المعلومات واستغلالها للأنظمة الآلية المعتمدة في تسيير الخدمات الراهنة سواء للأفراد أو المؤسسات الحكومية التي بدوره تنتج خسائر بالغة، حيث نشر مكتب التحقيقات الفيدرالية الامريكية **(F.B.I)** استبيانًا **بتاريخ 12-04-2001** مما شارك أكثر من **500 مسؤول** عن أمن المعلومات، **إذ يبين 85% قد تعرضت مؤسساتهم للجرائم المعلوماتية مما ترتب خسائر مقدرة بـ 378 مليون دولار، في حين تقدر الأرباح العائدة من وراء بيع برامج الفيروسات حوالي 275 دولار سنويًا، أما في فرنسا قد ارتفع حجم خسائر الشركات عن أفعال التحايل المعلوماتي حوالي 700.000.00 أورو، كما كبدت منذ سنة 2000 حوالي 1600 مليار دولار مع تضييع 3,3% في ترميم أنظمتها المعلوماتية المخربة.** [18]

➢ 2. التأثيرات النفسية الاجتماعية

تتعدى جرائم تقنية المعلومات الكيان الاقتصادي نحو التأثير بالعوامل النفسية الاجتماعية الماسة بكافة الفئات سواء أكانوا بالغين أم القصر والذين تقودهم للانحراف إلى الإجرام لاسيَّما الاستغلال الجنسي المواقع الإباحية، الاحتيال، السطو، إذ يحتاج هؤلاء المراهقين مراقبة حتمية تفاديًا لسلبيات البيئة الرقمية التي تؤدي إلى التجسس في تفكيك الروابط الأسرية لاسيَّما في ظل تفاشي مواقع التواصل الاجتماعي.

حيث تجدر الإشارة إلى ما وقع في الجزائر خلال سنة 2016 أين تم **"تسريب امتحانات شهادة الباكالوريا و نشره عبر مواقع التواصل الاجتماعي تسهيلاً لعملية الغش مما تسببت بآثار نفسية جمة على المترشحين نتيجة إعادتهم الجزئية للامتحان،**

---

[18]- AZZOUZI Aliel *«La cyber criminalité au Maroc»*، Bishop solution، Casablanca، Maroc, 1er édition, 2010، p18.

ـ تشير الإحصائيات المسجلة لشركة سمانتيك(Symantec) الأمريكية المختصة في حماية الشبكة المعلوماتية أنَّ المعدل السنوي لكُلفة الجرائم المعلوماتية حول العالم قد يبلغ حوالي 114 مليار دولار، مما أصدرت تقرير تحت عنوان نورتون سيبركرايم عام 2011 التي وصلت إلى ما يقارب 431 مليون بالغ حول العالم كانوا ضحايا للتهديدات الإلكترونية أي معدل مليون ضحية يوميًا بما يقارب145 ضحية في الثانية، كما بلغت الخسائر المالية عام 2010 حوالي 388 مليار دولار والتي تجاوزت قيمة السوق السوداء بما يقارب 288 مليار دولار دون الخسائر التي تم احجام المجني عن الإبلاغ لاسيَّما المؤسسات المالية، كما تنبأت شركة الأبحاث الأمريكية للأمن السيبراني Cyber Securityعام 2016، أنَّ معدل الجرائم الإلكترونية ستكلف للعام 6 تريليونات دولار أمريكي سنويًا بحلول عام 2021 ستزيد ضعف عن كلفتها التي بلغت 3 تريليونات دولار أمريكي عام 2015.

انظر/ وائل نعيم، مقال منشور بتاريخ: 2018/03/02، على الموقع الالكتروني:
https://www.albayam.ae/across-the-uae/accdents/2018-30201.3200109.

بالإضافة إلى الأضرار الاقتصادية التي تكلف بتأطير إعادة الامتحان"، كذلك قد يمتد على المستوى السياسي الذي يساهم في ممارسة أساليب الضغط لاسيَّما ترويج الآراء الفكرية باستخدام فضاءات التواصل الاجتماعي، لذا يستوجب من سلطات الدولة بمبادرة الحماية الأمنية لأجل التخلص على العراقيل المثبتة و التخفيف من حدة المخاطر الرائدة **(19)**.

(19) – SEMLALI Redouane، *«cyber criminalité: menaces et centre mesures»*، Digital Maghreb، Maroc، N°4 février 2013، pp 42-43.

الفرع الثالث
تمييز الجريمة المعلوماتية عن الجريمة المادية

تتطلب البيئة المادية حركة عضوية حاسمة للفاعل بغرض تنفيذ المخطط الإجرامي، حيث قادت اشكال جديدة معياره الاستغلال غير المشروع للأنظمة المعلوماتية نظرًا لتلاشي الأليات التقليدية، بذلك نستند للإشارة على الخصوصية المشتركة بين الجرائم المادية والمعلوماتية من أجل إثبات الصلة المرتبطة فيما بينهما مع الأخذ بعين الاعتبار صراحةً للأوصاف المتعارضة إن وجدت تمامًا.

الملاحظ بين الجرائم المادية والمعلوماتية في الأصل متناسقان، بالرغم من ذلك تم إبعادها عن الدائرة المادية واستعادتها في دعامة جديدة، حيث تستهدف المعنويات دون الماديات الملموسة بالنظر لالتحام الشبكات الرقمية على البعد الجغرافي بين الدول، كذلك خففت من حدة العبء على الأعمال الواقعية، إلا أنَّ الأمر تحول إلى فوضى إجرامية في كافة القطاعات، مما تعددت المصطلحات الدالة على المعلوماتية والمسماة بـ: الجرائم الحديثة، الجرائم التقنية، الجرائم المتطورة، إذ يتبين ذلك ليس بمصطلح قانوني بحت يحدد العناصر التجريمية التي أطالها القانون إنما وصف لأنماط الجرائم المتولدة تبعًا للتكنولوجيا الرقمية فلا يجمع سوى حداثتها، حجمها، خطورتها، تعدد الجناة، أساليب ارتكابها، نتيجةً للتغيرات البنى الاقتصادية، الاجتماعية، السياسية باتت الجريمة التقليدية متأثرة بطرق غير مألوفة قد يستفيد مرتكبيه على تنفيذ المشروع الإجرامي باستعمال التقنية العالية (**الفضاء السيبراني**) (**Cyber Espace**). [20]

تظل المعلوماتية جرائم مادية بطبيعته، فلا خلاف من حيث العناصر الإجرامية، خصوصية مرتكبيه، الدوافع المرغوب فيها، جسامة الخطورة، الاثر المترتب عليها بل حتى على إجراءات المتابعة وملاحقة المجرمين إلا قد يتعذر في التحري عن الأدلة رغم المهارات التي يتقبلها الفاعل مفاده استحواذ ثروة المعلومات، فلا يتسنى معرفة بصمة الجريمة لانعدام مشاهدة الجاني على المسرح الافتراضي بل يتخذ في هيئة محجوبة، في حين المجرم العادي قد يبذل جهدًا ذهنيًا نسبي في التخطيط على بدء تنفيذ النشاط الإجرامي لممارسة شتى الاعتداء(النهب، العنف، السفك، التعدي) ذلك بدافع التغلب على المجني، أما عن محل الجريمة الأولى ذات طابع مادي ملموس لعلها(الأجهزة

[20] -بلعيد إلهام، "الجرائم المستحدثة"، "**مجلة الباحث للدراسات الأكاديمية**"، المجلد 09، العدد 02، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر-باتنة 1، الجزائر، 2022، ص ص 516-518.

الآلية، المعدات) و الثاني ذات طابع معنوي غير مرئي (المعلومات، البرامج) سواء أكانت ضحية بحد ذاتها أم وسيلة للارتكاب، كذلك استدراك النتيجة الاجرامية محتملة في كلتا الحالتين والذي يؤثر على الأمن القانوني الدولي.[21]

بناءً على ما سبق يتعين لنا تحديد الفارق الجوهري بين الجرائم المعلوماتية، الإلكترونية من حيث الدلالة والتي تتجلى فيمايلي:

استخدام شبكة الأنترنت في المعاملات الإلكترونية باتت مجالاً خصبًا للعديد من الأفعال الإجرامية التي يطلق بالجريمة الإلكترونية(cyber crime) بغض النظر عن الجريمة المعلوماتية(criminalité informatique) فلا خلاف في كل الأحوال استثناء الجرائم الإلكترونية قد تتم بربط جهاز الكمبيوتر متصلًا على شبكة الإنترنت أما الجرائم المعلوماتية فلا حاجة للاعتماد على التقنية العالية، مما يتعذر تحديد الأبعاد الفاصلة بينهما مادام القاسم المشترك يسري على الجهاز الآلي، إذ تستهدف الجرائم الإلكترونية لعلها(الابتزاز، الاحتيال، التجسس)، بالمقابل قد تندرج الجريمة المعلوماتية على البرامج والأنظمة المعالجة الآلية فلا تتأثر جديرًا بالآليات الإلكترونية التي هي من صور الاعتداء على المعلوماتية (سرقة البيانات، جرائم الملكية الفكرية، التزوير المعلوماتي).

سوف نبين أمثلة نموذجية عن تلك الجرائم وفق الجدول الموالي:(الواقع المادي إلى الفضاء الافتراضي)

[21] -السيد علي السيد محمد، الجرائم الإلكترونية، (ماهيتها، صورها، إثباتها، مكافحتها)، دار التعليم الجامعي، الإسكندرية، 2020، ص ص 21-24.

الجريمة المادية (التقليدية)	الجريمة الإلكترونية (المستحدثة)
الاحتيال	الاحتيال عبر شبكة الأنترنت الاحتيال بالمزاد والتسويق الإلكتروني
السطو	القرصنة على الأنترنت البرمجيات الخبيثة الاختراق على المواقع الالكترونية
القذف ـ السب ـ الشتم	التشهير عبر الأنترنت
الجرائم الأخلاقية الجنسية	المواقع الإباحية الدعارة عبر الأنترنت
تبييض الأموال الإتجار بالمخدرات والاعضاء البشرية	أنظمة الدفع على الشبكة إساءة الائتمان على بطاقات الدفع الإلكتروني
السرقة	الاستيلاء على المصنفات الفكرية الاعتداء على المعطيات المعلوماتية
التزوير على المحررات الرسمية	التزوير المعلوماتي ـ التوقيع الالكتروني

المطلب الثاني
الطبيعة القانونية للجريمة المعلوماتية

ثار الفقه الجنائي تساؤلاً حول الوضع القانوني للبرامج والمعطيات محل الجريمة المعلوماتية نظرًا للطبيعة التقنية المعقدة، مما طُرح جدالاً حقيقيًا في المسائل القانونية لاسيَّما الحماية الجنائية، حيث تشير المعلومة على عنصران هما التحديد والابتكار بالمقابل السرية والاستئثار، فالاعتداء على القيَّم المحمية يفترض دائما وقوعها على شيء منصبًا لحق محدد، بالرغم من ذلك هل تتم المعالجة بمنأى عن الدعامة المادية مادامت قيَّم قابلة للاستئثار وعند الاقتضاء باتت محلاً للاعتداءات القانونية ؟؟ بالمقابل هل يكفي الاعتماد بالتطبيق النصوص الجنائية التقليدية لقانون العقوبات الجزائري نحو مجابهة الإجرام المعلوماتي؟؟ كذلك هل تخضع إلى صنف الجرائم الواقعة على الأموال أم هي من طبيعة ذات نوعية مستقلة؟ وما التكييف القانوني للمعلومات؟؟

بناءً على ذلك قد سار الفقه الجنائي نحو اتجاهات متناثرة للبحث عن المدلول وطبيعة المعلومة الواردة في إطار جرائم الأموال مع الكشف عن المفاهيم الأصلية من المنظور التشريع الجنائي ومدى انطباقها على المعطيات [22].

لذا سنبين من خلال هذا المطلب الطبيعة الذاتية للمعلومات **(الفرع الأول)**، ثم نأتي للإشارة على محل الجريمة المعلوماتية **(الفرع الثاني)**، بعد ذلك نحدد مسألة حماية الأموال المعنوية من الإجرام المعلوماتي **(الفرع الثالث)**.

الفرع الأول
الطبيعة الذاتية للمعلومات

تستهدف الجرائم المعلوماتية على المعنويات دون الماديات التي ترتكب بواسطة النظام الآلي التي هي من المسائل المثارة في مجال المعلوماتية، إذ تطرح إشكالات حول

[22] -مصطفاوي عبد القادر، الآليات الجزائية الموضوعية لمواجهة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، أطروحة لنيل شهادة الدكتوراه ل. م. د في القانون العام، تخصص القانون الجنائي وعلم الإجرام، كلية الحقوق، جامعة الجزائر 1 -بن يوسف بن خدة، الجزائر،2022، ص 74.

الاعتراف بالمال المعلوماتي الذي يرجع إلى تحديد الطبيعة القانونية للجرائم المعلوماتية المسماة بالقانون الجنائي المعلوماتي.

تخضع الجريمة المعلوماتية لعقبات بالنظر إلى طبيعة المعلومة التي تنحصر على البيانات، المعطيات، البرامج، حيث يرد المال المعلوماتي على الشيء المادي إلا قد تغيَّر بالمنظور القانون الجنائي الحديث الذي بات يوصف على الأشياء ذات القيمة الاقتصادية، مما اجتهد الفقه الفرنسي على محاولة تحديد طبيعة المال المعلوماتي ذات وصف معنوي، فالأشياء المعنوية وفق المنظومة الجنائية قد أثارت جدال على الفقه الجنائي التقليدي حول مدى فعالية وقوع المال محلاً لجرائم الأموال.

إذ يرى الفقه أنَّ الأشياء المعنوية قد تنطوي على الحقوق الشخصية وتدوينها يجَّسم على قيمة مالية فالشق الأصلي معنوي بمعنى الحق أما الشق الثانوي مادي أي المحرر والمبتكرات الفنية بمثابة أشياء معنوية بحد ذاته لا تقع عليها جرائم الأموال إلا إذا احتواه المحرر لما يتضمنه من قيمة مالية محمية بمقتضى نصوص خاصة مستقلة. (23)

تجدر الإشارة إلى أنَّ المعطيات المعنوية تمثيل للمعلومة في شكل رقمي يقبله النظام المعلوماتي، فتصبح المعلومات بعد ذلك المضمون الفكري للمعطيات، مما يتبادر في الذهن تساؤل حول ما إذا كانت المعطيات والمعلومات لهما نفس المدلول القانوني؟؟ فإذا كانت المعلومات بحد ذاتها معطيات قد يصبح الاعتداء على المعطيات موازاة للاعتداء على المعلومات بدوره يرتبان نفس الأثر القانوني، أما إذ أُعتبر مفهومان متناقضين سيخلف آثار قانونية للاعتداء على المعطيات غير المعلومات، إذ أنَّ المعلومات المتداولة في البيئة الرقمية ماهي إلا معطيات تقبل المعالجة على الأنظمة الآلية مستجابة للاستيعاب. (24)

---

(23) ــ أشارت الدكتورة هدى قشقوش في إطار المحاولة لتحديد الطبيعة الخاصة للجرائم المعلوماتية ما يلي: **"يجب أن نعترف أننا بصدد ظاهرة إجرامية ذات طبيعة خاصة تتعلق بالقانون الجنائي المعلوماتي، ففي معظم حالات الارتكاب ندخل في مجال المعالجة الإلكترونية للبيانات وبالتالي تحديد الطبيعة يستلزم إضافة مجال معالجة الكلمات أو النصوص والتعامل مع المفردات الجديدة لعلها البرامج، البيانات، المعطيات، بالإضافة إلى أنَّ القانون الجنائي عاجز عن المواجهة هذا التبلور التقني الذي بدوره فشلت نصوص الحماية التقليدية وإضفاءها على حقل المعلوماتية".**

انظر/ سعيدي سليمة، حجاز بلال، جرائم المعلومات والشبكات في العصر الرقمي، دار الفكر الجامعي، الإسكندرية، 2017، ص 70-71.

(24) -محمود أحمد عبابنة، محمد معمر الرازقي، جرائم الحاسوب وأبعادها الدولية، مرجع سابق، ص 20.

ــ تؤكد التشريعات المقارنة حول مسألة إدراج البرامج المعلوماتية وفقًا للمعطيات المشمولة بالحماية، مما جاءت الاتفاقية الأوروبية لمكافحة الجرائم المعلوماتية بقولها: **"المعطيات المعلوماتية عرض للوقائع أو المفاهيم المعالجة داخل المنظومة المعلوماتية بما في ذلك البرامج التي تجعل المنظومة تؤدي الوظيفة"**

بالإحالة إلى المفاهيم التقليدية المتخذة على الفقه الجنائي قد تظل مستثناة بحد ذاتها على أيَّة قيمة ذات طبيعة خاصة تتعلق بالقانون الجنائي المعلوماتي، فلا تعد من قبيل القيم التي يرد الاعتداء عليها بينما هناك رأي معارض قد يستند على فكرة أنَّ المعلومة ذات قيمة مستحدثة، مما يتطلب تحليلاً قانونيًا لأجل تحديد طبيعة الاعتداء على المعلومة، فالاعتماد على التعاريف السالفة قد تثير على مفهوم المال من ناحية ضيقة والذي تم حصره على مكتسبات ذات قيمة مالية فقط، المتفق على الفقه أنَّ جرائم الأموال تقع على المال المادي المنقول المعبر عنه في نصوص التجريم بمصطلح **"الشيء"** ذلك غير دقيق كي يسمح لنا في التفسير، فقد تضمن المنقولات المادية محل الاعتداء لاسيَّما السرقة الذي يرد على الاختلاس أما النصب وخيانة الأمانة يرد على التسليم، فلا تتحقق إلا إذا كان الشيء ماديًا[25].

بناءً على ما سبق قد تم الإشارة إلى محل الأموال المعنوية فقهيًا، قانونيًا، فماهي الطبيعة القانونية للمعطيات المعلوماتية؟؟

حسب غالبية الفقه الجنائي قد يستند إلى أنَّ المعلومة ذات نوعية خاصة **(أولا)** بالمقابل هناك من يسند أنَّ المعلومة قيمة مستحدثة**(ثانيا)**

أولا: المعلومة ذات نوعية خاصة

أما التشريع الجزائري قد أخضعه صراحةً في القانون المتعلق بحقوق المؤلف والحقوق المجاورة رقم 05/03، إذ تم إدراج حماية قانونية نوعية على مصنفات الملكية الفكرية.

انظر/ محمود أحمد عبابنة، محمد معمر الرازقي، المرجع السابق، ص 21.

ـــ ورد المشرع الجزائري على تعريف المال في المادة الرابعة بمقتضى القانون 01/05 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتها فيما يلي: **"هي كل الممتلكات والأموال المادية وغير المادية المنقولة وغير المنقولة التي يمكن الحصول عليها، وهي كذلك الوثائق والمستندات التي تثبت ملكية تلك الأموال حيث ورد على سبيل الذكر الائتمانات المصرفية والشيكات والحوالات والأسهم والأوراق المالية والكمبيالات وخطابات الاعتماد".**

ـــ قانون رقم 05-01، المؤرخ في06فيفري2005، المتعلق بالوقاية من تبيض الأموال وتمويل الإرهاب ومكافحتها، ج.ر.ج.ج، عدد 11، الصادر في 9فيفري 2005.

-كذلك قد أشار القانون المدني إلى تحديد مدلول المال في القسم العام من خلال المادة 682 التي جاءت ما يلي: **"كل شيء غير خارج عن التعامل بطبيعته أو بحكم القانون يصلح أن يكون محلاً للحقوق المالية والأشياء التي تخرج عن التعامل بطبيعتها هي التي لا يستطيع أحد أن يستأثر بحيازتها وأما الخارجة بحكم القانون هي التي يجيز القانون أن تكون محلاً للحقوق المالية".**

ـــ أمر رقم 75-58، المؤرخ في 26 سبتمبر 1975، يتضمن القانون المدني، ج.ر.ج.ج، عدد 78، الصادر في30 سبتمبر 1975، معدل ومتمم.

ـــ إذ نستنتج أنَّ الأموال بالمنظور القانون المدني منقسمة إلى عقارات ومنقولات الواردة بمقتضى المواد 684/683 ق.م، حيث ركز المشرع على العقارات دون المنقولات، مما ترك المجال مفتوح قد يسمح باستيعاب أنواع متعددة، إلا أنَّ مدلول الأموال في التقنين المدني لم يجد قبول واسع لدى الفقه والقضاء الجزائيين نظرًا للتعارض في مسعى كلا القانونين المدني والجزائي فالأول يكاد للتنظيم والاستغلال على الملكية، بينما الثاني يسعى لحماية الملكية الفكرية، لذا كلا الجهتين تتماشى على مسار معاكس غير ملتقيان فيما بينهما.

[25] -مصطفاوي عبد القادر، مرجع سابق، ص ص 73-77.

يؤيد أنصار النظرية التقليدية أنَّ المعلومة تتمتع بالحماية القانونية من خلال اعتراف الفقه والقضاء على مسألة وجود الاعتداء أي الاستيلاء غير المشروع، ثم انتهى الى اعتبار الحق المعتدى ذو طبيعة معنوية قابلة للتملك لاسيَّما في إطار حقوق الملكية الفكرية غير ذلك لا تدخل في نطاق الحماية المقررة على الحقوق الذهنية، أما الأشياء القابلة للاستحواذ والاستئثار قد يضفي عليها القيمة المادية.

إذ يطرح التساؤل تمامًا في حالة الاستيلاء للمعلومة عن طريق الخطأ، حيث حاول الفقه الجنائي حماية المعلومات في دعوى المنافسة غير المشروعة عملاً بالمبدأ الذي أقرته محكمة النقض الفرنسية التي قضت على أنَّ: **"الغاية من دعوى المنافسة غير المشروعة هي تأمين حماية الشخص الذي لا يمكنه أن ينتفع بأي حق استثنائي"**، في حين يرى الأستاذ(Desbois) أنَّ الملكية العلمية ربما ستأتي يومًا يعترف بها صاحبه أنها لم تحصل على حق براءة الاختراع باعتبارها مستبعدة من مجال الملكية الذهنية، في حين يرى القسم التجاري لذات الهيئة القضائية أنَّ شروط المنافسة غير المشروعة غير متوفَّرة لحماية المعلومات فالأساس الذي نادى بها الفقيه(Desbois) قد تبُنى على المسؤولية التقصيرية ذلك ما اتخذته محكمة النقض الفرنسية في إحدى الأحكام القضائية، لذا جاء قرار المحكمة مؤيد لما استند اليه الفقيه(Desbois) حول مسألة الاعتراف بالحق على المعلومة في مجال الملكية العلمية.[26]

أما الأستاذ(Lucas) قد حاول تبرير الخطأ على الاستيلاء غير المشروع للمعلومة وفق نظرية الإثراء بلا سبب إلا أنَّ الحكم يرجح ذلك على أساس المسؤولية التقصيرية.

نادى الفكر التقليدي على مسألة انتفاء الأموال المنقولة معتمدًا الأسباب الواردة ما يلي:

- المعلومات غير ملموسة تتدارك إلا بالذهن
- المعلومات غير قابلة للحيازة إلا على الكيان القابل للاتصال المادي
- المعلومات غير قابلة للانتقال بالنسخ إنما المعالجة الآلية[27].

[26] -محمد على العريان، الجرائم المعلوماتية، (الجهود الدولية المبذولة في مكافحة الجرائم المعلوماتية)، دار الجامعة الجديدة، الإسكندرية،2011، ص ص 62-63.

نستخلص مما سبق أنَّ المعلومة تخضع إلى طبيعة خاصة فلا يضفي عليها الأشياء القابلة للاستحواذ والاستئثار استثناء حقوق الملكية الفكرية الخاضعة للحقوق الذهنية، في حين نادى الفقه بعدم مادية المعلومة التي لا تندرج حتمًا ضمن مجموعة القيم المحمية، فلا نفهم بأنها غير خاضعة للحماية بل معترف للفقه والقضاء، حيث سنَّ المشرع الجزائري نصوص عقابية مستقلة من خلال مراعاة الطبيعة الخاصة للمعلوماتية باعتباره أموال يستلزم المبادرة على الحماية الفعلية لمكافحة الإجرام المعلوماتي.

ثانيا: المعلومة ذات قيمة مستحدثة

تبنى الفكر الجنائي الحديث أنَّ المعلومة مستقلة عن الدعامة المادية ماهي إلا قيم مستحدثة، حيث يرى الأستاذ (Catala) **" المعلومة المستقلة على الاتصال المادي لها قيمة قابلة للاستحواذ وذلك وفقًا لتقويمها بسعر السوق متى كانت غير محظورة تجاريًا حيث ترتبط بالمؤلف على علاقة قانونية متمسكة هي بين المالك والشيء المملوك، وبالتالي أضفى وصف القيمة على المعلومة باعتباره قيمة اقتصادية بالمقابل هي رابطة التبني بين المعلومة والمؤلف مما يقودنا للإقرار بوصفها قيم مستحدثة وهو الجدير بالحماية"**، رغم أنَّ البيانات تؤخذ شكل نبضات إلكترونية مما اعتبره القضاء الفرنسي و المصري من قبيل الأشياء المادية، ذلك ما أيَّده المشرع الجزائري بشأن الكهرباء شيئًا ماديًا ملموسًا وفق المادة 3/350 قع فالمعلومة جوهر القيم المستحدثة تحمل وصف المال، لذا أحاط المشرع حماية قانونية مجسدة لكافة الاعتداءات لاسيَّما مصنفات الاعلام الآلي المتمثلة في برامج الحاسوب وقواعد البيانات استنادًا الى المادة 4 ف/أ بمقتضى القانون رقم 03-05 المتعلق بحقوق المؤلف على اعتبار برامج الحاسوب من المصنفات الأدبية، كذلك تم تنظيمه وفق المادة 44 من القانون 16-01 المتضمن للتعديل الدستوري، بذلك سار المشرع على حماية المكونات المعنوية بمثابة قيَّم مستحدثة من خلال تعديله لقانون العقوبات، قانون الإجراءات الجزائية بمقتضى نصوص مستقلة مع إدخال قواعد جديدة بالمنظومة القانونية لاسيَّما القانون المتعلق بحقوق المؤلف رقم 03-05 بمقتضى المادة 13/ لأجل إرساء الحماية الجزائية ضد جرائم تكنولوجيا الاعلام والاتصال. [28]

---

[28] - يزيد بوحليط، الجرائم الالكترونية والوقاية منها في القانون الجزائري، مرجع سابق، 51-52.

ـ راجع المادة 3/350 من الأمر رقم 66ـ 156، المؤرخ في 8 يونيو 1966، يتضمن قانون العقوبات، ج. ر. ج. ج، عدد49، الصادر في 11 يونيو 1966، معدل ومتمم.

ـ راجع المواد 4 ف/أ إلى 1/13 من الأمر رقم 03ـ05، المؤرخ في 19 جويلية 2003، ج. ر. ج. ج، عدد 44، الصادر في 23 جويلية 2003، يعدل ويتمم القانون 97ـ10، المؤرخ في 6 مارس 1997، يتعلق بحماية حقوق المؤلف والحقوق المجاورة، ج. ر. ج. ج، عدد13، الصادر في 12 مارس 1997.

نلاحظ من خلال استقراء الحجج الواردة على الفقه قد يدفعنا إلى طرح تساؤل **هل المعلومات مال أم شيء خاص أم كيان معنوي أم وعاء فارغ مرتبط بوعائها؟**

حيث نؤسس الفكرة على أنَّ المعلومة ذات طبيعة معنوية مستقلة عن الوعاء الفارغ، فالأصل عبارة عن حصيلة تراكم معرفي بشري لكل فرد حق الانتفاع والوصول إليها، مما نستنتج ذلك وفق النقاط الآتية:

- تمس المعلومات على قيمة اقتصادية قابلة للتملك أو الاستغلال غير الكيان المادي ذلك ما ساقه الأستاذ(Catala) الذي يعزز الحق على ملكية المعلومات، أما الأستاذ(Vivant) يستند إلى أنَّ المال المعلوماتي يدخل في سياق الأموال المعنوية المعترف بها مسبقًا، ذلك حينما قرر أنَّ المعلومة مالاً مبتكرًا وفق قواعد الملكية الأدبية الفنية.

- المعلومة موضعًا للاستئثار المعنوي بما في ذلك البرامج في جوهره معلومات تستحق الاعتراف على الحماية القانونية من خلال شموليته، نطاقه، فعاليته، فالإقرار على الحق في المعلومات يوجب مبادئ كفالة لحرية الوصول إليها في إطار قانوني نظرًا لإخضاعه على التصرفات المعنوية قد تؤدي لانتهاك الخصوصية. [29]

بناءً على الآراء الفقهية المقدمة حول الطبيعة القانونية للمعلوماتية، إذ هناك من ينشد فكرة الاعتراف بالمال المعلوماتي ذات طبيعة خاصة ليست بالأشياء القابلة للاستحواذ، كما هناك من يعارض ذلك باعتبار المعلومات قيم مستحدثه نظرًا لارتباطه على حقائق جديدة لعلها البرامج، البيانات التي تدخل في حيزها المعلومات بواسطة المعالجة الآلية للنظام، فالإقرار بصلاحية الحماية الجزائية على المعلومات وفق نصوص جرائم الأموال، كذلك تم اسباغ الحماية وفق القانون رقم 03ــ 05 بشأن مصنفات الإعلام الآلي، بذلك يكون المشرع قد عالج الفراغ التشريعي بتعديل القواعد العامة وفق أحكام جديدة في مجال الإجرام المعلوماتي حيث نسعى القول كيفما تدارك الأمر واتُخذ بعين الاعتبار للفقه

ــ تنص المادة 44 بمقتضى القانون 16-01 المتعلق بالتعديل الدستوري ما يلي: **"حرية الابتكار الفكري الفني العلمي مضمونة للمواطن، حقوق المؤلف يحميه القانون"**

ـ دستور الجمهورية الجزائرية الديمقراطية الشعبية لسنة 1996، الصادر بموجب المرسوم الرئاسي رقم 96- 438، المؤرخ في 7 ديسمبر 1996، ج. ر. ج. ج. عدد 76، الصادر في 8 ديسمبر 1996، معدل بالقانون رقم 16- 01، المؤرخ في 6 مارس 2016، ج. ر. ج. ج، عدد 14، المؤرخة في 7 مارس 2016.

[29] - محمد على العريان، الجرائم المعلوماتية، مرجع سابق، ص 63.

والقانون حول الكيان المادي إلا قد تم الاعتراف بالحماية المقررة له، مما يستوجب معاملته على نحو غاية تامة وفي إطار ثابت.

الفرع الثاني
محل الجريمة المعلوماتية

تعتبر المعلومة شجون الحاضر وغموض المستقبل في ظل الوقت الراهن، إذ أفرزت مجتمعًا تقنيًا راجع إلى سمات متجليَّة من حيث الكمية التخزينية العالية، النوعية، سرعة التداول، فلا نتصور نشاط استثماري ناجح دون توظيف المعلومة آلية مساعدة لتحقيق المشاريع الميدانية، إلا أنَّ الإغراء في استخداماتها قد تؤدي إلى تمادي الإجرام نتيجة الاتصال بالشبكات الرقمية على أنظمتها المعلوماتية. [30]

إذ تستهدف الجرائم المعلوماتية إحدى التيارات الأتية: المعلومات **(أولا)**، الأجهزة **(ثانيا)**، الجهات **(ثالثا)**.

أولا: المعلومات

تُشتَّق المعلوماتية من مرادفات متصلة بالعلم لاسيَّما اليقين، الإرشاد، التوعية، أما مصطلح(Information) يقصد بذلك عملية الاتصال، حيث ترتبط المعلومات بالبيانات والمسماة بالدورة الاستدراجية نظرًا إلى الوظيفة المؤدية من خلال عملية المعالجة، التشغيل، التحويل بواسطة النظام الآلي بعدما كانت تتداول على الأرشيف فلا تتأثر بالكشف عنها، في حين المعلومات المخزنة قد تؤدي لأضرار مؤكدة إذا لم يسري الفرد على التستر كيفما قررت الدساتير والقوانين المنظمة.

إذ يقع محل الجريمة المعلوماتية سواء على السرقة، التغيير، المحو، الإتلاف التي تكون غالبًا ذات قيمة مادية أم معنوية، مما ضاعف المشرع الجزائري الجزاء المقرر بالنسبة لأفعال التغيير، المحو، التعديل وفق المادة 394 مكرر ف 3/2 بمقتضى القانون رقم 04-15المعدل لقانون العقوبات. [31]

---

[30] -شنتير خضرة، الآليات القانونية لمكافحة الجريمة الإلكترونية، (دراسة مقارنة)، أطروحة مقدمة لنيل شهادة الدكتوراه الطور الثالث (ل.م.د)، تخصص القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية-أدرار، الجزائر، 2021، ص 19.

[31] - تنص المادة 394مكرر 3/2 بمقتضى القانون 04-15ما يلي:**" تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب النظام اشتغال المنظومة و تكون العقوبة بالحبس من ستة أشهر 06 إلى سنتين 02 و غرامة من 50.0000إلى 150.0000دج "**

ثانيا: الأجهزة

توصف الأدوات الحاسوبية مسارًا عابرًا نحو الولوج إلى الشبكات الآلية ووسيلة مساعدة لإدراج المعلومات داخل النظام، مما يقتضي حمايتها من الاعتداءات الماسة عليها، حيث تسري محلاً للجريمة المعلوماتية من خلال عملية تعطيل الأجهزة بواسطة إرسال فيروسات أو برامج تحوي على أنظمة هجومية قد تؤدي إلى تلف النظم أو شلل للأنشطة المرتبطة بها، كذلك يتم وقوعها على المكونات المنطقية الذي يُستلزم خبرة فنية عالية في مجال البرمجة).

إذ عاقب كلا من التشريع الفرنسي والجزائري على تعمُّد إدخال الفيروسات المعلوماتية في برنامج الغير مع الامتناع عن إخباره ولو حصل بصفة عرضية أو تم تعديل المعطيات المعالجة آليًا حتمًا يدخل في دائرة التجريم الواردة بمقتضى المواد 323 قع. ف/ 394 مكرر1 قع. ج، فالحكمة من التجريم يتجلى في توفير الحماية على العتاد تشغيل المنظومة المعلوماتية [32].

ثالثا: الجهات

اكتسحت العولمة الرقمية نحو تفاعل استخدامات شبكة الإنترنت التي باتت على دور القيادة في شتى الميادين، حيث مازالت متذبذبة بين الإيجابية والسلبية لما قد تتجاوز تلك الرعونة إلى الأجهزة الرقابية للدولة بدوره يؤثر على المنظومة القانونية، مما تظل الحماية الهادفة بغير الكفاية مقارنة عن تضخم الإجرام المعلوماتي، ثم أنَّ النصوص التقليدية السارية المفعول عسيرة في المجال التقني.[33]

يقتضي مبادرة مستحقة من المشرع الجزائري في سن قوانين مكملة في إطار المعلوماتية والسعي نحو التعاون الدولي لحماية المنظومة الجنائية مع صون حلول راسخة للحفاظ على الأمن المعلوماتي.

العقوبة المقصودة قد أوردتها الفقرة الأولى من المادة 394مكرر " يعاقب بالحبس من ثلاث أشهر إلى سنة وغرامة من 50.0000إلى 100.000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من المنظومة المعالجة الآلية للمعطيات أو يحاول ذلك"

ـ القانون 04ـــ15، المؤرخ في 10 نوفمبر 2004، المتضمن لتعديل قانون العقوبات، (ج. ر. عدد 71)، سالف الذكر.

[32] -شيخي عائشة، عياشي بوزيان، "الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وأشكالها الاقتصادية وآليات مكافحتها"، **"مجلة الدراسات الحقوقية"**، المجلد 2، العدد 2، كلية الحقوق والعلوم السياسية، جامعة الدكتور مولاي الطاهر-سعيدة، الجزائر، 2015، ص ص 149-184.

(37) ـ عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت، (دراسة مقارنة)، منشورات الحلبي الحقوقية، بيروت، 2007 ص ص 18-20.

الفرع الثالث
صلاحية الحماية على الأموال المعنوية من الجرائم المعلوماتية

غيَّرت المعلوماتية شتى المفاهيم القانونية التقليدية لاسَّيما السياسة الجنائية نظرًا لإبراز قيَّم مستحدثة محلها المعطيات، فقد اصطبغت على تسمية القرصنة المعلوماتية التي نالت موضوعًا جديرًا للحماية الجزائية، إذ حاول الفقه الجنائي تكييفها على اعتداء للأفكار بعدما كانت النصوص الجنائية لجرائم تقليد المصنفات الأدبية إحدى الحلول التي تطال على مواجهة المعلوماتية، مما أُعتبر الكيانات الطبيعية للحاسوب مال مادي منقول ذات قيمة للاستئثار تصلح لتطبيق النصوص التقليدية المنظمة لجرائم الأموال.

حيث أدى إلى بروز فراغ تشريعي قد يؤثر على أزمة القانون الجنائي في مواجهة واقع المعلوماتية التي يفرض البحث عن حلول ملائمة للحد من الاشكالات المقيدة على الفقه والقضاء، ذلك بمراعاة الشرعية الجنائية التي تتفرع على مبدأي التفسير الضيق وحظر القياس في مجال التجريم.

لذا يُطرح التساؤل تمامًا بمدى امكانية استعانة القاضي الجزائي لنصوص جرائم الأموال كمبدأ استثنائي يحقق حماية جنائية على المعلوماتية؟ وهل تُفلح تلك النصوص الجنائية على المال المعنوي باعتباره محلاً لجرائم الإعلام الآلي؟؟

حيث أتى المشرع الجزائري بمقتضى القانون 04-15 المعدل لقانون العقوبات نصوص جديدة مستقلة تكفل بحماية مصنفات الإعلام الآلي، بالإضافة إلى النصوص التقليدية لجرائم الأموال كذلك القوانين المنظمة للملكية الفكرية بمثابة البرامج منتجات فكرية، ذلك بغية التصدي على الإجرام المعلوماتي.[34]

مما كرَّس على حماية المصنفات الفكرية بمقتضى القانون 03ــ 05 المتعلق بحقوق المؤلف استنادًا إلى المواد 159/153، بعدما كانت خاضعة لقيود قانون العقوبات الواردة **في القسم التاسع تحت عنوان "جنح التعدي على الملكية الأدبية والفنية" من**

ـــ تجدر الإشارة على إلقاء القبض لشاب فرنسي البالغ من العمر 23 سنة، إذ تمكن من الوصول إلى حسابات توتير الخاصة بشخصيات أمريكية وعلى إثر ذلك تم الحكم عليه لمدة 5 أشهر مع وقف التنفيذ.

Voir/ BAILLY Emilie, EMMANUEL Daoud, *« cyber criminalité et réseaux sociaux la repense pénale, la base de données juridique »*, éditions Dalloz, France, AJ pénale, 2012, p .252

(38) - عمري فيصل، " الحماية الجنائية للمعلوماتية في التشريع الجزائري"، **"مجلة آفاق للعلوم"**، المجلد 7، العدد 1، كلية العلوم الإنسانية والاجتماعية، جامعة زيان عاشور، الجلفة، الجزائر، 2022، ص466.

الفصل الثالث الخاص بالجنايات والجنح ضد الأموال" وفق المواد 394/390 بشأن الاعتداءات الواقعة على حقوق الملكية الأدبية الفنية ثم أخرجت من مظلتها لما لها تجريم مستقل في إطار حقوق المؤلف، بالمقابل استقر القضاء على اعتبار البرامج المعلوماتية منتجات فكرية تندرج ضمن نصوص المنظمة على الملكية الفكرية. (35)

إذ أولى المشرع حماية جزائية مستحقة على مصنفات الإعلام الآلي نظرًا إلى نسبية الحماية بمقتضى نصوص جرائم الأموال، حيث تم اعتراف المشرع على برامج الحاسب الآلي واستبعاد القانون المتعلق ببراءة الاختراع فلا جدوى من تطبيق مصنفات الاعلام الآلي، بخلاف الأجهزة المادية يكفي حمايتها في إطار نصوص جرائم الأموال، لذا نتساءل ما مدى اعتبار الكيان المعنوي ذات وصف المال؟ وهل هي كافيةً بالتصدي على الاعتداءات الواقعة للمعلوماتية أم يستوجب التدعيم بقواعد التجريم جديدة تتناسب مع الطبيعة الخاصة لبيئة النظام الآلي؟؟ رغم ذلك تظل مسألة جدال بمدى تطبيق قواعد التجريم التقليدية على الأموال المعنوية مادام برامج الحاسب الآلي دعامة مثبتة ذات قيمة اقتصادية على صفة المال، فإذا إذا كانت مستقلة فلا يصدق عليها وصف المال استنادًا الى المبادئ التقليدية أما إذا كانت مسجلة على الدعامة قد تصلح محلاً لجرائم الأموال، بالمقابل هل تدخل البرامج تحت مدلول الشيء المنقول محلًا لجرائم الأموال؟

نستند على مدى اعتبار البرامج مالاً بصدد جريمة السرقة الواردة بمقتضى المادة 350 قع، إذ لم تشترط أن يكون المال موضوعًا للجريمة فقد تقع على الكيانات المادية أو المعنوية حسب ما ورد في المادة 350 قع، مما يجعل وقوع المال المعنوي أمرًا لا يصطدم بمبدأ الشرعية الجنائية بصدد جريمة السرقة بينما يساغ الرأي لدى الفقه باعتبار البرنامج مالاً بصدد جرائم الأموال، مما يصلح محلاً للسرقة على احتمال ضئيل جدًا، ذلك التفسير مسلم بالمنظور التشريع الجزائري.

أما اعتبار البرنامج مالًا بصدد جريمة النصب استنادًا إلى المواد 373/372 قع يبين أنَّ الأشياء المادية المنقولة قد تصلح محلاً لجريمة النصب لاسيَّما الواردة على سبيل

(39) ـ بركان فضيلة،" حماية حقوق المؤلف والحقوق المجاورة في الجزائر"، **"مجلة الدراسات القانونية"**، المجلد 8، العدد 1، كلية الحقوق والعلوم السياسية، جامعة يحيى فارس، المدية، الجزائر،2022، ص300.

ــ راجع المواد 151 إلى 159من القانون رقم 03ـــ05، المؤرخ في 19 جويلية 2003، المتعلق بحقوق المؤلف والحقوق المجاورة (ج. ر. عدد 44)، سالف الذكر.

ــ راجع المواد 390 إلى 394 من القانون رقم 04ـــ 15، المؤرخ في 10 نوفمبر 2004، المعدل لقانون العقوبات، سالف الذكر.

الحصر بمقتضى المادة 372 قع، إذ لم يحدد المشرع صراحةً على طبيعة المنقول بل سعى إلى إدخال برامج الحاسب ضمن الأشياء الواقعة على جريمة النصب، بالمقابل يتضح أنَّ المشرع لم يقيَّد حتمًا من نطاق مفهوم المال فقد تكون الأشياء المعنوية محلاً للنصب وفق النصوص التقليدية مما تسبق عقبات مثارة لانعدام نشاط مادي ملموس.

إذ بالرجوع إلى المادة 376 قع التي تنص على جرائم خيانة الأمانة مما نلاحظ وقوع الاعتداء إلا على الأموال المنقولة المحددة على سبيل الحصر فلا مجال لوقوع الأشياء المعنوية وفق نصوص جريمة خيانة الأمانة، أما اعتبار البرامج محلاً للجريمة قد يظل رأي غير مرهون للإعمال به مطلقًا، حتى يتم هناك إحداث تغيير من قبل المشرع سواء التعديل أو الإلغاء بغرض التوسيع من نطاقها دون قيد، لذلك قد يؤدي تطبيق جرائم النصب وخيانة الأمانة على مجال المعلوماتية في حيز نسبي جدًا. [36]

بناءً على ما سبق يتبين مدى انطباق الكيانات المعنوية محلاً للاعتداء بمقتضى نصوص جرائم الأموال أمرًا عسيرًا في التعامل مع التقنيات الآلية، إلا إذا وردت نصوص التجريم قد تتوافق مع الطبيعة المعلوماتية، مما نستدرك من ناحية الحماية المنظمة لجرائم الأموال لاسيَّما جرائم الإتلاف والسرقة قد يحقق حماية جنائية ثابتة ضد الإجرام المعلوماتي خلافًا عن النصب وخيانة الأمانة توفر حماية ضئيلة جدًا.

إذ استدعى تدخلًا تشريعيًا لأجل تدارك الفراغ القانوني، حيث تم إصدار مشروع تعديل قانون العقوبات لقمع الاعتداءات الواردة على المنظومة المعلوماتية، مما استدرج نصوص عقابية بمقتضى القانون رقم 04-15 إلا لما الغاية لحماية المال المعنوي على المنظومة الجنائية، بالمقابل نلاحظ أن المشرع ركز على الاعتداءات الماسة بالأنظمة المعلوماتية وأغفل للاعتداءات الماسة بمنتوجات الإعلام الآلي لاسيَّما التزوير المعلوماتي الذي يتطلب حماية حاسمة للمجابهة نظرًا لاستفحال الإجرام، أما الطبيعة القانونية تم الإشارة إليها في المادة الثانية بمقتضى **القانون09ـــ04 المتعلق بتكنولوجيا الإعلام و الاتصال** فقد تؤثر طبيعة المعطيات على التكييف القانوني خلافًا على الاعتداءات الواقعة بمنتوجات الإعلام ذات دعامة معنوية من صور الغش المعلوماتي نظرًا إلى الدور الذي يؤديه على الحاسب الآلي، إلا أنَّ المشرع أُسند أفعال التزوير على المحرر غير المعلوماتية لما يقتضي مراجعة منظومته القانونية من خلال التعديل أو ادراج نص خاص متعلق بالتزوير المعلوماتي.

---

(36) - حفيظة رفاس، "الحماية الجزائية من جرائم المعلوماتية في القانون الجزائي الجزائري"، **"مجلة البحوث القانونية السياسية"**، المجلد 2، العدد 10، كلية الحقوق والعلوم السياسية، جامعة مولاي الطاهر، سعيدة-الجزائر،2018، ص503.

ما يسعى بنا القول أنَّ المشرع لم يراعي ذلك النمط من الإجرام الواقع على المنظومة المعلوماتية نظرًا لما تحمله من جسامة ناهيك عن الحماية التي قد نتساءل إذ ما يجدر تطبيق النصوص الواردة في قانون العقوبات على الاعتداءات الماسة بمنتوجات الإعلام الآلي لاسيَّما التزوير، حيث تظل مسألة محصورة نسبيًا لمكافحة الإجرام المعلوماتي وفق المنظومة القانونية الجزائرية.

المـــطـلـب الثـــالـــث
الـــمجـــــرم المـــعلـــومـــاتي

يرتبط جوهر الإجرام المعلوماتي بشخصية المجرم و الدوافع الإجرامية التي يتم من خلالها إستغلال الآليات التقنية وإثارة المتعة عند الفحص عن كثب النظام الآلي أو ملحقات الأدوات الرقمية أيًّا كانت طبيعتها، حيث يرجع الأمر إلى القدرة الدماغية لدى المجرم في التحكم بالديناميكية الآلية غير حاملاً على سلاح الجريمة أي الإستغناء عن العنف المادي، إذ ينفرد على تقنية المعلومات التي قد ينظر إليها أداة محايدة بالمقابل مصدر إنتهاك تساهم في إسقاط على خانة الإجرام الواقعة بالأنظمة المعلوماتية، مما حُظيت أبحاث علم الإجرام على محاولة كشف النقاب لفكرة المجرم المعلوماتي باللجوء إلى ارتكاب الإجرام داخل الفضاء الرقمي والذي أُثير انتباه الباحثين في المجال القانوني لذاك النمط من السلوك غير المشروع و رسم نموذج جديد في علم الإجرام الجنائي إضافة إلى الدراسات السيكولوجية التي أثبتت مشروعية الشعور بالطبيعة الإجرامية و الأفعال المقترفة بعدم استحقاقهم للعقاب و مدى تبريره على جسامة الجرم لهؤلاء المجرمين.

لذلك يتعين علينا تحديد السمات الخاصة للمجرم المعلوماتي **(الفرع الأول)**، ثم نبين أصناف مجرمي المعلوماتية **(الفرع الثاني)**، بعد ذلك نعرج عن الضحية في الجريمة المعلوماتية **(الفرع الثالث)**.

الفرع الأول
سمات المجرم المعلوماتي

رغم الحقيقة المشارة في دراسات علم الإجرام بشأن تحديد شخصية المجرم من خلال إثبات السمات المشتركة والدوافع المؤدية إلى ممارسة الوظيفة الإجرامية على الحيز الافتراضي معتمدًا تقنية المعلومات، مما يتعذر الالمام بمداها نظرًا لحجم وقوعها ذات أثر بالغ على الأمن الدولي.

حيث يتبين أنَّ هناك سلالة ماهرة تتمتع بالدهاء والذكاء عالي المستوى، كذلك الدراية على معرفة الأنظمة التقنية وكيفية سيرها استجابةً للذهن، فلا يستوعبه شخص بسيط متوسط الخبرة.

إذ يلجأ إلى تنفيذ الإجرام بفعل تقنيات خفية بواسطة التدمير الناعمة أي التلاعب والعبث على البيانات المخزنة في النظام المعلوماتي، مما يتحدى تلك العقبات التقنية من خلال تغيير نواياه إلى لغة رقمية في هيئة محجوبة تتأثر بفضل مساعي الشبكة المعلوماتية، بالرغم من ذلك تظل محلًا للعديد من الإشكالات يتطلب التأصيل بالبحث والدراسة من أجل انتقاء حلول هادفة على المجال القانوني[37]

لذا يجدر بنا اجمال تلك الخصائص أو الصفات المتعلقة بالمجرم المعلوماتي عن المجرم العادي والمبينة فيمايلي:

أولا: الاحترافية

يتمتع المجرم المعلوماتي بدرجة من المهارة ، الخبرة ، المعرفة التقنية، الشعور بالعظمى ضد الغير يصنف ضمن طائفة نوابغ المعلوماتية مع انتمائه إلى الطبقة المثقفة

---

(37) -بكوش محمد أمين، هروال نبيلة هبة، **"**خصوصية المجرم الالكتروني**"** (مجرم الأنترنت نموذجًا)، "**مجلة البحوث في الحقوق والعلوم السياسية"**، المجلد 7، العدد 1، كلية الحقوق والعلوم السياسية، جامعة ابن خلدون، تيارت، الجزائر، 2021، ص78.

ـ نستند للإشارة إلى مصطلح المجرم المعلوماتي حسب الكاتب الخيال العلمي الأمريكي **"ويليم جيبسون"** الذي **"أقرَّ بأن شخصية المجرم المعلوماتي مرتبط بالطلاب المختصين في مجال علوم الحوسبة أو المهووس بالتقنية، فلا يستهدف سوى اختبار في مواجهة النظم المعلوماتية، فقد تظل فكرة جديدة للفقه الجنائي، وفي الجرائم المعلوماتية لسنا بصدد سارق أو محتال عادي لكننا أمام مجرم رقمي له دراية بالتقنية ويستغلها للاعتداء على الشبكة المعلوماتية".**

ــ كما تسبق الإشارة إلى أنَّ شخصية المجرم مزيج بين الملامح والدوافع، فلا يميل لفئة واحدة أو دافع معين بل يعتمد التصنيف على مدى جسامته الاجرامية، الباعث المحفز، مما يساعد الأجهزة الأمنية في كشف ستاره بملاحقتهم نظرًا إلى صعوبة التعامل في مجال التقني مع استحالة إحصاء العدد الحقيقي للجرائم، بالمقابل انعدام رؤية الطابع الخفي على الاتصال المباشر بين الضحية والمجرم قد يجعله عائقا للجهات الأمنية.

انظر/ مراد دمشوش، شول بن شهرة، " السمات الخاصة للجريمة المعلوماتية"، " مجلة المستقبل للدراسات القانونية والسياسية، معهد الحقوق والعلوم السياسية، المركز الجامعي أفلو، الأغواط، الجزائر، 2020، ص15.

برغبة جامحة و التحدي على الحيلة التقليدية، مما يهوي إلى الكشف عن سرية النظام الآلي و الاستحواذ على معدات الشبكة الرقمية ، فلا يحتاج لأدنى مجهود عضلي التي تحدد أسلوب الارتكاب، إذ ينفذ عملية النشاط الاجرامي في هدوء حتى لا تترك أثر مادي واضح قد يساعد الأجهزة الأمنية في البحث عن الأدلة، فكلما قللت المعرفة كلما اتسعت إلى التعقيد عن الإثبات لدى الأمن القانوني، فلا يتصور التعامل مع الخوارزميات الآلية إلا على الأدمغة الناشطة دون البؤساء لما يمتلكون ندرة ضئيلة عن المعرفة الفنية للخوض في عالم الإجرام المعلوماتي حيث تَحفظَّ الفقه حِيَّل رسم هيئة المجرم المعلوماتي بشأن إسناده لأنماط الإجرام (الإتلاف، تدمير النظام الآلي، سرقة المعطيات المخزنة) بالنظر لما يؤسسه الواقع، حيث أراد تحقيق الغاية عن شغف حتى لا يفاجئ بأمور غير متوقعة بشأنها تحال على إفشال مخططاته الإجرامية [38].

ثانيا: التخوف على كشف الجريمة

تُصاحب الرهبة على المجرم المعلوماتي جراء انفضاح أفعاله الخبيثة ما يترتب من فقدان مركزه

لاسيَّما ذوي الكفاءات المرموقة، مما تساعد الحفاظ على سرية الأعمال وطبيعة الأنظمة المعلوماتية، فالخوف الذي ينتب المجرم راجع إلى التكييف الاجتماعي حسب رأي(Bismuth) شخصية حادة جدا بالاتصال مع الفضاء المعلوماتي ورسم حدوده المعروفة بالمنطقة الذاتية المؤقتة، لذا أثبتت الدراسات في تبرير ارتكاب الإجرام عائدًا لعدم مشروعية المجرم على الأخلاقية لاسيَّما الحالات التي يقف عند القهر للأنظمة وتخطى الحماية الأمنية المفروضة لما تلحق إضرار بالأشخاص على العدوانية مع الاستيلاء على الأنظمة الآلية للمؤسسات متحملًا ذلك النتائج المسجلة، بالمقابل التعاود على الاجرام قد يؤدي إلى الكشف عن الثغرات الخفية ولو لم يفلح في سدها مما سيضبط جليًا ويقاد لمحاكمته، فلا تنفي تلك الصفات بكونه مجرمًا وحدود جريمته افتراضية رقمية، بل تضفى على أساس ارتكاب سلوك إجرامي لابَّد من إقامة المسؤولية الجزائية ، أما عن عدم الميل إلى العنف قد يتصف المجرم المعلوماتي بالسهولة خلال تنفيذ جريمته دون اللجوء الى العنف المادي كما هو الحال لدى المجرم العادي، إذ ينتمي إلى جرائم الحيلة الذي يتطلب تحديًا على الشبكات التقنية بغرض كسب المبتغى، حيث ترتكب عادة من شخصين إحداهما يراعي الجانب الفني للمشروع الإجرامي والثاني يغطي عملية التلاعب

(38) –CHAWKI Mohamed، *«la cyber criminalité combattre»*، édition 2، Paris، 2009، p75.

مع تحويل المكاسب المادية فأحيانًا يتم تجنيد المجرم ضمن عقبات الجريمة المنظمة عبر شبكة الإنترنت [39].

لذا يرمز الأستاذ باركر أحد الباحثين الذين عانوا على الإجرام المعلوماتي عامة وسلوك المجرم خاصةً في تحديد السمات المشتركة لهؤلاء المجرمين برمز **(S.K.A.R. M)** [40].

الفرع الثاني
أصناف المجرم المعلوماتي

دار البحث بشأن تصنيف مجرمي المعلوماتية باعتباره من المسائل الموضوعية المستوجبة للضبط نحو مسلك الردع والمكافحة، إذ توصَّلت الأبحاث إلى التصنيف الأمثل القائم على أساس الاعتداء من غير التكتيك على الوسائط، مما أورد كلا من **(WILLIAM VONSTAR, KARLSE GRE, DAVID L'OVER)** في مؤلفاتهم جرائم الكمبيوتر الصادر عام 1995 الذي تم تقسيم مجرمي المعلوماتية إلى ثلاث طوائف **القراصنة(المخترقون، المحترفون، الحاقدون)،صغار نوابغ المعلوماتية، مجرمي الجريمة المنظمة،** فلا نعني لكل مجرم يندرج تحت فئة محددة بل مزيج فحسب دراسة ميدان السلوك الإجرامي قد تتعدد أنماط المجرمين إلى سبع فئات المبينة فيمايلي: [41].

---

[39] -هشام بشير، "الآليات الدولية لمكافحة الجريمة الإلكترونية"، بحث مقدم إلى المركز الدولي للدراسات المستقبلية والاستراتيجية، (قضايا محاولة لبلورة تطورات جارية)، مصر، 2004، ص 13.

[40] -حدد الأستاذ باركر السمات المشتركة للمجرم المعلوماتي والمبينة فيمايلي:

ـ المهارة(SKils) تتطلب تنفيذ النشاط الإجرامي التي قد يتلقاه إما بالكفاءة المتخصصة، الخبرة التقنية، التفاعل الاجتماعي.

ـ المعرفة (KNOWLEDGE)مرتبط بالظروف المحاطة للجريمة على مدى إمكانية التحقيق أو احتمال الفشل، وبالتالي استطاعة المجرم وضع تصورًا مماثلاً للإجرام نظرًا للمسرح الذي يمارس فيها الوظيفة وفق الأنظمة الآلية المستهدفة قبل نفاذ الجريمة.

ـ السلطة(AUTHORITY) المزايا التي يتمتع بها المجرم لارتكاب الإجرام، حيث تتمحور على شفرة الدخول للنظام المعلوماتي، مما تفتح منافع متعددة من خلال إجراء التعاملات الإلكترونية.

ـ الوسيلة(RESOURCES) يراد بالحاجيات المزودة للفاعل بإتمام العملية الإجرامية أي التلاعب بالأنظمة المعلوماتية والتحكم باستخدام شبكة التقنية العالية، فكلما كان النظام المعلوماتي على خصوصية غير مألوفة باتت عائقًا لتحديات المجرم

ـ الباعث(MOTIVES) أي الإرادة والعزيمة للفاعل كذلك الرغبة إلى تحقيق مكاسب مادية بطرق غير مشروعة، حيث يأتي الباعث ثم القهر للأنظمة الآلية وتخطي الحواجز الأمنية بعد ذلك الانتقام سواء على الأشخاص أو المؤسسات ما يطلق بأعراض روبن The Roben Hood Syndrome.

انظر/ سهام خليلي، **"خصوصية المجرم الالكتروني"، " مجلة المفكر"**، المجلد 12، العدد 2، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2017، ص 413.

[41]-غريبي بشرى، **"خصوصية المجرم المعلوماتي ودوافعه"، "مجلة نوميروس الأكاديمية"**، المجلد 2، العدد 2، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد-تلمسان، الجزائر، 2021، ص 105.

أولا: صغار نوابغ المعلوماتية (the Criminally Négligence/LESBLAGUEURS)

هم الشباب البالغين المفتون بالأنظمة المعلوماتية إلا هناك فئة مازالت دون سن الأهلية مولعين بالحوسبة والاتصال، فحسب الدراسات الاستطلاعية الإعلامية التقنية قد توصف بمصطلح **المتلعثمين** الدال على الصغار المتحمسين بالأجهزة الألية والشعور بالبهجة، دافعهم التحدي، الشغف، الفضول، المغامرة، الاثارة، إذ تتعدى تلك الفئة مرحلة الهواية، العبث لتدخل إلى مرحلة الاحتراف على ارتكاب الجرائم المعلوماتية، إذ هناك مخاوف لاحتضانهم عصابات الجريمة المنظمة الذين قد يستفيدوا من مهاراتهم في تناصر خدمة أمن المعلومات ووسائل الحماية الأمنية و من أشهر المدافعين عن الهاكرز الصغار **"هيوج كورن"** [(42)].

ثانيا: القرصنة (HACKERS)

هم المبرمجون المحترفون ذوي الخبرة في المجال التقني، يهدفون إلى اقتحام الأنظمة مع خرق الحواجز الأمنية المحيطة بالشبكات، مما يصنف إلى عدة فئات متسلسلة فيما يلي:

القراصنة الهواة المسمى بـ**(HACKERS)**هم المتطفلون، المتسللون، العابثين الذين يتحدون إجراءات أمن الشبكات، إذ يستغلون على اختراق الأنظمة التقنية بدافع التحدي، القدرة الذاتية، مما يمارسون مواهبهم لغرض المعرفة، الشغف، اللهو فلا يستبعد على احتمال انزلاق هذه الفئة بمجرد هواة إلى محترفين، فقد لا يدركون المخاطر المحتملة التي تؤديها أفعالهم غير المشروعة، عادة ما تكون من فئة التلاميذ أو طلبة الجامعة النجباء في علوم تكنولوجيا الاتصالات أو الشباب العاطلين عن العمل فلا يميلون نحو رغبة حاقدة أو تخريبية.

أما القراصنة المخترقون المسمى بـ **(CRACKERS)** هم المقتحمون، المحللون قد يكونون الشباب البالغ من العمر 25 سنة أو المهنيون ذوي الاختصاص التقني

(42) -على قابوسة، "الجريمة الإلكترونية في الفضاء الإلكتروني"، (المفهوم والأسباب، سبل المكافحة مع التعرض لحالة ليبيا) "**مجلة آفاق البحوث والدراسات**"، المجلد 2، العدد 4، كلية العلوم الاقتصادية، جامعة اليزي، الجزائر، 2019، ص 247.

الذين يستخدمون برامج في محاولات الاختراق بغرض الحصول على المعلومات السرية، الاقتحام على الشبكات الأمنية، التلاعب بالمواقع، الاستيلاء على البطاقات الائتمانية، مما تعاكس رؤية هاجسه تبنى عن ميولات إجرامية مقارنة بالهاكرز قد يطلق عليهم **بالعناكب(Spiders)**، فالدافع المحفز لهم تحقيق مكاسب مادية على الجهات المكلفة كذلك الدعاية و الإعلام داخل الفضاء الافتراضي، فلا يخفى عن فئة الكراكرز المبتدئون الذين يستخدمون برامج الإتلاف بدون دراية، إذ ينتهي الأمر بين أيدي الأمن السيبراني كونهم سطحيين في إخفاء معالم الجريمة.

ثالثا: مجرمي المعلوماتية في الجريمة المنظمة (Personnel problème subers)

تتخذ المنظمات الإجرامية هيكل موزع محدد على عائدة أنشطتها الإجرامية إلى الأعضاء، مما بات يطلق عليها **عصابات المافيا**، بالرغم من دخول المنظمة في الفضاء الرقمي اتسعت عائدة الجريمة نظرًا لاحتكاك بالشبكات التقنية العالية تؤدي الى تشكيل هيئات إجرامية منظمة بدافع الجشع وتحطيم أرباح هائلة. [43]

الفرع الثالث
الضحية في الجريمة المعلوماتية

يلعب الضحية دور مستهان بغير إرادة صريحة قد تكون على شخصية غير متجلية أمام الجاني الذي يرى سوى الحاسبات الإلكترونية دون تدارك القيمة المستوحاة على الواقع، بالمقابل التأثير في إحداث الجريمة على المسرح الافتراضي دون الانتباه في معرفة المرآة الحقيقية للدوافع التي قد يناصرها في التحكم على تنفيذ الخطط الإجرامية،

---

(43) -يونس عرب، جرائم الكمبيوتر والإنترنت، (المعنى والخصائص والصور واستراتيجيات المواجهة القانونية)، على الموقع الالكتروني: http://www.arablawa.org، تم الاطلاع عليه يوم:14أفريل 2023 على: 12سا و30د.

-تجدر الإشارة لقضايا شهيرة عن جرائم الحوسبة المرتكبة ضمن فئة الصغار المعلوماتية تتلخص فيما يلي:

-الحدث ماكسوس البالغ من العمر 18 سنة قد اتهم بالاستيلاء على بطاقات الائتمان والأرصدة الحسابية من خلال شبكة الأنترنت، حيث تم سرقة الآلاف من البطاقات للزبائن في إحدى مواقع الشراء عبر الإنترنت ونشرها على تلك الشبكة، مما أثارت ذعرًا لدى البنوك الأمريكية من أوسع عمليات السطو عبر الأنترنت.

-محاولة قرصان أمريكي اللذان لم يتجاوزا 12 عام على اختراق نظام وزارة الدفاع الأمريكي البنتاجون غير عابئ بالنظام الحماية عالية التقنية فكان بالإمكان تعريض البشرية للإبادة لو تم الوصول للمخزون النووي بفك الشفرة الخاصة وضبطها وتصويب القنابل النووية.

انظر د/عبد الفتاح بيومي حجازي، الأحداث والأنترنت، (دراسة متعمقة عن أثر الإنترنت في انحراف الأحداث)، دار الفكر الجامعي، الإسكندرية، 2004، ص ص 86 – 230.

حيث قد يرتكب الإجرام المعلوماتي سواء شخصًا طبيعيًا أو معنويًا أما صفة المجني قد تكون محلاً للأشخاص أو الهيئات مادام الأداة قد تسري في المعلومات فإن غالبية الجرائم الواقعة على النظام الآلي مستهدفة القطاعات المالية نظرًا لأهمية المعلومة المجردة في الوقت الراهن عماد للمعاملات الالكترونية في شتى الميادين، إلا قد بات التيار الرقمي منعزلاً دون الجدوى باعتبارها الدعامة المثبتة في تسيير الأعمال، مما نسلط الضوء على إجمالها فيمايلي:

ترتبط المعلومات المالية بالمؤسسات المصرفية والبنوك التي تسري في تداول مشاريع الاستثمار حيث قد تثبت محلاً للاعتداء نظرًا للاستيلاء على حساباتها الخاصة الماسة بالنظام المعلوماتي وإزالة الحواجز الأمنية بفك الشفرات، مما يؤدي إلى العبث بالمعطيات أو المحو أو التغيير بدوره قد يتسبب في إضرار تلك المؤسسات والتي تؤدي للإحجام عن الإبلاغ أو إفشائها أمام العملاء.

أما المعلومات الشخصية قد تمثل خصوصية الأشخاص سواء الطبيعية أم المعنوية مهما كادت تلك المعلومات المخزنة بالذاكرة أو المدخلة في بنوك المعلومات قد يؤدي إلى تخريبه، تشويهه، تسريبه، إبرازه على غير حقيقته القائمة، حيث تدخل في الإطار المعلومات المتعلقة بأسرار الدولة، المشاريع الصناعية المرتبطة بالتسليح الحربي باعتبارها عرضة للاعتداء، بالرغم من ذلك يسري دور المجني في كبح الجرائم المعلوماتية بنسبة ضئيلة، مما يفضل التكتم عن الاضرار حفاظًا على السمعة الحاسة لمركزهم المالي دون النظر إلى تدابير الحماية غير فعَّالة قد تسبب عزوف للعملاء، فضلاً عن عجز الإثبات و خشية احتمال المسألة القانونية عن واجب الإشراف على المعلومات المستهدفة لامتلاك سلطة التقدير على إجراءات الحماية. لذا أقدر عن الوضع الذي ينطبق في بلادنا العربية مقارنة بالتشريعات الغربية لها الوعي الحاد في المجال الفني فلا يخشى للإعلان على حدوث الجريمة بغية تحصيل حقوقهم ومعاقبة فاعليه عائد بالفائدة للأجهزة القضائية مع تحديد أطر الإجرام وفق حلول ناجعة للمكافحة مستقبلا. [44]

[44] -رمزي حوحو، "مواجهة الجريمة المعلوماتية في الجزائر"، **"مجلة الحقوق والحريات في الأنظمة المقارنة"**، المجلد 2، العدد 2، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، 2014، ص49.

المبحث الثاني
أشكال الاعتداء على النظام الآلي

تدول نقاش بين الأوساط القانونية على مدى تحديد تقسيمات جرائم الحاسب الآلي، مما يتعذر الحصر رغم الحداثة، السرعة، التنوع، التفاعل بفضل التأثر بالتقنيات الرقمية، حيث تصبح محلًا للاعتداء ووسيلة مستهدفة من خلال تحكم الجناة ببراعة على المجال الفني، لذا عمد الفقه الجنائي من خلال الجهود المضنية التي سعى إليها في تصنيف الجرائم إلى فئات متعددة متفاوتة قد تتجلى لكل منها على سمات مستقلة، فهناك من يصنفها حسب المعيار المعتمد شاملة الجرائم الواقعة بواسطة النظام المعلوماتي أو الجرائم الواقعة على النظم المعلوماتية، بالمقابل هناك من يراعي التصنيف تبعًا لأنماط السلوك الإجرامي الذي يتخذ إما على أساس الأسلوب المنتهج أم الباعث المحدد لارتكاب الإجرام بغرض تحقيق مزايا شخصية، كذلك هناك من يهدف التصنيف حسب تعدد محل الاعتداء الذي ينصب على البيانات المخزنة، البرامج بمثابة مصنفات رقمية تستحق حماية جنائية حاسمة، إذ تلاحظ السياسة الجنائية في مجال مكافحة الإجرام المعلوماتي على أنَّ التقسيم المثالي لجرائم الحاسب الآلي يفترض في المصلحة المحمية أي الحق في المعلومات شرط هناك انسجام يراعي كفالة تدفقها، تنظيم معالجتها مادام موضوعا للاعتداء، أما الدور الذي يؤديه الحاسب الآلي قد يرد على الأداة المستهدفة أم الوسيلة المنفذة نظرًا لقيامه بالوظائف الطبيعية داخل النظام المعلوماتي، مما نستخلص أنَّ التقسيمات لم تراع خصوصية أنماط الجرائم مع موضوعاتها بل استند على معيار وحيد متناسية معايير أخرى، فالرأي الراجح على التصنيف حسب غالبية الفقه يرد في المعيار المعتمد(الجرائم الواقعة بواسطة النظام المعلوماتي، الجرائم الواقعة على النظام المعلوماتي). [45]

بالرجوع إلى التشريع الجزائري قد أورده بمقتضى المادة الثانية من القانون 09ـــ04 المتعلق بجرائم تكنولوجيا الاعلام والاتصال، بالمقابل كرَّس القانون 04ـــ 15 المعدل لقانون العقوبات شتى أنواع الجرائم المعلوماتية بمقتضى المواد 394مكرر إلى مكرر7، إذ ينبغي الاعتراف بحقيقة الجهود المبذولة على المشرع في مجال مكافحة الاجرام المعلوماتي الذي يتبين من خلال تدارك الفراغ التشريعي في سن قواعد

(50) ـ نائلة عادل محمد فريد قوره، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، لبنان، 2005، ص 34.

موضوعية إجرائية مكملة نظرًا لنسبية الحماية الجنائية بمقتضى النصوص التقليدية لجرائم الأموال، ما دفع ذلك بالتعديل تجاوبًا لطبيعة الجرائم المعلوماتية محل الاعتداء.

تأسيسًا على ذلك سوف نعرض صور جرائم المعلوماتية المتفق على غالبية الفقه فيما يلي: الجرائم الواقعة بواسطة النظام المعلوماتي **(المطلب الأول)**، الجرائم الواقعة على النظام المعلوماتي **(المطلب الثاني)**، ثم نعرج إلى مسألة الحماية الجنائية على النظام المعلوماتي **(المطلب الثالث)**.

المطلب الأول
الجرائم الواقعة بواسطة النظام المعلوماتي

يُبنى التصنيف استنادًا على المعيار المعتمد لدى الفقه شاملًا الجرائم المتصلة بالمعلوماتية مادامت موضوعًا للاعتداء سواء الواقعة داخل النظام الآلي أم بواسطته، فالحاسب الآلي في هذا الصدد وسيلة لتسهيل النتيجة الاجرامية ومضاعفًا لجسامتها، حيث يسعى الجاني عادةً من وراء ارتكاب تلك الجرائم كسب مادي غير مشروع، مما تتنوع الأنماط راجع لإساءة استخدام النظام المعلوماتي، بذلك تتولد مسرح اتساع الإجرام داخل البيئة الافتراضية الماسة أساسًا بالقيَّم المحمية لاسيَّما الجرائم الواقعة على ذات المعطيات مستهدفة اتلاف البيانات، برامج الحاسوب بما في ذلك نشر الفيروسات إلى جانب الجرائم الواقعة لما تمثله المعطيات سواء أكانت أموالًا أم أصولًا لعلها جرائم الغش، التحوير، الاخلال، الاتجار بالبيانات المخزنة، العبث داخل النظم الالية بما في ذلك تزوير المستندات المعالجة، بالمقابل هناك جرائم مستهدفة المعطيات الشخصية أو البيانات المتصلة بالحياة الخاصة، ضف إلى ذلك جرائم الملكية الفكرية بما في ذلك جرائم قرصنة البرمجيات، التقليد دون ترخيص.[46]

عندما نتمعن في الغرض المشترك للاعتداء على المعطيات قد تتحقق في القيمة الذاتية أو لما تمثله، أما الاعتداء على حقوق الملكية الفكرية يقتصر في الاستخدام غير المشروع للبرامج مادامت محلًا للاعتداء، حيث تنحصر الحماية الجنائية بما يلاحظ الفقه على إمكانية تطبيق القواعد القانونية المقررة في جرائم الأموال بالمقابل إرساء منظومة تشريعية رادعة من خلال اصدار نصوص مكملة تكفل بحماية المعطيات ذات الطابع الشخصي، أما فيما يتعلق جرائم الملكية الفكرية قد اعترف المشرع بمقتضى القانون رقم

(51) – غانم مرضي الشمري، الجرائم المعلوماتية، (ماهيتها، خصائصها، كيفية التصدي لها قانونيًا)، دار العلمية الدولية، عمان، الأردن، 2016، ص 51.

05ـــ03 المتعلق بحقوق المؤلف، رغم استحداث تعديلات عديدة تسعى إلى ملئ الفراغ التشريعي التي لازالت مقيدة بمبادئ المنهج التقليدي نظرًا لانعدام مرجعية مستقلة تكفل بالنصوص الجنائية التقليدية، مما بات النظام المعلوماتي محل الحماية الجنائية.

للإحاطة على ذلك سوف نركز لأهم الجرائم الواقعة باستخدام النظام المعلوماتي المبينة فيمايلي: الجرائم المعلوماتية الواقعة على المعطيات الشخصية **(الفرع الأول)**، الجرائم المعلوماتية الواقعة على المال المعلوماتي **(الفرع الثاني)**، الجرائم المعلوماتية الواقعة على المصنفات الرقمية **(الفرع الثالث)**

الفرع الأول
الجرائم المعلوماتية الواقعة على المعطيات الشخصية

تنطوي على جرائم الاعتداء بذاتية المعلومات السرية بما في ذلك الاعتداء على البيانات الشخصية المتصلة بالحياة الخاصة، حيث تنقسم حسب القيمة إلى نوع الحق المعتدى أما الدور في اقترافها على النظام المعلوماتي، مما باتت المعلومة سلاح تقني بين أيدي قراصنة المعلوماتية نظرًا لاتساع فضاء الانترنت معتمدًا على الأجهزة الآلية الذي أدى إلى تنوع صوره المرتكبة في البيئة الرقمية، ضف الى أهميتها المثبتة على الواقع سواء تعلق بطرق معالجتها على النظام المعلوماتي أم تداوله على الفضاء الافتراضي بغرض التفاعلية و الاتصال، بذلك تظل المعلومة ثروة مستحقة على الميدان و التأثر عليها قد يحذو على مخاطر هاجسه تنصب بالأمن القانوني. (47)

حيث عمد المشرع الجزائري إلى إضفاء الحماية الجنائية على المعلومات الشخصية من خلال إصدار القانون رقم 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي منعًا من تسريب، إفشاء، إساءة استخدام تلك المعطيات دون حق قانوني، إذ جلَّ اهتمام الدساتير الدولية بما في ذلك الدستور الجزائري على حرصه لحماية الحياة الخاصة بمقتضى المادة 39من الدستور مما سعى المشرع إيزاء الفراغ القانوني في تكريس مبادئ مؤطرة تلائم خصوصية الطبيعة الملموسة للمعلوماتية، بالمقابل أعطى عناية نزيهة على المعطيات الشخصية في تجسيد فعالية الحماية تبعًا للسياسة الجنائية العقابية ومن المنطلق الامن القانوني السيبراني

(52) ـــ منسل كوثر، شاوش حميد، "حماية المعطيات الشخصية في التشريعات العربية"، (دراسة مقارنة)، "**مجلة الدراسات القانونية المقارنة**"، المجلد 7، العدد 2، كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بوعلي، الشلف، الجزائر،2021، ص 582.

والتشريعات الدولية سواء تستهدف الأموال أم الأصول بدوره تساهم في ارتكاب جرائم عجيبة داخل النظام المعلوماتي.[48]

للإشارة إلى ما سبق سوف نحدد أهم الصور الواقعة على المعطيات الشخصية نظرًا إلى التعدد إلا قد أثرنا للدراسة على إحدى أنواعها بمعالجة الإشكالات التي تؤرق إليها سواء تعلق الأمر في تحديد العناصر التجريمية أم التكييف القانوني، حيث اعتدنا في التقسيم على صورتي المبينة فيمايلي: الاعتداء على المعطيات الشخصية**(أولا)**، الاعتداء الالكتروني على الحياة الخاصة**(ثانيا)**.

أولا: الاعتداء على المعطيات الشخصية

أولى اهتمام لدى الفقه الجنائي في مسألة حماية المعطيات الشخصية الالكترونية التي طرحت في علاقة القانون بالمعلوماتية على المستوى التشريعي، حيث صاحب استخدام النظام الآلي في معالجة المعطيات الشخصية السارية من قبل الهيئات المعنية على إساءة استعمال النظام المعلوماتي مع إفشاء سرية البيانات و تسهيل فرص الاطلاع عليها دون إذن مرخص بما في ذلك اعتداء على الطابع الشخصي المتصلة بالحياة الخاصة والحريات العامة، مما باتت المعلومة الشخصية تتضاعف على أهمية جديرة في إطار إسباغ الحماية الجنائية المكفولة في الصكوك الدولية ذلك بإدراج قواعد قانونية مستقلة تراعي حرمة الحياة الخاصة، رغم ذلك لم تشر إلى المعطيات بحد ذاته حق يقتضي حمايته قانونًا، لذا خطَّى المشرع الجزائري للالتحاق بعصرنة نظم المعلومات الهادفة إلى إرساء مبادئ تحكم معالجة البيانات مع فرض إجراءات قانونية صارمة ضد الاعتداء على الخصوصية.[49]

إصدار القانون 18ـــ 07 قد يبرر في تعزيز احترام الحقوق والحريات العامة تبعًا لمقتضيات التعديل الدستوري 2016 من خلال الاعتراف للأشخاص الطبيعيين بحق حماية المعطيات الشخصية في مجال المعالجة نظرًا لاقتصار النصوص التقليدية في

(53) ـ **تنص المادة 39 من الدستور الجزائري ما يلي: " لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميهما القانون. سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة."**
ـ دستور الجمهورية الجزائرية الديمقراطية الشعبية لسنة 1996 الصادر بموجب المرسوم الرئاسي رقم 96ـ 438، المؤرخ في 7 ديسمبر 1996، ج. ر. ج. ج، عدد 76، الصادر في 8 ديسمبر 1996، معدل ومتمم.

(54) -ANDRÈ Lucas، JEAN Devèze et JEAN Freyssinet، *«droit de l'informatique et l'internet»* UPF، Paris، 2001، p82.

توفير حماية مؤطرة على المعطيات الشخصية، بذلك حاول المشرع الجزائري التكيف مع منظومته الجنائية من خلال استحداث القانون رقم 18ـ07 الذي يعتمد على نموذج قانوني موحد يحكم بإدارة معالجة البيانات الشخصية في القطاع العمومي والخاص، مما يبين صحة البيانات مع مشروعية عملية المعالجة، كذلك قد تمنح لأصحابها حق الاطلاع، الاعتراض، التصحيح على المعطيات ذلك تحت تعليمات الهيئات الإدارية المخولة وفق القانون.

حيث تؤكد المادة الثانية من القانون 18ــ07 شرط عدم المساس بالحريات الأساسية من خلال إفشاء أسرارهم المرتبط في نطاق المعطيات محل الحماية مع نوع المعالجة التي تدخل في التنظيم، مما أدلى المشرع على تسمية البيانات بمصطلح المعطيات ذات الطابع الشخصي الواردة بمقتضى المادة 05 من القانون رقم04ــ15 المعدل لقانون العقوبات كذلك المادة 47 المتضمن لتعديل الدستوري 2020، إذ أشار إليها المشرع في المادة 1/03 من القانون 18ــ07 الذي يتطلب احترام مبادئ معالجة المعطيات الشخصية المحددة في المادة 09 من القانون 18ــ07، بذلك فرض على المسؤول عن المعالجة التزامات مقيدة وفق إجراءات شكلية تراعي ضمان حقوق الأشخاص مع سرية المعطيات من مخاطر المعالجة الآلية فلا ننسى التدبير لكافة الإجراءات التقنية التنظيمية لحماية المعطيات. **(50)**

---

(55) ـ مليايني عبد الوهاب، **"** الجرائم الماسة بالمعطيات الشخصية على ضوء القانون رقم 18-07 **"**، **"مجلة البحوث القانونية والاقتصادية"**، المجلد 6، العدد 1، كلية الحقوق والعلوم السياسية، جامعة عمار ثليجي، الأغواط، الجزائر، 2023، ص 274.

ـ تنص المادة 47 / 4 من الدستور الجزائري لسنة 2020 ما يلي: **"حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي".**

ــ المرسوم الرئاسي رقم 20ــ 442، المؤرخ في 30 ديسمبر 2020 المتعلق بإصدار التعديل الدستوري، المصادق عليه في إستفتاء أول نوفمبر 2020، ج. ر. ج. ج، عدد 82، الصادر في 30 ديسمبر 2020.

ــ تنص المادة 1/03 من القانون 18ــ 07 ما يلي: **"المعطيات ذات الطابع الشخصي تقصد كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه والمشار إليه أدناه، "الشخص المعني" بصفة مباشرة أو غير مباشرة.... هويته البدنية أو الفيزيولوجية أو الجينية أو البيو مترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية. "الشخص المعني": كل شخص طبيعي تكون المعطيات ذات الطابع الشخصي المتعلقة به موضوع معالجة.**

ـ قانون رقم 18ــ07، المؤرخ في 10يونيو 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج. ر. ج. ج، عدد 34، الصادر في 10 يوليو 2018.

ــ **نلاحظ من خلال استقراء المادة قد تم استبعاد المعطيات المتعلقة بالأشخاص المعنوية في مجال الحماية، مما تخص الأشخاص الطبيعيين بالإشارة إلى تحديد السمات المميزة لهم على سبيل الحصر، فالقانون يحمي جل المعطيات متى كانت ذات طابع شخصي إلا أنَّ المشرع وصف المعطيات بالحساسة المتعلق بالأصل العرقي، الجيني، الأراء السياسية الانتماء النقابي للشخص المعني، بذلك أورد القانون على المعطيات بأحكام مشددة على الحماية تخوفًا لإحداث التمييز العنصري أو تصنيف الأشخاص بدافع الإقصاء أو تتبع مراقبتهم بما يتعلق تحديد البيانات السرية ثم باتت الحاجة إلى التجميع و التنظيم بغرض المعالجة.**

(56) ـ فريدة بن عثمان، **"**حماية معالجة المعطيات الشخصية: قراءة في القانون 18ـ07**"**، **"مجلة التواصل"**، المجلد 27، العدد 1، كلية العلوم الإنسانية والاجتماعية، جامعة باجي مختار، عنابة، الجزائر، 2021، ص220.

بناءً على ذلك نبين النموذج القانوني لإحدى صور الاعتداء على المعطيات الشخصية ثم رصد الجزاء الجنائي المقرر عليها والذي سنتناوله فيمايلي:

- **. تجريم الاستغلال غير المشروع للمعطيات الشخصية:**

ترتكب حال استخدام المسؤول لعملية المعالجة الآلية، حيث يفترض استيفاء كافة الشروط المسبقة لإنجاز المعالجة إلا أنَّ الجاني يدفع باستغلالها دون إذن قانوني مشروع لأجل بلوغ الغاية المنشودة، مما ترتقي إلى جرائم معاقب عليها جزائيًا بما في ذلك مخالفة شروط التصريح بالمعالجة، إفشاء السر المهني لغير المؤهلين، ضف إلى ذلك هناك مخالفات قد تؤدي للإضرار بالمعطيات الشخصية.

لذا يتعين علينا تحديد صورتي الاستغلال غير المشروع على المعطيات الشخصية في حالتها البسيطة المشددة والمبينة فيمايلي:

1. تجريم انتهاك بنود التصريح في الصورة البسيطة:

إذ بمجرد تقبل السلطة الوطنية لحماية المعطيات الشخصية على التصريح المقدَّم لإنجاز المعالجة عند الضرورة الفعلية، تصبح بذلك جاهزة للاستعمال شرط احترام بنود التصريح الواردة في المادة 14 من القانون رقم 18ـ07 لاسَّيما البند المتعلق بتحديد الأغراض المقصودة من المعالجة ضف إلى مدة حفظ المعطيات، أما في حالة الترخيص يقتضي توافر بندين أيًّا كانت طبيعة التصريح عادي أم بسيط، مما جرَّم المشرع أيُّ سلوك يؤدي لانتهاك تلك الشروط بما في ذلك تجريم استعمال المعالجة لأغراض غير تلك المصرح بها، تجريم الاحتفاظ بالمعطيات ذات الطابع الشخصي بعد انتهاء المدة تطبيقًا للمواد 58/65 من القانون 18ـ 07، مما يتجلى تحديد ركني الجريمة ما يلي:

أ ـ الركن المادي:

تتحقق جريمة استعمال المعالجة عند تغيير المسؤول لتلك الأغراض أو يوسع من نطاقها، فالبحث عن النشاط الإجرامي يفترض الرجوع إلى التصريح لأجل التأكد من الأغراض المنجزة للمعالجة، بعد ذلك يتم المقارنة مع التي تُبع الجاني بسببها طالما قد تتشابه في الغرض الأصلي، مثلًا لو تمت المعالجة لأغراض علاجية ثم تستغل في الدعاية التجارية نظرًا لاستعمال سجلات طبية أُنجزت المعالجة فيها لأغراض اجتماعية ثم تتحول إلى دعاية سياسية، مما حدد المشرع على المسؤولين جزائيًا و المشار إليها بعبارة **" كل**

من قام بإنجاز أو باستعمال المعالجة ..." بمعنى الأشخاص الحائزين على المعطيات في كافة مراحل المعالجة من التجميع إلى التنظيم كذلك الأشخاص المعينون لتصلهم المعالجة.

إذ يقتضي الدقة في تحديد التصريح لاسيَّما فيما يتعلق بنص قانوني او تنظيمي، أما عن الصلاحية قد ترجع إلى السلطة الوطنية في حالة ما إذا تم توسيع الأغراض المصرح بها أم خروجًا عنها حيث يقصد المشرع بعبارة**:" إنجاز المعالجة و استعمالها لأغراض أخرى"** أي القيام بتغيير هدف المعالجة بمثابة إنجاز مرحلة جديدة تتخذ لأغراض متعددة، فقد يثور الخلط بين أغراض المعالجة و الأفعال المعاقب عليها بمقتضى المادة 56 من القانون 18ـ 07المتعلق بإنجاز معالجة غير مصرَّح بها، بالمقابل قد يتم استعمال وسائل تعسفية تدليسيه في المعالجة ما يتعارض مع مضمون المادة 69 المتعلق بتجريم التسبب أو الإهمال في الاستعمال التعسفي للمعطيات، فالمشرع هنا قد أشار إلى المراد من المعالجة مادام الجاني يستغل حيازته لاستعمال المعطيات دون حق مرخص ولو تمَّ إفشائها لغير المؤهلين.[51]

ب ـ الركن المعنوي:

يلاحظ التشريع الفرنسي بمقتضى المادة 58 من القانون رقم 18ـ07 بمثابة جريمة عمدية، فلا يكفي توفر القصد الجنائي العام الذي يؤدي إلى تغيير الأغراض المصرح خلافًا عن إنجاز المعالجة، مما اتفق الفقه الجنائي الفرنسي على اشتراط توافر القصد الخاص المتمثلة في نية الغش، إذ يثبت الجاني على أنَّ الأغراض المصرح عليها قد تم توجيهها للتمويه لأجل إخفاء الأغراض الحقيقية المراد الوصول إليها خلال المعالجة، ذلك مالا يتماشى مع نص المادة 58من القانون رقم 18ـ07 نظرًا لتشديد العقاب من قبل المشرع الفرنسي مقارنةً بما ورد في المواد 58/ 56 من القانون رقم 18ـ07 قد تسري على عقوبة جنحية بسيطة، ففي المادة 58 تعاقب **بالحبس من ستة أشهر إلى سنة و غرامة مالية من 60.000دج إلى 100.000 دج** بالمقابل المادة 56 تتعدى **الحبس من سنتين إلى خمس سنوات وغرامة مالية من 200.000 دج إلى 500.000 دج**، أما فيما يتعلق تجريم الاحتفاظ بالمعطيات خارج المدة المحددة عبارة عن جنحة وفق المادة2/65

(57) ـ مشتة نسرين، بن عبيد إخلاص، "الحماية القانونية للمعطيات الشخصية في ظل القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي"، **"المجلة الجزائرية للحقوق والعلوم السياسية"**، المجلد 6، العدد 1، كلية الحقوق والعلوم السياسية، جامعة أحمد بن يحي الونشريسي، تيسمسيلت، الجزائر، 2021، ص 686.

من خلالها جرم المشرع الاحتفاظ أو الإبقاء رغم انتهاء المدة المقررة للمعالجة، مما ورد مدة الحفظ بمقتضى نص تنظيمي في المادة 14من القانون 16ـــ03 المتعلق بالبصمة الوراثية.[52]

2. تجريم إفشاء المعطيات الشخصية لغير المؤهلين في الصورة المشددة:

أُعتبرت من الأفعال المشددة التي أشار إليها المشرع بمقتضى المادة 301 قع المتعلق بإفشاء السر المهني التي تحيل إلى المادة 40 من القانون 18ـ07 على إلزامية من اطلع على المعطيات الشخصية بحكم مهامه بالسر المهني، مما فرض على أعضاء السلطة الوطنية بمقتضى المواد 27/26/23 من القانون رقم 18-07 الحفاظ على السر المهني حتى بعد انتهاء المهام، ضف إلى ذلك جرَّم صور الإفشاء وفق المادة 60 من خلال السماح لغير المؤهلين بالدخول إلى المعطيات، بالمقابل عاقب على فعل التسبب ولو عن طريق الخطأ بإيصال معطيات لغير المؤهلين.[53]

أ ـ الركن المادي:

تتخذ المسؤولية الجزائية على من يحوز معطيات ذات طابع شخصي سواء المسؤول عن المعالجة المعالج من الباطن، أعضاء السلطة الوطنية، حيث يتجلى النشاط الإجرامي في السماح لغير المؤهلين بالدخول إلى المعطيات من خلال اتخاذ تصرف معبر عن قبوله بغرض التمكن من الاطلاع على النظام المعلوماتي، مما أُعتبر أنَّ الأشخاص غير

(58) ـ طباش عزالدين، "الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري"، (دراسة في ظل القانون 18ـــ07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات الشخصية)، "**المجلة الأكاديمية للبحث القانوني**"، المجلد 9، العدد 2، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميره، بجاية، الجزائر، 2018، ص51، متوفر على الموقع التالي:**https://www.asjp.cerist.dz/en Présentation Revue/72**

ـ تنص المادة 2/65 من القانون رقم 18ـ07 ما يلي:" **... يعاقب بنفس العقوبة وهي غرامة من 200.000دج إلى 500.000دج كل من قام بالاحتفاظ للمعطيات ذات الطابع الشخصي بعد المدة المنصوص عليها في التشريع الساري المفعول أو تلك الواردة في التصريح أو الترخيص."**

ـ راجع المواد 14، 69،58 من القانون رقم 18ـ07، المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، (ج. ر، عدد 34)، سالف الذكر.

ـ حددت المادة 14 من القانون 16-03 المتعلق بالبصمة الوراثية على مدة الحفظ للمعطيات الجنية هي 25 سنة بالنسبة للأصول، فروع الأشخاص المفقودين، المستفيدين بأمر انتفاء وجه الدعوى، الحكم بالبراءة نهائيًا، أما مدة 40 سنة بالنسبة للأشخاص المحكوم عليهم، المتوفين مجهولي الهوية.

ـ قانون رقم 16ـ03، المؤرخ في 19 يونيو 2016، يتعلق باستعمال البصمة الوراثية في الإجراءات القضائية والتعرف على الأشخاص، ج. ر. ج. ج، عدد 37، الصادر في 19يونيو 2016.

(59) ـ بن اجعوب فوزية، بوقرن توفيق، "الحماية القانونية للمعطيات الشخصية في ظل القانون 18 ـ 07"،"**مجلة الدراسات القانونية والاقتصادية**"، المجلد 5، العدد 2، معهد الحقوق والعلوم الاقتصادية، المركز الجامعي سي الحواس-بريكة، باتنة، الجزائر،2022، ص968، متوفر على الموقع الإلكتروني التالي: https://www.asjp.cerist.dz تم الاطلاع عليه يوم 16ماي 2023، على: 12سا و33 د.

المؤهلين بالولوج إلى المعطيات شرط مثالي في تحقيق الجريمة أما الذين بحكم الوظيفة قادر على الاطلاع لا نكون بصدد جريمة، لذلك أشار المشرع إلى خصوصية الركن المادي على سبيل الحصر شاملًا الأشخاص المخاطبين، الأشخاص الذين قدموا طلبات التصريح بالمعالجة الأشخاص المعنيين لمعالجة المعطيات الشخصية ثم تحدث عن المعطيات المعالجة التي يشترط لقيامها اكتمال كافة مراحل المعالجة إلا أنَّ الجاني يستطيع ارتكابها بمجرد استلام المعطيات عند عملية الجمع ثم إيصالها لغير المؤهل بسلوك إيجابي من خلال إرسال، تقديم، وضع المعطيات في متناول الغير، فالسماح لغير المؤهل في الولوج إلى المعطيات ذات الطابع الشخصي يؤدي دور إيجابي فعَّال باعتباره القائم بالولوج للمعطيات فلا حق للاطلاع عليها.(54)

كذلك قد يجرَّم المشرع الجزائري سلوك إيصال المعطيات المعالجة إلى غير المؤهلين المعاقب عليها بمقتضى المادة 60 من القانون 18ـ07 الذي يتخذ حقيقة لعدة أفعال إجرامية بما في ذلك الاستعمال التعسفي للمعطيات ضف إلى إيصال المعطيات لغير المؤهلين، مما يشترط لقيام الجريمة أن يأتي الجاني على حركة مادية شاملًا إرسال المعطيات في متناول الغير التي تختلف تمامًا عن جريمة السماح لغير المؤهل بالولوج الى المعطيات الواقعة بطريق سلبي من خلال استقبال غير المؤهلين على تلك المعطيات، حيث يظل الدور سلبي على عكس جريمة السماح لغير المؤهل بالولوج باعتباره من يقوم بالولوج.

ب ـ الركن المعنوي:

جريمة عمدية تتطلب توافر القصد الجنائي قوامه علم الجاني أنَّ ذاك الشخص غير مؤهل بالولوج إلى المعطيات ثم تتجه الإرادة إلى إتيان السلوك الإجرامي، فإذا سمح بالولوج عن خطأ معتقدًا على تأهيله فلا تسري الجريمة بحقه إنما يُسأل سواء بمقتضى المادة 65 باعتباره من قام بخرق التزام السرية وسلامة المعطيات أم تطبق عليه المادة

(60) ـ غزال نسرين، "حماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي"، "**المجلة الجزائرية للعلوم القانونية والسياسية**"، المجلد 56، العدد 1، كلية الحقوق، جامعة الجزائر 1-بن يوسف بن خدة، الجزائر،2019، ص123.
ـ راجع المواد 60،40،27،26،23 من القانون رقم 18ـ07، المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي (ج. ر، عدد 34)، سالف الذكر.
ـ قضي في قيام جريمة المعالجة الآلية دون تصريح في حق المسؤول عن الموقع الالكتروني الذي تمَّ بإدراج اسم الشخص في المحتوى التحريري دون تصريح قانوني مسبق (le contenu rédactionnel)، مما أقرَّت المحكمة أنَّ العملية بمثابة معالجة آلية، بذلك تمت إدانة المسؤول لعدم تقديم تصريح مادام القانون لم يمنح لغير المؤهل بمعالجة معطيات شخصية دون تصريح.
انظر/ **طباش عزالدين، "الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري"، مرجع سابق، ص41.**

69 من القانون 18–07 في صورة التسبب في إفشاء المعطيات ولو عن إهمال، أما الشخص غير المسموح بالولوج سيظل شريك في الجريمة إذ ما كان عالمًا بالعناصر الإجرامية من خلال عدم تأهيله مع النظر لطبيعة المعالجة أكانت الية، بذلك تتم المتابعة على أساس جريمة الدخول غير المشروع لنظام المعالجة الآلية المعاقب عليها بمقتضى المادة394 مكرر قع، أما جريمة إيصال المعطيات لغير المؤهلين قد تبرز الخصوصية إذ ما تم الإيصال عمدًا أو عن طريق الخطأ من خلال ما أشار إليها المشرع بعبارة **"... يتسبب أو يسهل ولو عن إهمال ..."**، فإذا وصلت إلى شخص غير مؤهل للاطلاع على معطيات شخصية نتيجة ممارسة المكلف بالمعالجة دون الالتزام بالحيطة على سرية المعطيات سيسأل بذلك عن الافشاء الواقع بغير عمد.(55)

➢ . الجزاء الجنائي في تجريم الاستغلال غير المشروع لمعطيات الشخصية:

كيَّف المشرع الجزائري الصورة المشددة للاستغلال غير المشروع فيما يتعلق جريمة إفشاء المعطيات الشخصية لغير المؤهلين بدرجة جنحة معاقب عليها بالحبس من **سنة إلى خمس سنوات وغرامة مالية من 100.000دج إلى 500.000دج** تطبيقًا لأحكام المادة 69 من القانون 18–07، حيث تضاعف العقوبة في حالة ما إذا تم السماح لغير

(61) ـ مشتة نسرين، بن عبيد إخلاص، **"**الحماية القانونية للمعطيات الشخصية في ظل القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي**"**، مرجع سابق، ص 688.

ـ تنص المادة 60 من القانون 18–07 ما يلي:**" يعاقب بالحبس من سنتين إلى خمس سنوات وغرامة مالية من 200000دج إلى 500000دج، كل من سمح لأشخاص غير مؤهلين بالولوج لمعطيات ذات طابع شخصي."**

ـ قانون رقم 18–07، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، سالف الذكر.

ـ تنص المادة 394مكرر من القانون 04–15 المعدل لقانون العقوبات ما يلي**: "يعاقب بالحبس من ثلاثة أشهر إلى سنة وغرامة مالية من 50.000دج إلى 100.000 دج، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من المنظومة المعالجة الآلية..."**

ـ قانون رقم 04–15، المؤرخ في 10 نوفمبر 2004، ج. ر. ج. ج، عدد 71، يعدل ويتمم أمر رقم 66ـ 156، المؤرخ في 8 يونيو 1966، المتضمن لقانون العقوبات.

ـ تجدر الإشارة لإحدى القضايا النموذجية الصادرة من محكمة النقض الفرنسية والتي تتلخص وقائعه فيما يلي:

قضي في قيام جريمة إفشاء المعطيات عن طريق الخطأ في حق المكلف بالمعالجة الذي تم بتقديم وثيقة لإحدى الهيئات ورد فيها رقم الهاتف لأحد الأشخاص دون انتباه على ذلك، مما أُعتبر القضاء على أنَّ الرقم الهاتفي من المعطيات الشخصية الإسمية التي تمكن من معرفة صاحبه مباشرة، إذ أدين المسؤول عن المعالجة رغم أثر الدفع جاء عن قوة قاهرة مادام ملزمًا بتقديم الوثيقة.

Trib. Correctionnel Briey, 15/09/1992, cité par : PRADEL Jean, DANTI-JUAN Michel**,** *Droit pénal spécial*, 2Ème édition, Edition Cujas, Paris, 2001, p.671.

المؤهلين بالولوج الى المعطيات ذات طابع شخصي المشار إليها في المادة 60 من القانون 18-07 دون الخيار بين العقوبتين، أما بالنسبة للأشخاص المعنوية قد يسأل بمقتضى المادة 71/70 من القانون 18-07 الواردة في قانون العقوبات على غرار مسألة الحماية متعلق بالأشخاص الطبيعيين في مجال المعالجة الآلية، بالمقابل يعاقب على الشروع في كافة الجرائم الماسة بالمعطيات الشخصية استنادًا الى المادة 73 بينما تضاعف في حالة العود تطبيقًا لأحكام المادة74.

بناءً على الدراسة نستنتج أنَّ المشرع الجزائري ساهم في إرساء حماية تنظيمية مجسدة في إطار المعالجة الآلية ذات الطابع الشخصي، مما حرص المسؤول عن المعالجة باتخاذ إجراءات تقنية إدارية فيما يتعلق مراقبة عملية المعالجة الذي يمنع الدخول بدون تصريح أو البقاء دون رخصة ضمانًا على سرية البيانات، بالمقابل يتم تأطير ضوابط مستهدفة على الاستخدام المشروع للمعطيات دون مخالفة مبادئ الدستور التي تتولى في تعزيز الدعامة الشخصية، إذ نأمل من المشرع إعادة صياغة محتوى النصوص القانونية لأجل إزالة اللبس الذي يتعذر تحديد نطاق المعطيات المشمولة بالحماية، مما يفترض تمديد صلاحية الهيئات المعنية التي تؤدي دور الرقابة على مدى تطبيق الحماية و نجاعتها.

ثانيا: الاعتداء الالكتروني على الحياة الخاصة

يلعب الفضاء السيبراني دور على التأثير بالخصوصية الشخصية بمثابة مستودع رقمي لمعلوماتنا و إحدى الأساليب التقنية المتعلقة بحفظ الأسرار الخاصة، إذ يمنع على الغير من محاولة الكشف أو المراقبة على الخصوصية الذاتية لما يلحق إنتهاك بحرمة الحياة الخاصة بعدما كانت تكسو على ظلال إلا وقد باتت أمام علنية شبكات الرقمية شفافة و مبينة تمامًا، حيث يتجلى الحق في المساس بالحياة الخاصة عبر شبكة الأنترنت من المسائل التي تُطرح نقاش قانوني باعتبارها تتعدى للإشكاليات التقليدية، لذا انتشر الحديث عن التهديدات التي تسري على الحياة الشخصية من خلال استخدام التكنولوجيا الرقمية لاسيما مجال الاتصالات، مما تعددت صور الاعتداء على أساس احترام الحياة الخاصة ذات صلة وثيقة بحرية الفرد ومن المبادئ المصونة دستوريًا و التشريعات الدولية، لذلك يقتضي الأمر بالحماية الفعلية للدفاع عنها سببًا في التطفل الواقع على الغير من خلال البحث عن خبايا الحياة الشخصية و التلصص بمحتوياتها أو إذاعة جزئياتها والذي بدوره يؤدي إلى اختراق حدوده الثابتة التي ترجع عن الاستغلال غير المشروع على الاليات التقنية.

تدخل حرمة المراسلات والاتصالات السرية والتقاط الصور ضمن عناصر الحق في الحياة الخاصة المحمية تشريعيًا دستوريًا والتي باتت عرضة للاعتداء من خلال الإفشاء او الكشف على محتوياتها أو نشر المعلومات الشخصية لغايات مستهدفة، وبالتالي أنافت على أهمية حقيقية باعتبارها من الموضوعات القانونية المترددة نظرًا لتنوع الاعتداء والتي باتت محلًا للتعامل أمام المنصة الرقمية، مما أعاد بحث مسألة مدى تمتع الأفراد بالحق في سرية المراسلات و الاتصالات إذ ما كانت تلك الوسائل أمنة كفاية للتراسل و الاتصال الشخصي أم عدم استعمالها بما يتصف الخصوصية و ذلك قد تعرقل على المنظومة الجنائية المكفولة بالحماية على الحياة الخاصة.((56))

لذلك سنبين بالتحديد لأهم صور الماسة بالحرمة الخاصة والتركيز على النقاط الدقيقة رغم التعدد والتنوع قد حاولنا بقدر من الوضوح للإشارة إلى العناصر التي ترتبط حتمًا بالبحث والوقوف على مدى نجاعتها في حماية الحياة الخاصة والتي تتجلى فيمايلي:

1. الاعتداء على المراسلات والمحادثات الإلكترونية والتقاط الصور:

لقد اقتحمت تكنولوجيا المعلومات مجال التراسل وقدمت اشكالا جديدة تعتمد على الحواسيب والهواتف المحمولة وشبكات الاتصال لما لها فعالية على صعيد المعاملات الشخصية والرسمية، حيث تتم الجريمة باطلاع الشخص عليها مباشرة بطرق غير مشروعة قد تتضمن أسرار تتعلق بطرفي الرسالة أو المحادثة أو الصورة كما قد تتعلق بالمرسل أو المرسل إليه إلا أن الاعتداء المجّرم وفق القانون تسري سواء اكانت متصلة بحرمة الحياة الخاصة أم لم تتضمنها تلقائيا، كما تعد محل الحماية بمجرد المساس بإحدى هاتيه الوسائل و التي تحرص كافة التشريعات كفالة سريتها نظرا لما يتم في اطار الخصوصية بعيدا عن العلانية، لذلك فإن وجه السرية و الحرمة فيها واضح تماما دون الاعتداد بمكان تواجد جهاز الاتصال سواء في مكان عام أو خاص، فلا عبرة للخوض في مسائل خاصة فالتبادل يضفي للحديث طابع الخصوصية و السرية بالمقابل استخدام وسيلة اتصال إعلامية جماهيرية يحقق العلانية.

لذا نلاحظ أن المشرع الجزائري قد أورد الرسائل الالكترونية في ملحق المرسوم التنفيذي رقم 123/01 المتعلق بنظام الاستغلال المطبق على مختلف الشبكات و المواصلات السلكية اللاسلكية بالإضافة إلى ما جاء بها الدستور 1996 بمقتضى المادة

(89) – زروقي عاسية، "جرائم الاعتداء على الحياة الخاصة عبر شبكات التواصل الاجتماعي وآليات الحماية"، **"مجلة القانون والعلوم السياسية"**، المجلد 8، العدد 2، كلية الحقوق والعلوم السياسية، جامعة صالحي أحمد، النعامة، الجزائر،2022، ص 13.

39 في الفقرة الثانية مادام حرمة الحياة الخاصة من الحقوق الشخصية و مبدأ دستوري يستوجب الحماية الحاسمة لها، ولما اتجهت اغلب التشريعات القانونية الدولية و الداخلية الى الاعتراف بالحق و تعضيد مشروعيته بالأليات التشريعية التي تستهدف للحماية ضد أي اعتداء قد يخل بسلامته، و بذلك أقرّ المشرع العمل على كافة قوانينه العادية نحو تدعيم سبل الوقاية في ظل التغير المستمر للعناصر الداخلة محل الجريمة و التطور السريع للأساليب المستخدمة في الاعتداء((57)).

الفرع الثاني
الجرائم المعلوماتية الواقعة على المال المعلوماتي

الثابت على الآلات التقنية قد أُخترعت لأجل تسيير المعاملات المالية الالكترونية لاسيما البدائل الاقتصادية التجارية، رغم ذلك تم إساءة استخدام المعطيات لأغراض غير مشروعة من قبل الجناة، امر بات يثير عواقب ملحوظة، فإذا ساهمت شبكة

(90) ــ فاطمة الزهراء ربحي تبوب، "سرية المراسلات والاتصالات الالكترونية حقًا يضمنه القانون"، **"مجلة الدراسات القانونية"**، المجلد 7، العدد 2، كلية الحقوق والعلوم السياسية، جامعة يحيى فارس، المدية، الجزائر،2021، ص ص623ــ 626.

ــ **عرف المشرع الجزائري الرسائل الالكترونية في ملحق المرسوم التنفيذي رقم 123/01 المتعلق بنظام الاستغلال المطبق على مختلف الشبكات والمواصلات السلكية اللاسلكية والتي جاءت ما يلي: "تبادل وقراءة وتخزين معلومات في شكل رسائل معطيات بين الموزعات الموجودة في مواقع متباعدة، ويمكن المرسل إليه أو (المرسل إليهم) قراءة الرسالة المبعوثة في وقت حقيقي أو في وقت مؤجل، تخضع هذه الخدمة لتوصيتي الاتحاد الدولي للاتصالات."**

ــ المرسوم التنفيذي رقم 123/01، المؤرخ في 09 ماي 2001، المتعلق بنظام الاستغلال المطبق على مختلف الشبكات والمواصلات السلكية اللاسلكية، ج. ر. ج. ج، عدد 27، الصادر في 13 ماي 2001.

– Art01 dernier alinéa du IV de l'article1er de la loi N° 2004 –575، pour la confiance dans l'économie numérique، JORF n°143 du 22juin 2004:" On entend par courrier électronique tout message، sous forme de texte، de voix، de son ou d'image، envoyé par un réseau public de communication، stocké sur un serveur du réseau ou dans l'équipement terminal du destinataire، jusqu'à ce que ce dernier le récupère» ; disponible sur: www.legifrance.gouv.fr

ـ تنص المادة 2/39 من الدستور 1996 والتي جاءت ما يلي:**" سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة."**

ــ دستور الجمهورية الجزائرية الديمقراطية الشعبية لسنة 1996 الصادر بموجب المرسوم الرئاسي رقم 96ـ 438، سالف ذكره.

ـ جاءت المادة 47 من التعديل الدستوري 2020 والتي تنص ما يلي: **" لكل شخص الحق في سرية مراسلاته واتصالاته في أي شكل كانت، لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة القضائية...." يعاقب القانون على كل إنتهاك لهذه الحقوق."**

ـ المرسوم الرئاسي رقم 20ــ442، المؤرخ في 30 ديسمبر 2020، يتعلق بإصدار التعديل الدستوري، سالف ذكره.

(91) ــ طباش عزالدين، شرح القسم الخاص من قانون العقوبات، (جرائم ضد الأشخاص والأموال)، الطبعة الثانية، دار بلقيس للنشر، الجزائر،2023، ص123.

المعلومات في إرساء الدول نحو الدخول لمستقبل الرقمية وتفاعلها على كافة الأنشطة الميدانية، إلا قد ركنت بحد رهيب نحو عولمة الجريمة وتحولها إلى ساحة عابرة للحدود في عالم المعلوماتية والتي تسودها أدمغة إجرامية بمراوغتها على الفضاء الافتراضي، مما يجعل الأجهزة الأمنية تتحدى تلك المخاطر الناجمة تحديدًا في اتساع نطاق تعدد الجرائم و تنوعها، تداركًا باقتراف أفعال إجرامية تهدد بالأمن الدولي.

حيث امتدت تلك الجرائم نحو أفاق مطردة ابتداء من سرقة البيانات و الحسابات المصرفية، الاحتيال المعلوماتي على البطاقات المالية، اتلاف المعطيات المعلوماتية، التزوير و إساءة الائتمان مرورا الى اختراق الشبكات و المواقع، قرصنة البرامج وزرع الفيروسات، الاعتداء على أنظمة المعالجة الالية، التجسس المعلوماتي والابتزاز الالكتروني، فمازالت تتلاحم الى حد مستمر نظرًا للحداثة و التطور التقني في مجال المعلوماتية، مفادها الاعتداء على المعلومة الالكترونية و التلاعب بها بدافع الجشع و تحقيق غايات نفعية بغير حق قانوني مستهدفة اضرار معادية سواء ماديا أو معنويا، لما لها دور قانوني فعَّال يشترك فيها النظام المعلوماتي آلية مساعدة في تنفيذ الإجرام.((58))

لذا عمدت التشريعات القانونية المقارنة البحث عن سبل منتهجة و التغلب على العقبات المؤثرة بالسياسة الجنائية المكفولة بالحماية رغم الحاجة الى النصوص القانونية اللازمة لمواجهتها والتي تطرح إشكالات مثارة لاسيما المجال المعلوماتي بالنظر الى الحداثة و التطور لأنماط تلك الجرائم، كذلك التعقيد في كيفية التعامل مع تطبيقاتها التقنية التي مازالت تتحكم بالأوضاع المادية التقليدية، إذ حرصت إضفاء الحماية الجزائية بمقتضى نصوص التجريم التقليدية و التي لم تقصر الاعتداء على الأشخاص بل طالت على الذمة المالية للغير، أما جرائم المعلوماتية بوصفه الغش المعلوماتي قد سن لها المشرع الجزائري نصوص عقابية مستحدثة مستقلة نظرا للطابع الرقمي على الأدلة الناتجة عن ارتكابها خلافا للجرائم المادية.

لذلك سنحاول دراسة الجرائم الماسة بالمال المعلوماتي من خلال الإشارة لأهم صوره وذلك في تحديد النموذج القانوني للتجريم والعقاب مع رؤية موقف المشرع الجزائري في مدى صلاحية تطبيق النصوص التقليدية في إطار المعلوماتية والمبينة فيمايلي: اتلاف المعطيات المعلوماتية(**أولا**)، سرقة المال المعلوماتي(**ثانيا**)، الاحتيال المعلوماتي(**ثالثا**).

(119) ـ أمين طعباش، الحماية الجنائية للمعاملات الإلكترونية، مكتبة الوفاء القانونية، الإسكندرية، 2005، ص **78.**

أولا: إتلاف المعطيات المعلوماتية

أُستهل تداول المعطيات والأموال على الفضاء الافتراضي معتمدًا على ذلك النظام المعلوماتي الذي يتسم بالسيولة والمرونة في تجميع البيانات وتخزينها لأجل المعالجة، إذ يتبين عند تحقيق المجرم لأغراض غير مشروعة نحو الدخول على النظام أو التعمد في البقاء فيها دون إذن قانوني، ما يدفع الى الاطلاع بالمعطيات المخزنة أو التلاعب بالمكونات المعنوية لنظام المعالجة الألية الذي بدوره يؤدي الى انتهاك بقيمتها أو سلامتها لما يسري على **"جريمة اتلاف المعطيات المعلوماتية "** ((59)) الماسة بالكيانات المنطقية للنظام الآلي، حيث تنطوي على اعتداء غير مشروع للنظام المعلوماتي من خلال عملية المحو او التعديل أو التغيير لتعليمات البرامج او البيانات بحد ذاته، فلا يهدف التدمير أو التشويه لمجرد الحصول على منفعة سواء الاستيلاء على المال أو الاطلاع على المعلومات بل احداث ضرر بالنظام المعلوماتي و اعاقته عن أداء الوظيفة الطبيعية للحاسوب، فالملاحظ على هذا النوع الجديد لما له أهمية استثنائية والذي يراعي تساؤلات غير متناهية لم تنال على اثراء نقاش جاد بين الأوساط القانونية لأجل التعرف على المعايير المشتركة التي تدخل في نطاقها و التمحيص على موضوعاتها مع تحديد الوصف القانوني الدقيق بالمقارنة عن باقي جرائم الأموال، لذا يستدعي الحال تحديد النموذج القانوني من خلال تحديد العناصر التجريمية و رصد العقوبات المطبقة عليها مع الإشارة الى موقف المشرع الجزائري في تطبيق النصوص التقليدية على المعلوماتية وذلك ما سنتناوله فيمايلي:

1. أركان جريمة اتلاف المعطيات المعلوماتية:

يتحدد الإطار القانوني اعتمادا على نشاط اجرامي يتمحور في سير نظام المعالجة الالية بشتى التصرفات الصادرة من الجاني، حيث استقرت التشريعات العقابية المقارنة نحو اسباغ حماية قانونية مستحقة تخص بالأموال المعنوية، مما جرّمت فعل الاعتداء بمقتضى نصوص مستحدثة، لذا سنحاول اسقاط العناصر التجريمية المكونة لها مع رصد العقوبات المطبقة عليها، إضافة الى إقرار موقف المشرع الجزائري بمدى خضوع الإتلاف المعلوماتي إلى نصوص التجريم التقليدية المبينة فيمايلي:

(120) - عرفت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على الاتلاف المعلوماتي بمقتضى المادة الثامنة والتي جاءت كمايلي:"... تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية قصدا وبدون وجه حق.
ــ المرسوم الرئاسي رقم 14ـــ 252، المؤرخ في 8 سبتمبر 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، ج. ر. ج. ج، عدد57، الصادر في 28 سبتمبر 2014.

أ ــ الركن المادي:

يرتكز النشاط الاجرامي عموما على عنصرين هما فعل الاتلاف ووقوع الضرر، حيث يمتد فعل الاتلاف في المجال المعلوماتي إلى المكونات المادية أو المعنوية للنظام الآلي و جعلها غير صالحة للاستعمال سواء اكان الاتلاف تاما ام جزئيا، وفي كلتا الحالتين تؤدي الى تخريب الأموال مادية أم معنوية، إذ يتمحور سلوك الجاني في اتلاف المكونات المادية للنظام إما بالتخريب، التعطيل، يقصد بالتخريب أي التوقف الكلي أو الجزئي على أداء الوظيفة المرصود لها ولو لم تفنى مادته بجعله غير صالحا، كذلك التعطيل أي التوقف عن القيام بالوظيفة في فترة مؤقتة، أما فيما يخص فعل الاتلاف على الكيان المعنوي المنطقي للنظام المعلوماتي l'alteracation(معطيات، معلومات، برامج) قد يتخذ ثلاث عناصر سواء المحو، التعديل، الإدخال غير المشروع، إذ يصبح الإتلاف معيبا سواء كلي أو جزئي للنظام، مما ورد المشرع الجزائري تلك الأفعال بمقتضى المواد 394 مكرر1 التي تحيل للمادة 3/323 ق. ع. ف، كذلك جاءت بمقتضى المادة الرابعة من اتفاقية بودابست.((60))

. السلوك الاجرامي:

حدد المشرع الجزائري الاتلاف في ثلاث أفعال الواردة على سبيل الحصر والتي تتجلى فيمايلي: الإزالة، التعديل غير المشروع، الإدخال غير المشروع للمعطيات.

(123) ـ تنص المادة 323/ من قانون العقوبات الفرنسي ما يلي: "إذا ترتب على الأفعال المذكورة حذف او تغيير للمعطيات النظام أو تخريب اشغال النظام...."

"lorsque il en est résulté soit la surpression، ou la modification de donnés contenus dans le système soit du fonctionnement de ce système، la peine…"

Voir/ PHILIPPE Conte, Patrick Maistre de chambon, droit pénal gènèral,7ème édition, Armand Colin, Paris,2004, pp 213-214.

ـ حيث تنص المادة الرابعة من اتفاقية بودابست ما يلي:"...أو محو أو إتلاف أو طمس لبيانات الحاسب..."

اتفاقية بودابست لمكافحة الجرائم المعلوماتية، المنبثقة عن اجتماع المجلس الأوروبي تحت رقم 185، بودابست، المجر، بتاريخ 21 نوفمبر 2001.

- **الإدخال غير المشروع للمعطيات:**

يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بها سواء أكانت خالية أم فيها معطيات مسبقا.

- **التعديل غير المشروع للمعطيات:**

يقصد بالتغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات جديدة، حيث يتحقق فعل التعديل عن طريق برامج غريبة تتلاعب بالمعطيات سواء محوها كليًّا أو جزئيًّا، أما تعديلها باستخدام القنبلة المعلوماتية وبرنامج الفيروسات، لذا يتخذ فعل التعديل احدى صور الاتلاف شيوعا، حيث يتضمن إما تعديل حالة البيانات أو طرق معالجتها أو وسائل انتقالها، هناك تعديلات تؤدي الى نتائج سلبية تتعلق بحالة البرامج والمعطيات أو تعديلات الغير المصرح بها قد تساعد في تحسين المكونات المنطقية للحاسب الآلي.((61))

. النتيجة الاجرامية:

يدخل الاتلاف ضمن جرائم الضرر غير الخطر، فلا جريمة اتلاف دون ضرر الذي يستند على إثره تحقق النشاط الاجرامي، حيث تشترط غالبية التشريعات لقيام الجريمة وقوع نتيجة معينة، فالضرر يختلف حسب طبيعة المال محل الاتلاف قد يتخذ على شكل إنقاص كلي أو جزئي الذي يؤثر في المال وتعطيله، كذلك يتخذ شكل إبطال أداء المال (الكيان المادي المعنوي) عن وظائفه وحرمان الغير من الاستفادة على ماله، فالقول حجم الضرر وطبيعته ومدى شموله على المال قد يؤدي إلى انعدامه أو تعطيله جزئيا، فلا ينظر إليه بمدى تحققه بل حصر مدى محدوديته على المال محل الضرر تلقائيا.((62))

ب ــ الركن المعنوي:

اتلاف المعطيات من الجرائم العمدية المقترنة وجوبا بالقصد الجنائي على عنصريه (العام، الخاص) فالقصد العام يلعب دور ملم في الجريمة، إذ يقتضي توافر العلم والإرادة الذي يسري على كافة العناصر المؤلفة للركن المادي، فلابد أن يعلم الجاني على تلك

(124) ـ هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، القاهرة، 2010، ص ص11-12

(126) ـ أسامة أحمد المناعسة، جلال محمد الزغبي، جرائم تقنية نظم المعلومات الالكترونية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2014، ص ص121-122.

المعطيات والبرامج الواقعة محل الاعتداء مملوك للغير مع اتجاه الإرادة إلى إتلاف أو تخريب النظام المعلوماتي، ذلك ما نصت عليها المادة الرابعة

من اتفاقية بودابست والتي تحيل الى المادة 394 مكرر1ق. ع. ج، حيث يتبين القصد الجنائي في جريمة الاتلاف من خلال ما ورد في المادة علم الجاني بما يقوم به من شأنه يحدث تخريب، تدمير، محو، اتلاف المعطيات داخل النظام المعلوماتي مع اتجاه الإرادة إلى ذلك، إذ تتحقق الجريمة متى تعمد الفاعل ارتكاب الفعل الذي حدده القانون أو يؤدي الفعل من شأنه الى التعطيل، الانتقاص من منفعته ما يجعله غير صالح للاستعمال، أما عن القصد الخاص فلا يكفي عنصري العلم و الإرادة لقيام جريمة الاتلاف بل يستوجب توافر النية الاجرامية لدى الجاني مع اتجاه الإرادة الى تخريب، إفساد، تغيير حالة المعطيات والبرامج الموجودة في النظام المعلوماتي، ذلك ما ورد في اتفاقية بودابست بمقتضى المواد 5/4 التي تشترط توافر القصد الجنائي الخاص المتمثلة في نية الإضرار.((63))

ج ـ الجزاء الجنائي:

أقرّ المشرع الجزائري تطبيق المسؤولية الجزائية على الأشخاص الطبيعية المعنوية في غالبية الجرائم وبالتحديد الجرائم المعلوماتية لاسيما جريمة الاتلاف المعطيات، لذلك سنبين العقوبات المقررة على الشخص الطبيعي ثم الشخص المعنوي.

(127) ـ حسام محمد نبيل الشراقي، الجرائم المعلوماتية، (دراسة تطبيقية مقارنة)، دار الكتب القانونية، مصر، ص328.

- **العقوبات المقررة على الأشخاص الطبيعية:**

المعلوم في السياسة الجنائية قد تنحصر مسؤولية الشخص الطبيعي إما العقوبات الأصلية شاملة الحبس، الغرامة أو العقوبات التكميلية والتي تتجلى فيمايلي:

. العقوبات الأصلية:

يعاقب المتلف على المعطيات **بالحبس من ستة أشهر إلى ثلاث سنوات** وغرامة مالية من 500.000دج إلى 2.000.000دج بمقتضى المادة **394مكرر1 ق. ع. ج.**

. العقوبات التكميلية:

الحكم بالمصادرة طبقا المادة **394 مكرر6** ما نستشفه من خلال عبارة**" يحكم بمصادرة"** بمعنى **المصادرة** وجوبي متى تعلق الآمر بالمعطيات والبرامج، كذلك يفهم من عبارة الوسائل المستخدمة متعلق بمحل المصادرة ونطاقها مهما يكن نوعها وطبيعته، فلا تخل عقوبة المصادرة على حسن النية.

أما **الغلق** قد ترد العقوبة صراحة بمقتضى المادة **394 مكرر6** الذي يمس المواقع المستعملة في ارتكاب الجريمة أو المكان الذي يستعمله الجناة في ارتكاب جريمتهم.

- **موقف المشرع الجزائري:**

اعتمد المشرع الجزائري على موقف صارم بشأن الجرائم المعلوماتية لاسيّما الاتلاف على المعطيات المعلوماتية، إذ تم إدراجها في نطاق الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بمقتضى المواد 394 مكرر إلى 394 مكرر6 والذي جرّم الاتلاف طبقا المادة 394 مكرر1، أما بالنسبة للقانون 09ـــ04 قد أشار اليها عندما عرف الجرائم المتصلة بتكنولوجيا الاعلام والاتصال بمقتضى المادة 2/أ.[(64)]

ثانيا: سرقة المال المعلوماتي

أُتخذ الفضاء السيبراني مسرح الجريمة في ظل عصرنة نظم المعلومات والاتصال التي ترتكب بواسطة الأجهزة الآلية أو شبكة الانترنت وسيلة نحو التمادي للإجرام على

(129) ـ تنص المادة 2/أ ما يلي:" جرائم المساس في أنظمة المعالجة الالية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية"
ـــ قانون رقم 09ـــ04، المؤرخ في 5 أوت 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، (ج. ر، عدد 47)، سالف الذكر.

البعد الدولي، حيث تلاشت البؤرة المادية وتحويلها الى البيئة الافتراضية، الأمر الذي حدى لاستفحال تنوع الجرائم رغم اتساع نطاقها بدوره يؤدي الى الاستغلال غير المشروع من قبل مستخدميه، لما قد تؤرق على اثرها مسائل قانونية مترددة بشأن حماية المنظومة المعلوماتية محل الاعتداء لاسيّما المال المعلوماتي(المعطيات المخزنة، المعلومات، البرامج) التي تفتقر الى نصوص جزائية حتمية لأجل حمايتها رغم عجز المعايير التقليدية التي تترك ثغرات منعدمة، ما يقتضي على المشرع مراعاة تلك الإشكالات ايزاء الفراغ التشريعي القانوني دون عائق للتطبيق أمام الممارسة القضائية، ونظرًا لأهمية الدراسة البحثية التي تنحصر في الجرائم الواقعة على الأموال المعنوية باعتبارها من المنقولات اللامادية لاسيما السرقة المعلوماتية الماسة بالذمة المالية على الغير مازال محلا للدراسة و التمحيص على الصعيد الفقهي بشأن الأسلوب أو الطبيعة المتخذة متفاوتة تماما عن النموذج التقليدي، حيث ثار نقاش على مدى انطباق فعل الاختلاس على المال المعلوماتي و تصلح محلا للسرقة في الدعامة التقليدية؟ فهل تسري النصوص المنظمة على السرقة التقليدية كافية تماما لمواجهة الاعتداءات الواقعة على المعطيات المعلوماتية أم هناك قيود تفرضه مبدأ الشرعية الجنائية؟؟ وبالتالي هل يستدعي على المشرع بالتدخل التشريعي القانوني في اصدار منظومة جنائية جديدة حاسمة لحماية المال المعلوماتي على واقع الاجرام المعلوماتي؟؟

بالرغم من عدم استقرار الفقه الجنائي بشأن التعريف للجريمة المعلوماتية إلا قد يتفقون بمدى موضوع الاعتداء على المعلومة بمثابة مال معنوي يقتضي تقويمه، وعلى غرار التصنيف التقليدي لجرائم الأموال قد تعددت أنماط متنوعة تخرج عن دائرة انطباق وصف السرقة التقليدية ومدى استيعاب النصوص التقليدية على المال المعلوماتي مادام هناك غموض للتجريم السرقة راجع ذلك الى غياب التشريع مراده انعدام مرجعية خاصة للنصوص الجنائية من قبل المشرع، فإن قانون العقوبات غير قادر على مواكبة تطور الجرائم التقنية اذ لم تكن هناك سلسلة من التعديلات على تجريم المعلوماتية وفي اطار التأكيد لإتباع سياسة جنائية مشتركة تحصن لحماية المال المعلوماتي ولو تعذر على ضبط مكافحتها على المستوى الوطني الدولي.

لذا سنحاول الوقوف على تحليل الإشكالات المثارة في النصوص المنظمة على جريمة السرقة ومدى انطباقها على المعلوماتية ثم ادراج مسألة التكييف القانوني استنادا الى

الأحكام الصادرة عن محكمة النقض الفرنسية مقارنة على ندرة الاجتهادات القضائية الجزائرية ضئيلة في المجال المعلوماتي.((65))

- **مدى انطباق وصف المال على المعلوماتية:**

يقصد على المال المعلوماتي كافة المكونات المادية المنطقية للنظام الآلي، حيث تسمح دخول المعلومات لأجل معالجتها، تخزينها، استرجاعها عند الطلب، يضم الكيان المادي الأجهزة الالية من وحدات الادخال، الإخراج، التشغيل التي تتم بمقتضاه المعالجة والتخزين المعلومات أما الكيان المنطقي يتمحور على البرامج والمعلومات، فإذا كانت الأجهزة المادية ليست بالحاجة الى نصوص مستقلة لحمايتها جزائيا مادام هناك نصوص التجريم التقليدية، فالأمر ينعكس تماما على الكيانات المنطقية قد يطرح تساؤل بمدى اعتبار الكيان المعنوي مالًا؟ فهل يقتضي على المشرع اصدار نصوص جزائية على حمايتها؟؟

علما أن الأموال من الوجهة التقليدية قد تقع على الأشياء المادية، لكن بادي الحال يتضاعف مع مواكبة التحديات الرقمية في المجال التقني، مما تفوق الأشياء المعنوية في قيمتها على المادية لما يستدعي البحث على معيار طبيعة الشيء محل الحق المالي حتى يتم اسباغ صفة المال على الشيء المعنوي.((66))

(130) ـ العكايلة عبد الله ماجد عبد المطلب، "سرقة البيانات والمعلومات الالكترونية"، **"مجلة كلية الشريعة والقانون تفهنا الأشرف"**، المجلد 18، العدد 4، كلية الشريعة والقانون، جامعة الأزهر، القاهرة، 2016، ص2154.

(131) ـ عبد الرحمن لعمش، الحماية الجنائية للمال المعلوماتي، مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماستر أكاديمي، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة غرداية، الجزائر، 2020، ص9.

النموذج القانوني على جريمة السرقة المعلوماتية:

تخرج السرقة عن الإطار التقليدي معتمدا على الأجهزة التقنية في ظل التكنولوجيا الرقمية، ما ينعكس على إثره الاستغلال غير المشروع في استخداماته لأجل الاستيلاء على المال المعلوماتي بشتى اساليب الاعتداء لاسيما سرقة المعلومات، البرامج، البيانات المخزنة في النظام، ما يدفع بالتدخل التشريعي لإدراج تلك الأفعال الضارة بالمصلحة المحمية في دائرة التجريم فيما يتعلق الإجرام المعلوماتي بمقتضاه يتم إرساء حماية جنائية حتمية في مجال المعلوماتية، فلا سبيل لإنهاء معالم الجريمة وفق النصوص التقليدية ضئيلة غير متطابقة تلقائيا، حيث يقتضي الحال احداث منظومة قانونية مستقلة تحدد لأيُّ سلوك اجرامي بما يتلاءم الوصف القانوني الصحيح دون ما يترتب ثغرات قانونية فارغة، فمن البديهي لكل جريمة العناصر التجريمية المتخذة لها مقابل رصد الجزاء الجنائي المقرر عليها، كذلك الشأن بالنسبة للسرقة التي سنبين بالتدقيق على فعل الاختلاس ثم محل الجريمة بعد ذلك ادراج الى مسألة القصد الجنائي على المعلوماتية. ((67))

أ ــ الركن المادي:

ورد المشرع الجزائري على جريمة السرقة بمقتضى المادة 350 قع التي تنص على اختلاس مال منقول مملوك للغير بنية تملُّكه، حيث حدد بمقتضاه عناصر التجريم من النشاط الاجرامي (فعل الاختلاس) محل الجريمة (المال المعلوماتي)، النتيجة الاجرامية (التسليم)، حيث ترد محل جدال فقهي على الطبيعة المادية للجريمة، فلا يمكن الحصر تحت تكييف منفرد بالنظر إلى وقوع السلوك الاجرامي حسب تنوع لأنماط الجريمة، إذ تتم العملية إما بواسطة الالتقاط الذهني للبيانات سواء المشاهدة، استراق السمع أم نسخ البيانات المخزنة داخل النظام أو على وسائط معينة، فإن المسألة تتطلب توسيع نطاق مفهومها التقليدي كي تتطابق مع الحالات الجديدة ، ما دعا بالمشرع الجزائري لإعادة النظر في الإشكال بما يتفق ويتلاءم محل الاعتداء، حيث يستند الفقه و القضاء على اعتبار السرقة" **أخذ مال الغير دون رضاه**" فلابد من الاستيلاء على الحيازة دون إرادة مالكه أو حائزه، بالمقابل يتوفر فعل الاختلاس عند القيام بحركة مادية على نقل الشيء الى حيازة الجاني، ذلك ما سنتناوله فيمايلي:

(135) ـ محمد عبد المحسن بن طريف، فيصل صالح العبادي، هبة عبد المطلب الفضلي، "جريمة السرقة المعلوماتية"، "**مجلة الدراسات والبحوث القانونية**"، المجلد 7، العدد 2، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، الجزائر، 2022، ص ص 18ـــ20.

- **مدى انطباق فعل الاختلاس على المال المعلوماتي:**

لم يتضح القانون صراحة على معنى فعل الاختلاس **Soustraction** بصدد جريمة السرقة بل يتم معالجته من قبل الفقه والقضاء، حيث يتنافى الفقه حول محل وقوع الكيان المادي للحاسوب وملحقاته كذلك البرامج والبيانات المدونة على دعامات مادية التي يتم الاستيلاء عليها وحيازتها دون رضا مالكه أو حائزه، ما يتبين ذلك على سرقة الدعامة المادية محمولة في شكل معطيات قد يماثله سرقة كتاب مملوك للغير، فلا يشترط حيازة جديدة على الجاني بل قد تكون لغير مالكه، فمن يقوم باختلاس برامج المعالجة المعلوماتية و تسليمها الى الغير ليتدخل في تلك الحيازة قد تتحقق السرقة حال اكتمالها على غرار يفترض دخول الشيء في حيازة المتهم قبل دخوله في حيازة الغير. **((68))**

مادام فعل الاختلاس يقتضي نقل حيازة المال محل السرقة، ففي إطار المعلوماتية يتم نقل الحيازة دون عنوة بمجرد فتح النظام الآلي لغرض الحصول على المعلومة دون إذن قانوني، حيث تبقى المعلومات في حيازة المجني فلا تنتقل مباشرة الى الجاني بصورة تامة، فهناك حالات يتم فيها سيطرة الجاني على المال دون اللجوء الى أيُّ حركة مادية بل يقتصر دوره عند مجرد تهيئة السبل، ذلك ما يتم تطبيقه في السرقة المعلوماتية عندما يقف الدور أثناء سير المعلومات دون تدخل سلوك إيجابي لإتمام العملية مثلا **"من يخترق الشبكة المعلوماتية لإحدى المؤسسات ثم يعطي امرا بنسخ المعلومات السرية في الدعامة الممغنطة التي قام بإعدادها للغرض المرجو، ثم يأخذ دوره المراقب لسرد المعلومات و نسخها على الدعامات"**، لقد وسعّ الفقه من مدلول الاختلاس الذي لم يشترط نقل المال ماديا مع انتزاعه من حيازة الغير ، لكن الأمر يصطدم على عقبات مادام

(136) – سارة سلطاني، "عنصر الاختلاس في جريمة السرقة"، "مجلة الحضارة الإسلامية"، المجلد 13، العدد 17، كلية الحقوق والعلوم السياسية، جامعة أحمد بن بلة، وهران، الجزائر، 2012، ص187.

تتلخص وقائع قضية Bourquin فيمايلي:

تم قيام عاملين في مطبعة بوركاين على نسخ وتصوير 47 شريط يحتوي على قوائم أسماء العملاء الأثرياء ثم استولوا على 70 قرص ممغنط مع القيام باستخلاص المحتوى المعلوماتي على مكائنهم الخاصة، حيث جاء حكم محكمة النقض مؤيدا الحكم السابق بإدانة العاملين على ارتكابهم جرم السرقة من ناحية وسرقة المحتوى المعلوماتي طيلة الفترة التي استغرقتها عملية نسخ المعلومات ، ومن خلال استقراء موقف المحكمة نستنتج تطور قضاء محكمة النقض الفرنسية التي تنطلق بدايتها في تطبيق المبادئ العامة لجرمة السرقة شاملة اختلاس الأشياء من نقلها من حيازة الغير الى حيازته و سرعان ما يدرك القضاء الفرنسي على طبيعة الأشياء المادية و اختلاسها، فلا الجريمة لمجرد وضع اليد العارضة على الأشياء دون تملكها، لذلك فإن القضاء الفرنسي قد تجاوز فكرة انتقال الأشياء لاسيما سرقة المحتوى المعلوماتي المثبت على الآلة المطبعية، فالمعطيات المعلوماتية تصلح محلًا للسرقة وتحققها من خلال ما يحتويه القرص من معلومات ولو تم الاختلاس مؤقتا.

Cass. Crime, 12 janvier1989, BC n14.

الاختلاس ذو طبيعة مادية فلا يصح محله مال معنوي، حيث تبقى المعطيات المعلوماتية في حيازة المجني كليًا، فالاختلاس قد يقع على البرامج والمعلومات وفق اشكال متعددة سواء الالتقاط الذهني أو نسخ البيانات المخزنة دون رضا الغير باعتباره عنصرا مكمل للجريمة.((69))

ب ـ الركن المعنوي:

يسري القصد الجنائي في جريمة السرقة المعلوماتية على صورتي هما القصد (العام، الخاص)، إذ يقتضي علم الجاني على فعل الدخول أو البقاء في النظام لغرض الاستيلاء على المعطيات المعلوماتية بإخراجها من حيازة المالك وإدخالها في حوزته خلسة مع اتجاه الإرادة إلى تلك الأفعال، فإذا كان الدخول أو البقاء في النظام مسموح أم وقع الجاني في خطأ عن جهل يظل القصد قائما ولو أنَّ الباعث عن فضول وإثبات القدرة، مما نتساءل عن المعيار الذي يحدد مشروعية الدخول الى النظام المعلوماتي حتى يتسنى توافر القصد الجنائي بغرض الاستيلاء على المعلومة التي تؤدي لقيام السرقة؟؟

القصد الجرمي حقيقةً غير مكتمل مجرد توافر العلم والإرادة بمقتضاه يعلم الجاني أن المال قد تثبت ملكيته على الغير دون رضاه وادخاله في حيازته مبتغيا تحقق النتيجة بل مقترن بالقصد الخاص الذي ينصرف على نية تملك الشيء محل الاعتداء بواسطته يتم الاستيلاء على المعطيات بدوره يؤدي الى تبديل الحيازة من خلال ممارسته صفة مالك الشيء مع التنويه أنَّ هناك تزامن بين نية التملك وفعل الاختلاس، فإذا كان القصد الخاص لاحقًا لفعل الاختلاس ذلك يؤدي لنفي جريمة السرقة، لما يتعذر البحث عن آلية اثبات سوء النية فمن قام بالولوج الى النظام المعلوماتي قصد تملك المال ذلك يحتاج الى اثبات القصد في لحظة ارتكاب الفعل على اية حال يتم استخلاص القصد الجنائي من الناحية القانونية بمجرد دخول الجاني الى النظام مع تجاوزه لأنظمة الحماية دون تصريح، حيث يقر الفقه الفرنسي بمقتضاه انتهاك الجاني على النظام دليلًا على سوء النية، فالانتهاك بمثابة وسيلة الاثبات و الدخول غير المشروع عنصر مقترن للجريمة.((70))

(137) ـ علي عدنان الفيل، الإجرام المعلوماتي، (دراسة مقارنة)، منشورات زين الحقوقية، العراق، 2011، ص56.

(145) ـ إبراهيم بلعيات، أركان الجريمة وطرق اثباتها في القانون الجزائري، دار الخلدونية للنشر والتوزيع، الجزائر، د. س. ن، ص121.

ج ـ الجزاء الجنائي على جريمة السرقة المعلوماتية:

أخضع المشرع الجزائري جريمة السرقة المعلوماتية على عقوبة جنحية طبقا للقواعد العامة المنظمة في السرقة التقليدية بمقتضى المادة 350 قع، إذ يعاقب بالحبس من **سنة** إلى **خمس سنوات** وغرامة مالية من **100.000دج** إلى **500.000دج**، في حين لا يتلاءم طبيعة تطور الجرائم نظرًا لما يلحق من أضرار معادية على النظام المعلوماتي ماديًا معنويًا، لذا نستنتج بخصوص مسألة الحماية الجزائية على المال المعلوماتي وفق النصوص التقليدية غير قادرة تمامًا لانعدام مرجعية جنائية مستقلة تكفل لحماية المال المعنوي رغم غموض معالمها، جسامة خطورتها و اتساع نطاقها على البعد الدولي، فلابُّد على المشرع الجزائري السعي الى انتهاج سياسة عقابية رادعة للتصدي و المجابهة بمحاولة إيجاد سبل ايزاء الفراغ القانوني لاسيّما في جرائم الأموال فلا جدوى من تطبيق النصوص التقليدية ولو تم اصدار قوانين مستحدثة مستقلة بمقتضى الامر رقم 15ـــ04 المعدل لقانون العقوبات شاملةً المواد 394 مكرر الى 394 مكرر7 بالإضافة الى القانون 09ـــ04 في مادتها الثانية إلا لم تراعي بدقة كافة أنماط الجرائم لاسيما السرقة المعلوماتية التي تفتقر الى نص خاص يعالج الأفعال التجريمية المكونة لها بما يتناسب الجزاء المقرر، كما لم تحدد صراحةً الجرائم التي تدخل في نطاقها مادام المال المعلوماتي محل للاعتداء، لذلك سايرت التشريعات الجنائية المقارنة على تنشيط حركة عاجلة في مجال المعلوماتية في ظل غياب التشريع مع ضرورة التوسيع من مفهوم المال المعلوماتي شاملًا الأشياء المعنوية التي تصلح لتحقق فعل الاختلاس ولو لم يدوم الى الوقت اللازم لإعادة انتاجها كالنسخ على الدعامة ونقلها على النظام الآلي راجع لتلك الوقائع مادية غير معنوية خلافا على الاتلاف قد تم إفراده وفق نصوص خاصة بالتجريم أفعال متعددة.((71))

ننادي على المشرع الجزائري مواكبة النصوص التقليدية المنظمة لجرائم الأموال سواء ادراجها في تشريع مستقل ام تعديلها في قسم خاص بالجرائم الواقعة على المال المعلوماتي ذلك بما يتفق مع طبيعة المال المعنوي خلافًا على الأشياء المادية تفاديا للعقبات المؤثرة بشأنها امام الفقه والقضاء بمعنى دون اثارة نقاش حاد كي نكون قد سددنا فراغ قانوني الذي مازال محل جدال في الأبحاث القانونية، اما فيما يتعلق توسيع مضمون المال من ناحية المنظومة الجنائية قد يتطلب من المشرع إعطاء تحليلا دقيقا واضح يشمل الكيان المعنوي بما في ذلك المعطيات المعلوماتية على غرار لم تشترط وقوعها على المنقول

(146) ـ معتوق عبد اللطيف، الإطار القانوني لمكافحة الجرائم المعلوماتية في التشريع الجزائري والمقارن، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر، 2012، 38.

المادي بل تعدى على الأشياء المعنوية مادام اعترف ذات وصف مال، إذ لم يعد الاعتماد على التضييق للتفسير النصوص الجنائية بمقتضاه التحكم بالأفعال الاجرامية دون التعارض مع مبدأ الشرعية الجنائية،

الفرع الثالث
الجرائم المعلوماتية الواقعة على المصنفات الرقمية

الملكية الفكرية احدى فروع العلوم القانونية تأثرًا بالتكنولوجيا لاسيَّما المصنفات الرقمية الواردة على الدعامة الالكترونية ووليدة الابداع التقني الحاصل بين ازدواجية الإنتاج الفكري والعولمة، إذ تنتمي الى بيئة افتراضية مستندة آليات النشر الالكتروني والتشفير التي ترتد على أعمال التأليف وتطوير المنتجات المعرفية، مما تتيح للأشخاص استخدام تلك المصنفات لأغراض غير مشروعة تمامًا وذلك قد يلحق خسائر اقتصادية على ذاتية المؤلف، حيث ابتدأ التفكير في حماية المصنفات الرقمية بمقتضى براءة الاختراع و مع بزوغ ثورة تقنية المعلومات و الاتصال احتدم بالدول الى مراجعة تشريعاتها القانونية و العزوف عن نظام براءة الاختراع نحو الانضمام الى الاتفاقيات الدولية لعلها (اتفاقية تريبس، برن، الاتفاقية العربية، Wi po) التي حازت على حماية مستقلة لحقوق الملكية الفكرية، أما التشريع الداخلي قد تم وضع منظومة قانونية تكفل حماية حقوق المؤلفين في مجال الغش الالكتروني، فالمنظومة التشريعية الجزائرية لم تكن بمعزل عن المواكبة بل تم اصدار الأمر رقم **05/03** المتعلق بحماية حقوق المؤلف بعدما باتت الحماية تدور حول الجرائم الواقعة على برامج الحاسوب و قواعد البيانات بمقتضى القانون **10/97** من بين المصنفات الرقمية التي أقر المشرع صراحة دون شك للإشارة اليها على غرار تعمَّد لفسح المجال مستقبلا في حين لم يتم ادراج مضمونها بل لجأ إلى تعدادها على سبيل المثال لا الحصر استنادا للمادة 4 بمقتضى الأمر رقم 05/03، لذا نلاحظ أنَّ المسألة مازالت مصدر اهتمام على الصعيدين المحلي الدولي و محل الدراسة الفقهية لما تطال على اعتداءات تنتهك حقوق المؤلفين الذي بدوره تُعرض الفقه القانوني الى عقبات شائكة لاسيَّما الحماية الجزائية التي عجزت عن تحقيق التوازن الثابت بين استغلال المعلومات و حماية حقوق المؤلفين ضد التقليد، النسخ، القرصنة مع ظل

تضخم المواقع الالكترونية وشيوع التجارة الالكترونية بذلك تم انشاء قوانين المنظمة الفكرية لحماية الابداعات.((72))

المطلب الثاني
الجرائم الواقعة على النظام المعلوماتي

تُقترن فكرة تكنولوجيا المعلومات بالنظام الآلي الذي يتم من خلالها حفظ البيانات لغرض المعالجة مع تنفيذ عملية التخزين حسب تعليمات البرنامج، حيث تنوعت أساليب الاعتداء بشكل مفاجئ لاسيَّما المنظومة المعلوماتية بدوره تصبح وسيلة الارتكاب أو بيئة الجريمة، إذ تسهل من ارتكاب جرائم عبر الحدود بواسطة محترفين تقنيين والذي يتسلح على الأجهزة الآلية بفضل عملية المحو، التعديل التخريب، الاستيلاء على المعطيات المعالجة آليًّا، إضافةً الى الجرائم الواقعة باستخدام النظام المعلوماتي هناك تصنيف معتمد على محل الاعتداء(مادة الجريمة) شاملةً جرائم الماسة بالأنظمة المعلوماتية، جرائم الماسة بمنتوجات الاعلام الآلي الى جانب جرائم الأنترنت (73)، لذا ساهم التطور التقني في عجز التشريعات الجنائية لمجابهة تلك الأنماط نتيجةً لخصوصيتها، طابعها غير الملموس يتعذر تطبيق النصوص التقليدية لقانون العقوبات و أية محاولة لتحميلها بما لا يطاق قد تصطدم بمبدأ الشرعية الجنائية، مما يقتضي التنويه بإلزامية محاصرة الإجرام المعلوماتي وفق قواعد مستحدثة مستقلة تتلاءم مع الطبيعة الخاصة لها لاسيَّما التشريع

(154) ـ فرج الحسين، "المصنفات الرقمية والاعتداءات الواقعة عليها وسبل حمايتها"، **"مجلة العلوم الإنسانية الاجتماعية"**، المجلد 3، العدد 3، كلية العلوم الإنسانية الاجتماعية، جامعة الجيلالي بونعامة، خميس مليانة، الجزائر،2022، ص44.

ـ أضفى المشرع الجزائري حماية مزدوجة على المصنفات الرقمية من خلال تكريس **القانون 15/04 المعدل لقانون العقوبات مبيِّنا كافة الأفعال المكونة للجريمة المعلوماتية أما القانون 03/05 المتعلق بحقوق المؤلف يشير الى كافة الأفعال المشكلة لجرائم التقليد والنسخ مع رصد العقوبات المطبقة عليها بعدما كانت تسري على حماية برامج الحاسوب وقواعد البيانات بمقتضى القانون 10/97 ثم وسع من نطاقها شاملة الاعتداءات الواقعة على الملكية الفكرية الأدبية الفنية و استبعاد نظام براءة الاختراع لحماية تلك المصنفات، فالمسألة قد تثار من ناحية التكييف القانوني لتلك الجرائم رغم حدة جسامتها التي باتت ترتكب في بيئة رقمية لما قد تتغير درجة العقوبة من جنح الى جنايات مادام أمامنا مصنفات مستقلة عن الطبيعة التقليدية، ما يستدعي على المشرع بإعادة التكييف لأجل إرساء ترسانة قانونية جزائية رادعة تهدف إلى تحقيق حماية حقوق المؤلف خاصة و الملكية الفكرية عامة.**

انظر/ هشام مسعودي، "حماية الملكية الفكرية لحقوق المؤلف للمصنفات الرقمية (قراءة في المدلول وسبل الحماية)"، "مجلة الدراسات القانونية"، المجلد 8، العدد 2، كلية الحقوق والعلوم السياسية، جامعة يحيى فارس، المدية، الجزائر، 2022، ص860.

Logiciel : arrêté de22 décembre 1981 publie au JO du 17 janvier 1982 au titre duquel i s'agit de « l'ensemble des programmes, procèdes et règles, éventuellement de la documentation, relatif au fonctionnement d'un ensemble de traitement de données

Voir/ MATHIEU Martin, "des logiciels et des programmes d'ordinateur", « entre droit d'auteur et brevet », disponible en ligne 17 mars 2015, sur www.grapi.fr

(151) ـ ذكي أمين حسونة، جرائم الكمبيوتر والجرائم الأخرى في مجال التكنيك المعلوماتي، ورقة بحث مقدمة الى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 25-28 أكتوبر، 2017، ص471.

الجزائري باعتباره من الأوائل الذين تفطنوا لهذا النوع من الاجرام مع استدراك الفراغ القانوني و لو هنالك ضعف الحماية الفنية، بدوره سارع الى تعديل قانون العقوبات في 2004/11/10 و أورد قسم مستقل تحت عنوان" **المساس بأنظمة المعالجة الآلية للمعطيات(les atteintes au système de traitement de donnes)** الذي تناول لأهم الجرائم التي تمس المنظومة المعلوماتية من المواد 394مكرر إلى 394مكرر7 رغم هناك اختلاف من حيث التجريم والعقاب إلا قد تحقق حماية جزائية لنظم المعالجة الآلية.

لذا نستعرض خلال هذا المطلب بدراسة موجزة لأبرز الجرائم الحديثة التي أدرجها المشرع الجزائري في تعديله لقانون العقوبات والماسة بالمعالجة الآلية باعتباره المنظومة العابرة لكافة مكونات المعلوماتية، حيث يقتضي منا إثبات النموذج القانوني لتلك الجرائم مع رصد العقوبات المطبقة عليها والمبينة فيمايلي: الاعتداءات الماسة بالأنظمة المعلوماتية **(الفرع الأول)**، الاعتداءات الماسة بمنتوجات الإعلام الآلي **(الفرع الثاني)**، جرائم الأنترنت **(الفرع الثالث).**

الفصل الثاني

الإطار الإجرائي التطبيقي في البيئة الرقمية

بات الإجرام المعلوماتي الابن غير الشرعي الذي جاء إثر تزاوج بين تقنية المعلومات مع العولمة الرقمية، مما فطن بالمنظومة الجنائية على كبح الجريمة نظرًا لسهولة إخفاءها قد تظل عائقًا أمام القصور التشريعي مع تنوع النظم القانونية الإجرائية فضلا عن إشكالات تسليم المجرمين لمكافحة الجريمة، إذ يؤكد حتمية تنسيق الجهود الدولية بهدف زيادة فاعليتها على مبررات التعاون الدولي لاستفحال الإجرام، رغم تعذر ضبط الجريمة المعلوماتية على الصعيد الوطني إلا هناك مبادرة من المشرع ضد ملاحقة المجرمين متأثرًا بحلول الدول العربية التي تمت بإبرام اتفاقيات دولية ثنائية مع استصدار قواعد موضوعية إجرائية متكلًا على تعزيز التعاون الدولي بين الهيئات القانونية.

استدرك المشرع الجزائري على أنَّ المواجهة الفعالة قد تتم إلا بإرساء قواعد قانونية إجرائية مراعية لمقتضيات مبادئ قانون الإجراءات الجزائية، إذ وضع هناك ترتيبات تقنية لمراقبة الاتصالات الالكترونية مع القيام بإجراءات التفتيش داخل المنظومة المعلوماتية مخولة الى السلطة القضائية، لم تكتنف بحماية موضوعية نظرًا لاقتصار النصوص التقليدية. بما يتماشى مستجدات تكنولوجيا المعلومات، حيث تم تكريس القانون 06–22 المؤرخ في 20 ديسمبر 2006إلى جانب القانون 09ـــ04 المتعلق بتكنولوجيا الاعلام والاتصال. ألقت القضايا المعلوماتية ظلالها على عاتق التشريعات القانونية لأجل التصدي على واقع المعلوماتية، مما دفع بالمجتمع الدولي الى حشد قواه في توحيد جهود مبذولة مع ذلك تظل عوائق حادة ضد المجابهة لاسيَّما القصور التشريعي تعارض بين المصالح، تنوع النظم القانونية الإجرائية، تنازع الاختصاص القضائي فضلا عن إشكالات تسليم المجرمين ذلك كله يؤكد حتمية تنسيق جهود دولية بهدف زيادة فاعليتها على المجابهة. مؤتمر الأمم المتحدة لمنع الجريمة ومعاملة مبررات التعاون الدولي. التعاون الدولي البنى الركيزة لمجابهة الاجرام المعلوماتي نظرًا لاستخدام التقنيات الآلية قد تعترضه عدة إشكالات سواء الصعيد الوطني أم الدولي التي يجب التغلب عليها بمبادرة جدية ضد استفحال الإجرام. رغم تعذر ضبط الجرائم المعلوماتية على الصعيد الوطني إلا هناك جهود مبادرة أقبلها المشرع ضد ملاحقة المجرمين متأثرًا بحلول الدول العربية التي تمت على وضع قوانين مجابهة، مما أولى المشرع أهمية قصوى للحفاظ على الامن القومي قد تم ابرام اتفاقيات دولية ثنائية مع استصدار قواعد موضوعية إجرائية لأجل التصدي بغض النظر عن عجز القوانين التقليدية لاستيعاب أنماط الاجرام المعلوماتي حفاظًا على مبدا الشرعية الجنائية متكلًا على تعزيز التعاون الدولي بين الهيئات القانونية غنى البيان أنَّ المشرع من خلال المنظومة التشريعية التي تعمل جاهدة لأجل مجابهة الجريمة المعلوماتية.

المبحث الأول

تكريس قواعد المتابعة الجزائية في البيئة الرقمية

سن المشرع الجزائري تطبيقًا لمبدأ الشرعية إرساء جملة من التدابير الإجرائية بمقتضى القانون 06ـــ22 التي من شأنها تساعد الهيئات الأمنية في الكشف عن ملابسات الجريمة لاسيَّما التنقيب على الأدلة لغرض الإثبات أمام القضاء وملاحقة مرتكبيه دون الانفلات من العقاب ذلك بمراعاة مقتضيات القانون الإجرائي مما أقبل على أساليب التحري بمقتضى القانون 04ـ09 منها المراقبة الالكترونية، اعتراض المراسلات، عملية التسرب، الحفظ والإفشاء العاجلان للمعطيات الإلكترونية شرط الحفاظ على الضمانات الفردية عند الإذن بالإجراء، حيث تخول ممارسة المهام على الضبطية القضائية تدعيمًا لسلطات التحقيق ضف إلى ذلك التمسك بالوسائل التقليدية لعلها إجراء التفتيش، المعاينة، الضبط قد تخص المسرح المادي للجريمة بل حتى على الفضاء الافتراضي يمكن تطبيقه بما يتماشى خصوصية البيئة الرقمية مع طبيعة الجريمة المعلوماتية بأشكالها المتعددة.

فلا ننكر دور تكنولوجيا المعلومات في إضفاء معالم التطوير والتفاعلية على كافة الأصعدة بما في ذلك ميدان التحري عن الجريمة، التحقيق الجنائي في الوسط المعلوماتي نظرًا لارتباطها بالنبضات الالكترونية المتذبذبة داخل الفضاء الافتراضي، حيث يسري التحقيق الجنائي في الفحص عن مكونات النظام المعلوماتي نظرًا لسهولة طمس الدليل الرقمي من قبل الجناة قد يعيق عملية البحث لدى الأجهزة الأمنية، مما تثير مشكلات قانونية نظرًا لقصور التشريع الإجرائي في متابعة الجريمة المعلوماتية بدءًا في مجال البحث و التحري مرورًا إلى التحقيق ووصولًا الى المحاكمة في ضوء بيئة رقمية محضة.

إذ يتعذر على رجال الأمن جمع الأدلة الرقمية لانعدام الخبرة الفنية، بذلك يسعى المشرع التكيف مع سياسته الجنائية الهادفة إلى المجابهة في تنظيم قواعد إجرائية جديدة تكفل التحقيق في الشبكة المعلوماتية بالمقابل يقتضي تفعيل الأساليب التقليدية بما يتلاءم ذاك النمط من الإجرام حتى يسهل مباشرة الإجراءات، ففي اطار المكافحة الإجرائية على الجريمة قد تم توسيع مجال الاختصاص القضائي إذ ما ارتكبت على النظم المعلوماتية الذي يؤول الى الأقطاب الجزائية المختصة في متابعة جرائم تكنولوجيا المعلومات ضف الى توسيع مهام وكلاء الجمهورية مع قضاة التحقيق حسب القانون 06ـــ22 المعدل لقانون الإجراءات الجزائية.

فضلا عن ذلك سنعالج خلال البحث دراسة مراحل المتابعة الجزائية بدءًا بعملية التحري عن الاستدلالات **(المطلب الأول)** ثم مرحلة التحقيق القضائي **(المطلب الثاني)** بعد ذلك نعرج إلى مرحلة المحاكمة **(المطلب الثالث).**

المطلب الأول
التحري عن الاستدلالات

أورد المشرع الجزائري مجموعة من الضوابط الإجرائية ذات طبيعة وقائية تحفظية التي تستهدف متابعة مرتكبي الجريمة المعلوماتية لأجل ضمان حماية المعطيات لاسيَّما أثناء جمع الاستدلالات، مما تلعب الأجهزة الأمنية دور إيجابي فعال حال وقوع الاعتداء على المنظومة المعلوماتية من خلالها يتم معاينة مسرح الجريمة مع ضبط الأدلة لغرض استجلاء الحقيقة التي تؤدي في الوصول لإدانة المتهم من عدمه ذلك بعد مساعدة سلطات التحقيق.

مما منح القانون 09ــ04 على الهيئات التقنية بالتنسيق مع السلطات القضائية في تلافي الاعتداءات الماسة بالأنظمة المعلوماتية ذلك بما يراعي الأحكام القانونية التي تضمن سرية المراسلات الالكترونية بصدد ذاك القانون تم إدراج ترتيبات تقنية لمراقبة الاتصالات الالكترونية مع تجميع محتوياتها في حينها القيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية ضف إلى ذلك ممارسة الأجهزة الأمنية سلطة الرقابة على المراسلات الالكترونية، وفي هذا السياق يجوز لضباط الشرطة القضائية الدخول بغرض التفتيش عن بعد للمعطيات المعلوماتية مع استطاعة اللجوء إلى مساعدة السلطات الأجنبية المختصة لأجل الحصول على المعلومات التي بصدد البحث عنها في بلد أجنبي، مما يسمح القانون على المحققين باستنساخ المعطيات محل البحث فأي إجراء قد استبقاه القانون على السلطة القضائية.

إذ ارتأى المشرع بعد تلاشي الأساليب التقليدية المقيدة على السلطة المختصة في التحري ميدانيًا لمكافحة الإجرام المعلوماتي على احتوائه وسائل جديدة مستقلة ذات فعالية تواكب شخصية محترفي المعلوماتية الذي يتحكم في التقنيات الآلية لاستفحال الإجرام المتمثلة في اعتراض المراسلات، المراقبة الالكترونية، التسرب إعمالًا بمبادئ الاتفاقيات الدولية المكفولة بإحترام الضمانات الفردية عند الخوض في الإجراءات، مما ننوه على واقع النصوص القانونية المتعلقة بالقواعد الإجرائية غير خاضعة تمامًا بين جرائم الواقعة على النظم المعالجة الآلية مع جرائم تكنولوجيا الاعلام سببًا في صدور القانون 06ــ22 قبل استحداث القانون 09ــ04 رغم تعديل الإجراءات الجزائية لم يشمل اطلاقًا جرائم تكنولوجيا الاعلام وفق الإجراءات المستحدثة بل خصَّه على قواعد مستقلة الواردة في القانون 09ــ04.

بناءً على ذلك سوف نبين الأجهزة الفنية المكلفة في التحري عن الجرائم الماسة بالنظم المعلوماتية **(الفرع الأول)** ثم نعرج إلى تحديد إجراءات التحري التقني في البيئة الرقمية **(الفرع الثاني)** بعد ذلك نشير عن ممارسة أساليب التحري المستحدثة **(الفرع الثالث).**

الفرع الأول
الأجهزة المكلفة في التحري عن الجرائم الماسة بالنظم المعلوماتية

اعتاد أعضاء الضبط القضائي على إجراءات التحقيق الابتدائي في الجرائم العادية الواقعة على المسرح المادي بغرض جمع الاستدلالات على فاعليها، مما تعالت الأصوات على حتمية إنشاء الأجهزة المختصة في التحري عن الجريمة المعلوماتية في ظل تلاشي الهياكل التقليدية المعتمدة على التدريب الفيزيولوجي بل أصبحت تقتضي على التحدي الذهني في مجال تقنية المعلومات حتى يتسنى المحقق من ممارسة عملية البحث داخل الفضاء الافتراضي، حيث أشارت اتفاقية بودابست للإجرام المعلوماتي على إدراج ضوابط إجرائية تشريعية تكفل التحقيق في جرائم تقنية المعلومات مع الاحتفاظ بالحق في حالة عدم تطبيق الإجراءات إلا في جرائم محددة، ضف إلى ذلك إحداث أجهزة التحقيق على المستوى الوطني.[74]

أما التشريع الجزائري لم يحدد في قانون الإجراءات الجزائية على الهيئات المسندة للتحقيق و الفصل في جرائم المعلوماتية نظرًا لانعدام الخبرة الفنية لدى رجال الأمن في مجال تكنولوجيا المعلومات والاتصال، ذلك ما يتعذر من مواصلة التحقيق داخل البيئة الرقمية دون دراية مُحكمة، إذ يجيز القانون على استعانة القاضي بالخبرة التقنية لأجل تحديد بصمات القضية التي تؤديه الى الحقيقة، من الناحية قد يؤول الاختصاص في التحري إلى الضبطية القضائية فيما يتعلق الجرائم الماسة بأنظمة المعالجة الآلية بمقتضى القانون 06-22 ذلك بإذن من السلطات القضائية المعنية، أما جرائم تكنولوجيا الاعلام والاتصال قد تم إنشاء الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيا الاعلام والاتصال بمقتضى القانون 09-04، رغم ذلك قد يربطنا أمام معادلة غير متكافئة الأطراف بين أجهزة الضبط القضائي مع قراصنة المعلوماتية، فلا مناص على أعضاء

(1) – مجدوب نوال، " الأليات الإجرائية للكشف عن الجريمة المعلوماتية"، **" مجلة البحوث القانونية والاقتصادية"**، المجلد 6 العدد 3، كلية الحقوق والعلوم السياسية، المركز الجامعي أفلو، الأغواط، الجزائر، 2023، ص199.

الضبط القضائي العادي من مباشرة التحري في إطار المعلوماتية و التعامل مع محترفيها.[75]

تجتهد المنظومة الجزائرية في سبيل تطوير هياكلها الداخلية من خلال التعهد بسن قواعد قانونية ذات أليات وقائية تتيح مباشرة التحري ذلك ما أتى القانون09-04، بالمقابل تم الإشراف على ورشة تكوينية مع جهاز الاستخبارات الأمريكية التي تهدف ضباط الشرطة و القضاة باطلاعهم على معرفة تقنية إجراءات التحري مع كيفية استخدام الأدلة الرقمية في التحقيق، فلا مفر لأي دولة من مجابهة عواقب المعلوماتية لوحدها بل يستوجب التعاون الدولي لأجل تعزيز مؤسساتها المختصة في التحري عن الجريمة، إذ لم يمنع بإحالة الدور استثناءً الى بعض الهيئات التقنية من خلال تنسيق تلك الجهود العملية مع الضبطية القضائية المكلفة بالتحري مادام القانون أعطى لها حق الاستعانة بالخبرة الفنية ضمانًا على فاعليَّة ضبط الجرائم في الفضاء السيبراني مع تسهيل عملية سير التحريات القضائية.

رغبةً من المشرع الجزائري في إطار مكافحة الإجرام المعلوماتي قد تم استحداث هيئتين (وطنية قضائية) بمقتضى سند قانوني إحداهما صدر وفق المرسوم الرئاسي رقم 19-172 بما في ذلك الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، ضف إلى أجهزة الضبط القضائي المتمثلة في وحدات التابعة لسلك الأمن الوطني، قيادة الدرك الوطني الصادرة بموجب نص تشريعي.

للإشارة إلى ذلك سوف نتناول عن الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام (**أولا**) ثم نأتي لأجهزة الضبط القضائي (**ثانيا**)

أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

عبارة عن مؤسسة عمومية ذات طابع إداري خاضعة تحت وصاية وزارة الدفاع الوطني المنظمة بمقتضى المرسوم الرئاسي رقم 19-172 بعدما تم إلغاء للأحكام الواردة في المرسوم رقم 15-261 إثر الظروف السياسية الأمنية الطارئة على الصعيد الوطني بل تم إرساء ضوابط إجرائية تنظيمية مجسدة من خلالها سعى المشرع في تكييف الهيئة من فئة السلطات الإدارية المستقلة تحت رقابة وزارة العدل إلى جهة أمنية تقنية تابعة

(2) - بوقرين عبد الحليم، "حتمية إنشاء ضبطية خاصة بالجرائم الالكترونية"، **"مجلة العلوم القانونية والسياسية "**، المجلد 5، العدد 1، كلية الحقوق والعلوم السياسية، جامعة حمه لخضر، الوادي، الجزائر، 2016، ص ص151- 159.

لوزارة الدفاع الوطني تتمتع بالشخصية المعنوية والاستقلال المالي لها صلاحيات محددة بموجب سند قانوني صريح.

إذ تتولى مهمة المراقبة الوقائية للاتصالات في إطار الجرائم الموصوفة بالأعمال الإرهابية التحري التقني في الجرائم الماسة بأمن الدولة بما في ذلك جرائم التجسس، الخيانة العظمى باستخدام وسائط رقمية التفتيش داخل المنظومة المعلوماتية، حجز المعطيات المعلوماتية تطبيقًا لمقتضيات القانون 09-04 كذلك المرسوم الرئاسي رقم 19-172، بالمقابل أعطاها المشرع حق مباشرة أساليب التحري فيما يتعلق تسجيل المعطيات الشخصية المتصلة بسرية الدولة لكي تحقق الهيئة الوطنية دور ذات فعالية ونجاعة لابَّد من تشكيلته المكون من جهاز إداري تنفيذي (مجلس التوجيه، مديرية عامة) لأداء الاختصاصات المنوطة بها وفق تعليمات القانون، مما يترأس الهيئة وزير الدفاع أو ممثله (وزارة العدل، الوزارة المكلفة بالداخلية، الوزارة المكلفة بالمواصلات السلكية اللاسلكية)، فلا تبنى بمعزل عن الأهداف الحكومية بل الغرض المشترك من استحداث الهيئة تشجيع سياسة الدولة في كافة القطاعات لاسيَّما التداول حول استراتيجية التنسيق مع المؤسسات المعنية لمكافحة الإجرام السيبراني، المراقبة الدورية بشأن تقييم حالات التهديد ما يدل على ذلك تحكم وزارة الدفاع دون منح دافع الاستقلالية حتى لو باتت ذات كيان قانوني قائم بذاته.

حيث أولى المشرع بمقتضى القانون 09-04 على الهيئة الوطنية طلب المساعدة من الجهات القضائية الداخلية في حالة توفر معلومات عن احتمال اعتداء على المنظومة المعلوماتية ذات تأثير على الاقتصاد الوطني، الأمن العام، الوصول إلى تهم الأبحاث الجارية في إطار التحريات والتحقيق القضائي، أما التنسيق بالتعاون في التحقيق مع الجهات القضائية الأجنبية أثناء مراقبة الاتصالات الالكترونية، تفتيش النظم المعلوماتية تبادل المعلومات، ممارسة إجراءات تحفظية إعمالًا لأحكام المرسوم الرئاسي 19-172، كذلك كلف القانون مساعدة السلطات القضائية مع مصالح الشرطة في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيا الاعلام بما في ذلك تجميع المعطيات، إنجاز الخبرات القضائية، فالملاحظ أنَّ دور الهيئة قد يسري في الجرائم الالكترونية الواقعة على

أمن الدولة عبر الوسائط الرقمية، الدفاع الوطني، الأفعال الإرهابية علمًا أنَّ الأفعال تمس بالخصوصية الشخصية إلى جانب فقد الدولة على منظومته القانونية.(76)

ثانيًا: أجهزة الضبط القضائي

الشرطة القضائية صاحبة الولاية العامة في ميدان التحري عن الجريمة، مما ساهمت على إنشاء فرق متخصصة في إطار المعلوماتية على الصعيد الوطني الدولي، بالمقابل توافر مخابر التقنية ذات تكنولوجيا عالية لشرطة العلمية دعمًا في تجسيد سياسة أمنية حاسمة من خلال إتاحة العوامل المادية البشرية تسعى لضبط الجرائم داخل الفضاء الافتراضي بغية الحفاظ على الأمن القومي إلى جانب الأنظمة المعلوماتية المرتبطة باقتصاد الدولة، حيث تحتوي على وحدات مكلفة بالبحث والتحقيق بما في ذلك المخبر المركزي للشرطة العلمية بالعاصمة، المخابر الجهوية للشرطة العلمية في قسنطينة، وهران على سبيل تحقيق مصالح الشرطة القضائية تم استحداث بما يقارب 23 خلية لمكافحة الإجرام السيبراني داخل التراب الوطني.

أما عن الوحدات التابعة لقيادة الدرك الوطني شاملًا المصالح العلمية التقنية، هياكل التكوين لاسيَّما المعهد الوطني للأدلة الجنائية مكلف في تحليل الدعامات الالكترونية، المقاربات الهاتفية، حسن التسجيلات الصوتية، الفيديوهات، المصلحة المركزية للتحريات الجنائية، مراكز الرقابة من جرائم الاعلام الآلي مختص بالتحقيق في الجريمة المعلوماتية التابع إلى مديرية الأمن العمومية لقيادة الدرك الوطني، فالوظيفة المثلى على وحدة الدرك الوطني قد تسعى لخدمة العدالة، التشجيع على التحري في إطار مكافحة الإجرام المعلوماتي على غرار القاعدة الإجرائية ليست الغاية ذاته بل الوسيلة في حسن تطبيق القانون الجنائي الموضوعي ذات صلة وثيقة بالإجراءات الجنائية الماسة

(4) ـ سهيلة بوزبرة، "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: بين سرية المعطيات الشخصية الالكترونية ومكافحة الجرائم الالكترونية"، "**المجلة النقدية للقانون والعلوم السياسية**"، المجلد 17، العدد 2، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2022، ص ص563ـــ569.

ـ تنص المادة الثانية من المرسوم الرئاسي رقم 19ـــ172 ما يلي:" **الهيئة مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي توضع تحت سلطة وزارة الدفاع الوطني.**"

ـ المرسوم الرئاسي رقم 19ـ172، المؤرخ في 06 جانفي 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها وتنظيمها وكيفية سيرها، ج. ر. ج. ج، عدد 37، الصادر في 09 جانفي 2019.

بالحريات العامة عند الإهمال، إذ يمارس أعضاء الضبط القضائي صلاحيات رادعة مقارنةً بالشرطة الإدارية ذات أعمال وقائية تحفظية.[77]

خول المشرع على الضبط القضائي تطبيقًا لأحكام قانون الإجراءات الجزائية صلاحية تمديد عمليات المراقبة لأجل ملاحقة مجرمي المعلوماتية ذلك تحت إشراف الجهات القضائية عند الخوض في اجراء التحري إلى جانب مباشرة أساليب التحري الخاصة فيما يتعلق اعتراض المراسلات بواسطة وسائل الاتصال السلكية اللاسلكية، عملية التسرب المحددة في المواد 65 مكرر 5 إلى 65 مكرر18 ق. إ. ج، مراقبة الاتصالات الالكترونية معتمدًا على الخبرة التقنية لأجل الإفادة على معلومات ذات علاقة بموضوع الجريمة، القيام بإجراء التفتيش داخل المنظومة المعلوماتية، حجز المعطيات المعلوماتية استنادًا الى القانون 09-04.[78]

الفرع الثاني
إجراءات التحري التقني في البيئة الرقمية

ترشد عملية جمع الاستدلالات في إطار بناء الدعوى الجنائية قد يتولاها المشرع بدعم قضائي مرصد ذات أهمية ملمة في التحري عن مادة الجريمة لأجل تهيئة القضية بإحالته الى النيابة العامة بمثابة المدير التنفيذي المشرف على الضبط القضائي بشأن عرضها على سلطة التحقيق، إمعانًا من الفقه الجنائي في تأكيد المسألة قد تتعلق بالدور الفعال الذي يؤول على مأمور الضبط القضائي بمثابة خط دفاعي أولي قد يستعان أثناء التحري في مجابهة الجريمة، لم يسري على الدول إمكانية التصدي على واقع المعلوماتية في بداية إحداثها إلا الاعتماد على القواعد الجزائية القائمة بشتى فروعها الموضوعية الإجرائية ذلك تفاديًا لإفلات الجناة من العقاب لانعدام مرجعية مستقلة على النصوص الإجرائية قد

(5) ـ لوجاني نورالدين، "دور رجال الضبطية القضائية في مكافحة الجريمة الالكترونية"، مداخلة في يوم دارسي حول علاقة النيابة العامة بالشرطة القضائية ـ احترام حقوق الانسان ومكافحة الجريمة، بالتنسيق مع المديرية العامة للأمن الوطني، المنعقد في إليزي يوم 12 ديسمبر 2009، ص08.

(6) ـ موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية، بحث مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 2016، ص 15.

ـ للإشارة إلى أنَّ الأجهزة الأمنية الجزائرية بالتنسيق مع الهيئة الوطنية قد استطاع معالجة الجريمة الالكترونية نسبة 30% على مواقع التواصل الاجتماعي،11 قضية متعلق بالإرهاب المعلوماتي باسم تنظيم داعش، توقيف 58 متورط في قضايا الإرهاب خلال 2016، بالمقابل تم توقيف عن 160 جزائري ذات علاقة مع داعش في بلدان أجنبية، 30 خلية تسعى لاستقطاب الشباب عبر مواقع الانترنت لصالح الإرهاب إثر استخدام الأنظمة التكنولوجية المستحدثة.

ـ راجع المواد 65مكرر5 إلى 65مكرر 18 من القانون رقم 06-22، المؤرخ في 20 ديسمبر 2006، ج. ر. ج. ج، عدد 84، الصادر في 24 ديسمبر 2006، يعدل ويتمم الأمر 66- 155، المؤرخ في 8 يونيو 1966، المتضمن لقانون.إ.ج.

تتلاءم طبيعة الاجرام، بعد التطور الحاصل في مجال المعلوماتية بما صاحبه من انعكاسات من حيث محل الجريمة، الوسيلة المستعملة، نوع الجناة، مما باتت تلك القوانين لا تواكب العولمة الرقمية بل أضحت من غير جدية، فالمشرع الجزائري حينما أراد توسيع نطاق تطبيق إجراءات التحقيق التقليدية لمتابعة الجرائم الالكترونية قد يقصد بها الإجراءات التي تثير عقبات عملية تعود إلى خصوصية تلك الجرائم لاسيَّما التفتيش، الضبط، المعاينة، الخبرة، إذ تحتاج إلى التطوير لكي تتناسب الطبيعة المعلوماتية بالمقابل الدليل الذي يصلح لإثباتها، للاسترشاد على ذلك سوف نعالج تلك الإجراءات المادية بدءًا من المعاينة(أولا) ثم تفتيش النظم المعلوماتية (ثاني) بعد ذلك نعرج عن ضبط الأدلة (ثالثا).

المبحث الثاني
الآليات التشريعية العملية في مكافحة الجريمة المعلوماتية

تنتهج السياسة التشريعية جاهدةً على تجسيد التدابير القانونية الوقائية بغية التصدي لعولمة الجريمة من خلال تنظيم المعاملات عبر الوسائط الإلكترونية الرامية إلى إقرار حماية البيئة التقنية ضد القراصنة، مما يستهدي على مبدئية تأطير ضوابط عقابية إجرائية لاسيَّما تتبع آثر الأنشطة الإجرامية التي تتخذ عقبات يسيرة في تعضيد طرق المكافحة، حينئذ جل الاهتمام الدولي على بناء جهود تنسيقية تكييفًا مع واقع التكنولوجيا التي باتت ساحة بلا حدود لارتكاب شتى الاعتداءات الواقعة على الأمن المعلوماتي كلما طالت شخصية محترفي شبكات التقنية، بينما يعهد الدور جليًا إلى السلطات الأمنية المختصة لمجابهة جرائم تقنية المعلومات في ضوء تسليط المشرع الوطني على تأسيس معايير قانونية ملموسة بشأن فض عواقب المعلوماتية على الصعيد الإقليمي الداخلي مع فعالية النصوص الجنائية بما يتوافق بين الواقع و المأمول.

مما يعزز روح التعاون الدولي للحد من حذافير الجريمة العابرة ذلك بعقد اتفاقيات ثنائية متعددة قد يخفف عن تلاحم النظم الإجرائية بين الدول في ظل غياب نموذج إجرامي موحد من المشكلات الموجهة على التشريعات الوطنية، إذ يستدعي ممارسة ميدانية في سياق التعاون الأمني القضائي بما يراعي طبيعة تلك المستجدات مع التشجيع على استخدام تقنيات التحقيق الجنائي المساعدة في عمليات ضبط مادة الجريمة إفادةً للإثبات أمام العدالة لاسيَّما تجميع المعلومات، الوصول للأدلة، تسليم المجرمين، المساعدة القضائية العمليات المشتركة في إطار التدريب التقني على المحققين، القضاة، الشرطة القضائية تطبيقًا لأحكام الاتفاقية العربية، لكي تتحقق تلك الأجهزة بدرجة من الكفاءة الفاعلة على كشف غموض المنظمات الإجرامية الماسة على سرية الدولة، القبض على مجرمي المعلوماتية في زمن قياسي وجيز قد يتم إلا بتطوير أساليب التأهيل العلمي الفني، مواصلة الدورات التدريبية في ميدان المعلوماتية، اكتساب الخبرة التقنية في مجال الجهود الدولية كذا استقطاب المتخصصين بالانضمام إلى مصالح الأمن، إيمانًا من السلطات الجزائرية التي ليست بمعزل عن التهديدات الأمنية داخل الفضاء الافتراضي بل حاول سد الثغرة القانونية ولو نسبيًا بإجراء تعديلات مستحدثة من الناحية الموضوعية الإجرائية مع استصدار قواعد قانونية مستقلة، ضف إلى تكثيف الجهود الأمنية الوطنية على ردع المقنَّعين الذين يعمَّدون إخفاء أفعالهم الإجرامية في ضرب الحزام الأمني دون وقوع تحت طائلة العقاب بل يتطلب استمرارية المكافحة معتمدًا آلية التعاون الدولي الفعال.

تطبيقًا على ذلك سنعالج خلال الدراسة على دور المؤسسات العملياتية في التصدي الجريمة المعلوماتية **(المطلب الأول)** ثم نبين مسألة الجهود التشريعية الدولية في مواجهة الجريمة المعلوماتية **(المطلب الثاني)** بعدها نعرج عن الحلول المقترحة لمكافحة الجريمة المعلوماتية **(المطلب الثالث).**

المطلب الأول
دور المؤسسات العملياتية في التصدي الجريمة المعلوماتية

تتمحور الخطة الأمنية على تعزيز الفاعليَّة والنجاعة تجاوبًا مع المستجدات الراهنة نظرًا إلى استفحال فضاء الإجرام كذا تنامي الاحتجاجات الواقعية الناجمة عن الإخلال بالمنظومة القانونية الوطنية، مما تسعى إلى تكييف مؤسساتها الأمنية القضائية في قمع الاعتداءات الماسة عليها، حيث تبنت طرائق عديدة بما في ذلك تطوير الأداء العملي على الجهات القضائية ليتلاءم طبيعة الجرائم المراد الوقاية منها إطلاقًا، إذ تم إعداد مشروع قانون لمنتسبي الأمن الوطني تحت رقم 10-322 المؤرخ في 22 ديسمبر2010 باعتباره جهاز احترافي يتولى على صيانة أمن المجتمع معتمدًا بذلك خطة منهجية تتناسق فيها التدابير مع الغايات غرضه السياسة الوقائية، انطلاقًا من تحليل المعطيات المتعلقة بالمجتمع الجزائري، مواكبة العلوم ذات الصلة بالأمن الوطني بمقتضاه تم إنشاء تشكيلة ميدانية متخصص في مكافحة المعلوماتية التي تجتهد على تحقيق الرسالة السامية في إنجاز خدماتها الأمنية الإنسانية نحو متابعة الجرائم بالحد من التهديدات الهاجسة داخل الإقليم الوطني تعزز استراتيجية الهيكلة الأمنية بإنشاء خلية مكافحة الجريمة المعلوماتية لسنة2011 التابعة إلى نيابة مديرية القضايا الاقتصادية المالية لمديرية الشرطة القضائية بينما تم وضع فرع متخصص لسنة 2015 تابع لذات المديرية بما يتناسب مع اهداف تكنولوجيا الاعلام و الاتصال التي تشرف المصلحة على المستوى المركزي بقيام أسس النشاط العملياتي في التكوين والوقاية وفق مهام محددة، فلا ننسى تلك الأجهزة بالحاجة إلى التنسيق التعاون الدولي سواء فيما يتعلق التحقيقات المساعدة القضائية، التحريات العابرة الحدود في إطار المكافحة الدولية، التأمين على المراقبة التقنية في البيئة الافتراضية لحماية الأنظمة المعلوماتية، المشاركة في التكوين الأبحاث العلمية الأكاديمية بغية دعم الخبرة التقنية القانونية على الشرطة القضائية، التدريب على متطلبات الاحترافية في مجال الإعلام الآلي، استقطاب المتخصصين في ميدان المعلوماتية لاكتساب الكفاءة المؤهلة من قبل المديرية العامة للأمن الوطني وفق رزنامة التعاون الدولي كي تعم الإفادة بين اسلاك الشرطة القضائية ضف إلى ذلك تبادل علاقات تنسيقية في مجال التكوين

الخاص مع مؤسسات البحث العلمي في ميدان الأمن المعلوماتي و التحقيق الجنائي ناهيك عن الملتقيات الدولية في بناء روح المكافحة الوطنية الدولية.

علاوة على ذلك سنعرض خلال هذا المطلب عن المكافحة المؤسساتية الوطنية **(الفرع الأول)** ثم نأتي إلى المكافحة المؤسساتية الدولية **(الفرع الثاني)** بعدها نعرج لمكافحة الجمعيات على الجريمة التقنية (**الفرع الثالث**).

الفرع الأول
المكافحة المؤسساتية الوطنية

لقد خصَّت التشريعات القانونية مصالح ووحدات بشأن التصدي عن جرائم تقنية المعلومات فعلى الصعيد الوطني لإقليم الجزائر تم تكريس هيئات وطنية، مصالح مركزية تعالج جرائم المعلوماتية بما في ذلك الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني **(SCLCTIC)**، مركز الوقاية من جرائم الاعلام الآلي والجرائم المعلوماتية التابعة لقيادة الدرك الوطني **(CPLCIC/GN)**، المعهد الوطني للأدلة الجنائية و علم الإجرام التابع لقيادة الدرك الوطني **(INCC/GN)** إلى جانب ذلك قام المشرع الجزائري باستحداث منظومة لأمن الأنظمة المعلوماتية حتى يتسنى من تحقيق الاستراتيجية الوطنية على الأمن المعلوماتي التي تفرض عمليات حماية أنظمة المعالجة الآلية طالما أصبحت شرايين المعاملات الالكترونية في الوقت الراهن من خلال ربط قنوات الاتصال و شبكات الانترنت على المنصة العالمية، أما على الصعيد الدولي قد احتضنت معاهدات الرامية إلى التعاون الدولي الأمني لاسيَّما الإنتربول.

بناءً على المعطيات سوف نبين خلال الفرع عن المنظومة الوطنية لأمن الأنظمة المعلوماتية **(أولا)** ثم نعرج إلى وحدات الأمن الوطني المختصة في مكافحة الجريمة المعلوماتية **(ثانيا)**.

أولا: المنظومة الوطنية لأمن الأنظمة المعلوماتية

تجتهد المنظومة في السعي إلى تحقيق أمن المعلومات داخل الفضاء الافتراضي بمثابة ثروة ملحة تنشد كافة المستفيدين من الخدمات الإلكترونية إلى إقرار الحماية الملموسة ضد الهجمات التقنية التي تؤدي لاستفحال الجرائم بشتى ألوانها على البيئة الرقمية، حيث تفرض إلزامية حماية النظم المعلوماتية وفاءً على العهود التي قطعتها الدولة الجزائرية

في المجال من خلالها تم إصدار مرسوم رئاسي تحت رقم **20–05** المؤرخ في 20 جانفي 2020 تهدف إلى وضع منظومة وطنية لأمن الأنظمة المعلوماتية التابعة لدى وزارة الدفاع الوطني، مما باتت أداة الدولة في الإطار التنظيمي لإنجاز الاستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية الشاملة على مجلس وطني لأمن الأنظمة المعلوماتية المكلف بإعداد الاستراتيجية مع توجيهها، وكالة لأمن الأنظمة المعلوماتية المكلفة بالتنسيق تنفيذية الاستراتيجية، بالمقابل قد تتكفل المنظومة بإجراء التحقيقات في حالة وقوع الهجمات الإلكترونية، تقييم جمع المعطيات، تقديم المشورة على الهيئات العمومية ضف إلى مهام متعلق بالأمن السيبراني للمؤسسات العمومية.

من أجل معالجة هاتيه الهيئات يقتضي الإشارة إلى المجلس الوطني لأمن الأنظمة المعلوماتية ثم نتعرض إلى وكالة لأمن الأنظمة المعلوماتية فيما يلي:

- **1. المجلس الوطني لأمن الأنظمة المعلوماتية:**

عبارة عن خلية فرعية التابعة إلى المنظومة الوطنية لأمن الأنظمة المعلوماتية الذي يترأسه وزير الدفاع الوطني أو ممثله، حيث يحتوي المجلس من ممثل عن رئاسة الجمهورية، ممثل عن الوزير الأول، الوزير المكلف بالشؤون الخارجية، الوزير المكلف بالداخلية، الوزير المكلف بالعدل، الوزير المكلف بالمالية، الوزير المكلف بالطاقة، الوزير المكلف بالاتصالات، الوزير المكلف بالتعليم العالي، مما يستعين المجلس بإحدى المؤسسات بشأن تنويه الأعمال المقررة لها الذي يتوفر على أمانة تقنية المسيرة من قبل الأمين العام تحت تعليمات رئيس المجلس، إذ تتولى عدة صلاحيات بما في ذلك إنجاز مشروع القواعد الداخلية المنظمة على المجلس، جمع الوثائق اللازمة في تحضير ميزانية الأعمال لأي إدارة ذات مهمة حساسة منحت للأمانة التقنية التي ستتمكن من الاطلاع على معلومات الماسة بالخصوصية الفردية، بذلك يستدعي مرافقة آلية الحماية على الحرمة الشخصية مع التكفل من الانتهاك باسم القانون، بالمقابل تسهر الأمانة التقنية في تسيير الموارد البشرية المادية مع حفظ الأرشيف و الوثائق باعتبارها منسق بين المجلس والوكالة.[79]

بينما حددت المادة الرابعة من المرسوم الرئاسي رقم **20–05** المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية بداية تلك المهام المخولة على المجلس من خلال تحديد

(7) ـ حزام فتيحة، **"الحماية المؤسساتية للأنظمة الرقمية في الفترة التشريعية الممتدة بين 2009-2020"، " مجلة الأكاديمية للدراسات الاجتماعية والإنسانية"**، المجلد 13، العدد 2، كلية العلوم الإنسانية والاجتماعية، جامعة حسيبة بن بوعلي، الشلف، الجزائر، 2021، ص ص279–282.

عناصر الاستراتيجية الوطنية المقترحة من قبل الوكالة مع البث فيها، ثم يؤدي بدراسة التقارير المتعلقة بتنفيذ تلك الاستراتيجية المصادق عليها، تقرير نشاط الوكالة مع الاطلاع على مخطط أعمالها، فعلى المجلس الوطني دور جوهري في الموافقة على اتفاقيات التعاون مع الاعتراف المتبادل بين الهيئات الأجنبية في مجال أمن الأنظمة المعلوماتية، إذ يقتضي المساعدة الدولية في هذا المجال تبعًا لاستفحال عالم الإجرام التقني.

يسعى المجلس في صلاحية الموافقة على سياسة التصديق الإلكتروني المنجزة من قبل السلطة الوطنية للتصديق الإلكتروني، الموافقة على تصنيف الأنظمة المعلوماتية على سبيل المثال (نظم المعلومات الإدارية المسؤولة عن تقديم المعلومات اللازمة للإدارة، أنظمة دعم القرار التي تسمح باتخاذ الآراء المدعمة لحل المشاكل المطروحة)، فقد يتمكن المجلس من اقتراح التلائم بين الإطار الهيكلي أم التنظيمي الخاص بأمن تلك الأنظمة عند الضرورة مع إبداء الرأي عند اقتراح قوانين تشريعية تنظيمية ذي صلة بأمن الأنظمة المعلوماتية.[80]

➢ 2. وكالة أمن الأنظمة المعلوماتية:

عبارة عن مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي مقرها الجزائر العاصمة، حيث تتوفر الوكالة على مركز وطني عملياتي لأمن الأنظمة المعلوماتية، مصالح تقنية إدارية التابعة إلى سلطة المدير العام المسير لشؤون الوكالة، حيث تدير الوكالة لجنة توجيه مزودة على لجنة علمية ذات مهام محددة بمقتضى

(8) – La Cyber sécurité, Revue de la Gendarmerie Nationale avec la collaboration du centre de recherche de l'école des officiers de la Gendarmerie nationale, 4 trimestres, Edition esprit du livre, paris, 2012, p.04.

ـ المادة الرابعة من المرسوم الرئاسي رقم 20ـ05، المؤرخ في 20 جانفي 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج. ر. ج. ج، عدد 04، الصادر في 26 جانفي 2020.

ـ يتم الإشارة إلى نماذج مقارنة بين المؤسسات الأمنية المكافحة على المستوى الدول الأجنبية مع الدول العربية فيما يلي: سارعت الولايات المتحدة الأمريكية إلى إنشاء الأجهزة الأمنية المختصة في التصدي جرائم الأنترنت بما في ذلك المركز الوطني لحماية البنية التحتية التابعة إلى المباحث الفيدرالية، وكالة مكافحة القرصنة المعلوماتية، أما فرنسا قد ساهمت في إصدار مراكز متخصصة: المركز الوطني لمكافحة جرائم تكنولوجيا المعلومات الصادر بمقتضى قرار وزاري رقم 405/2000 على مستوى المديرية المركزية للشرطة القضائية التابعة لوزارة الداخلية، المركز الوطني لتحليل الصور الإباحية المكلف بضبط الصور، أما على الصعيد العربي هناك دولة الإمارات تمت تطبيق نظام الرقيب (PROXY) المكلف بالمراقبة على خدمات الأنترنت، بينما جمهورية مصر العربية تمت باستحداث الأجهزة الأمنية لمكافحة جرائم تقنية المعلومات منها الإدارة العامة للتوثيق والمعلومات المكلف في عمليات المتابعة الفنية، الإدارة العامة لمكافحة جرائم الحاسبات و شبكة المعلومات.

ABDE Kader, *« la loi Algérienne et le cyber criminalité »*, El Watan économie supplément N°18, 24/05/2005, Disponible en ligne à l'adresse suivante : http://elwatan.com

المرسوم الرئاسي رقم 20–05، مما تؤدي دور في التدقيق مجال أمن الأنظمة المعلوماتية تقديم اقتراح عن كيفيات اعتماد مزودي الخدمات، بناء المنظومات المعلوماتية، تسهيل عملية الحصول على معلومات متعلق في إطار الجريمة من خلالها تعمد على فحص الإمضاء الالكتروني، بينما منح القانون على الوكالة بإجراء تحقيقات رقمية حال حدوث الهجمات الإلكترونية ملزمة على السهر في تحليل المعطيات مع استخلاص المعلومات الملائمة، تحديد الأدلة العلمية، تقديم التوصيات التي تسمح بالتأمين منشآت المؤسسة الوطنية، مرافقة الإدارات العمومية لأجل وضع استراتيجية أمن الأنظمة المعلوماتية، بذل اليقظة التكنولوجية المساعدة على متابعة التطور التقني المرتبط بأنشطة المؤسسات، اقتراح مشاريع اتفاقيات التعاون مع الهيئات الدولية، إبرام مشاريع شراكة لأجل تعزيز ثقافة تأمين الأنظمة المعلوماتية بعد موافقة المجلس الوطني.

تفاديًا على المخاطر الناجمة لجرائم المعلوماتية في مواجهة أولئك القراصنة قد قامت العديد من الدول بشأن تأمين أنظمتها الوطنية سواء من الناحية التشريعية، الإجرائية، الميدانية لاسيَّما التشريع المصري تم بإنشاء المجلس الأعلى للأمن السيبراني، أما بالنسبة للتشريع الفرنسي استحدثت جهات فاعلة في مكافحة الجريمة المعلوماتية منها المديرية العامة للشرطة الوطنية (DGPN)، المديرية العامة للدرك الوطني (DGGN)، المديرية العامة للأمن الداخلي (DGSI)، ففي إطار تفاقم الأضرار المترتبة عن تلك الجرائم قد تم إصدار الوكالة الوطنية لأمن الأنظمة المعلوماتية (Agence Nationale de la sécurité des systèmes d'Information) المكلفة بالقيام كافة التدابير اللازمة لحماية الأنظمة المعلوماتية الفرنسية، تقييم أمن المنتوجات المتعلقة بأنظمة التكنولوجيا، اعتماد مراكز التقييم المطلوبة في إنشاء التوقيع الالكتروني بينما على الصعيد التعاون الدولي تسري الوكالة بالمشاركة في المفاوضات الدولية مع التواصل على نظيراتها، تعزيز قدرات الأمن السيبراني في الاتحاد الأوروبي.[81]

ثانيا : وحدات الأمن الوطني المختصة في مكافحة الجريمة المعلوماتية

(9) ـ نشله مصطفى، رابحي لخضر، " جريمة استهداف الأنظمة المعلوماتية للبنوك والمصارف"، **" مجلة العلوم القانونية والاجتماعية"**، المجلد 8، العدد 2، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، 2023، ص 978.

« The year2020 marks the Baining of a new Européen cycle. Europe must be able to asserte its sovereingnty in the cyber Field in ordre to promote its values of peace and stabilité in cyberspace at the international level »

FIC2020 : ANSSI calls for Européen sovereingnty in cyber Security, in the web site : https://www.ssi.gouv.fr/uploads/2020/01/anssi-press-release-fic-2020.pdf

التصدي على المعلوماتية من الأولويات الدولة الجزائرية، فلابد من الاستجابة للانشغالات الأمنية التي تسهر على صيانة الأمن العمومي داخل الفضاء الأزرق، مما سعت إلى إنشاء وحدات متخصصة لمكافحة الجريمة التقنية بما في ذلك المديرية العامة للأمن الوطني، قيادة الدرك الوطني ذلك ما سنفصله فيما يلي:

➢ 1. دور الشرطة الجزائرية في مكافحة الجريمة المعلوماتية:

من الأهداف الاستراتيجية التي تنويه مؤسسة الشرطة الاستعداد على عملية تتبع الجريمة وملاحقة مجرمي المعلوماتية للوقاية من مخاوفها المؤثرة على حماية الحريات العامة لأجل تشييد أداء المهام المسندة للأمن الوطني مثلما حددها التشريع الساري المفعول، وفي سبيل المكافحة الحادة خصص الأمن الوطني موارد بشرية من خلال تعزيز صفوف الضباط ذوي خلفيات جامعية عالي الكفاءة في ميادين العلوم الإنسانية الاجتماعية قد تستفيد من التدريبات في العلاقات العامة لإدارة عمل الفرق الشرطية التعامل مع حالات المجرمين، بينما تم تنظيم موارد هيكلية لمحاربة المعلوماتية لاسيَّما مديرية الشرطة القضائية، المصلحة المركزية لمكافحة الجريمة الالكترونية التابعة لمديرية الأمن الوطني الصادرة بمقتضى قرار من المدير العام للأمن الوطني سنة 2015، حيث وسعت الهيكلة الأمنية إلى فصائل على مستوى 48 ولاية التابعة لمصالح الولائية للشرطة القضائية ومن النماذج المثالية التي عالجتها تلك الفصائل لأجل مكافحة الجريمة التقنية بما في ذلك القضية المسجلة من قبل فرقة مكافحة الجرائم الالكترونية بالمصلحة الولائية للشرطة القضائية أمن ولاية عين الدفلى المتعلق بالغش في الامتحانات شهادة التعليم المتوسط دورة جوان 2019 بواسطة مواقع التواصل الاجتماعي.[82]

إذ أسفرت التحريات التقنية التي تجريها عناصر الفرقة بالتنسيق مع المصلحة المركزية لمكافحة الجرائم الالكترونية التابعة لمديرية الشرطة القضائية تحت إشراف الهيئات القضائية في توقيف ثلاثة متورطين وإحالتهم إلى العدالة، لأجل مواكبة التكنولوجيا، الرفع من المستوى المعرفي التقني على المحققين بمقتضاه تم استحداث صنفين من التكوين المتخصص، فالأول محقق في الجريمة المعلوماتية **ICC** متعلق بالمفتشية مصالح المحققة في مجال الجريمة المعلوماتية أما الثاني متدخل في الجريمة المعلوماتية **PICC**المتعلق بأعوان الشرطة العاملين في مجال مكافحة الجريمة المعلوماتية، بينما

(13) - براردي نعيمة، الاتصال بين الشرطة والمواطن ودوره في مكافحة الجريمة في الجزائر (دراسة تحليلية استطلاعية بالجزائر العاصمة)، رسالة لنيل شهادة الدكتوراه في علوم الاعلام والاتصال، كلية العلوم السياسية والاعلام، جامعة الجزائر 3، 2014، ص113.

يسعى الامن الوطني في التأهيل إعداد الكفاءات العلمية التقنية لمواجهة الإجرام ذلك في تطوير العملية التدريبية بغرض رفع مستوى الأداء الميداني على الاحتياجات الأمنية المستقبلية، حيث قامت المنظمات الحكومية الدولية بالتدريب رجال الضبط القضائي من خلال عقد دورات تكوينية في تزويد محققي الشرطة، العاملين في إدارات العدالة الجنائية على تقنيات الحوسبة باكتساب الخبرة المؤهلة في التحقيق الجرائم الالكترونية تنسيقًا مع الشركات الأكاديمية المتخصصة داخليا دوليا، بذلك تم إنشاء مرافق عديدة منها المعهد الوطني للبحث في علم التحقيق الجنائي الذي يضم خمس مخابر جهوية في(وهران، قسنطينة، ورقلة، بشار، تمنراست) المكلفة بإجراء التحاليل، الخبرة العلمية بشأن سير التحقيقات القضائية، الدعم التقني المجهز بالآليات الملائمة في تسيير مواقع حدوث الجريمة، التكوين الفني على السلسلة القضائية في مجالات البحث العلمي و علم التحقيق الجنائي، حيث تصنف المخابر الجهوية إلى مصالح مقسمة إلى مكاتب منها القسم التقني، مصلحة الخبرات المتعلق بالدلائل التكنولوجية المكلفة بإجراء تحليل الدلائل المادية إثر معاينة التحريات في ميادين الدلائل الالكترونية البصمات الصوتية، معالجة الصور، اعداد تقارير الخبرة التقنية المطلوبة منها السلطات القضائية، تسيير بنوك المعطيات في علم التحقيق الجنائي لاسيَّما المحفوظات الآلية للبصمات الصوتية، المخالفات المرتبطة بتكنولوجيا الاعلام و الاتصال.[83]

2. دور الدرك الوطني في مكافحة الجريمة المعلوماتية:

لا شك على قيادة الدرك الوطني من القوات الأمنية الفاعلة في محاربة السلاح التقني ووقاية الأمن المعلوماتي ذات دور جوهري في عملية تطبيق القانون، مما يسخر الإمكانيات المادية البشرية المعدة للمكافحة من أولويات الدولة الجزائرية في إطار الاستجابة الأمنية بإرساء الطمأنينة داخل الفضاء السيبراني الوطني، حيث بدأت الممارسة الميدانية في التصدي الجريمة الالكترونية خلال 2004 ثم استحدث بموجبه مركز الوقاية من جرائم الإعلام الآلي العصب المثالي في تسيير مهام اليقظة السيبرانية مع إلزامية احترام مبادئ القانون في الوقت الذي يبحر فيها ملايين المستخدمين عبر صفحات الأنترنت داخل البيئة الرقمية، بينما اجتهد المركز خلال 2008 على تأمين منظومة المعلومات لسلامة الأمن العمومي، قد يهدف ضباط الشرطة القضائية إلى ضبط الأدلة،

(14) ـ رشيد بلفكرات، "الجريمة الالكترونية كتهديد للأمن الوطني الجزائري"، "**مجلة العلوم القانونية والاجتماعية**"، المجلد 4، العدد 1، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، 2019، ص521.
ـ المرسوم الرئاسي رقم 19ـ 278، المؤرخ في 20 أكتوبر 2019، المتعلق بالمهام معهد الدراسات العليا في الأمن الوطني وتنظيمه وسيره، ج. ر. ج. ج، عدد 65، الصادر في 24 أكتوبر2019.

تحليل المعطيات، تحديد هوية مرتكبي المعلوماتية في ملاحقتهم بشأن دعم الجهات القضائية في التحقيق، إذ استطاع المركز معالجة حوالي **100** قضية خلال **2014** بينما تعلو الديناميكية المفعمة على المكافحة لدى الشرطة القضائية حوالي **500** قضية خلال **2015** ذلك فيما يتعلق جرائم المرتكبة عبر مواقع التواصل الاجتماعي المقدرة بـ**300** قضية أما القضايا الرقمية منها اختراق مواقع رسمية لمؤسسات عمومية مبتغيًا باستغلال الأنظمة المعالجة الآلية، وفي الخمسة الأشهر الأولى لسنة **2019** تم معالجة **1188** قضية ناجحة من مجموع **1515** قضية مسجلة مع توقيف حوالي **1512** متورط.[84]

قامت قيادة الدرك الوطني تنظيم حملات التوعية الحسية بالتنسيق مع وزارة التربية الوطنية على إفادة الطلاب ضد مخاطر الجريمة الالكترونية على غرار عملية المواكبة في ميدان التكنولوجيات يقتضي السعي في سبيل منح خدمات أمنية لإثراء تطلعات المواطنين، التفاعلية في تكوين إطارات لدى قيادة الدرك من خلال إنشاء معاهد التابعة لقيادة الدرك بما في ذلك المعهد الوطني للشرطة القضائية(سحاولة الجزائر العاصمة)، المعهد الوطني للأدلة الجنائية و علم الاجرام (بن شيشة أحمد بوشاوي الجزائر العاصمة) الذي يتم بإجراء الفحوص العلمية في إطار التحريات الأولية مع التحقيقات القضائية معتمدًا مناهج الشرطة العلمية التقنية الرامية إلى تحليل الوثائق المأخوذة من مسرح الجريمة بناءً على تصريح قانوني من السلطات القضائية، تصميم بنوك المعلومات كالبصمات الجينية بشأن استخلاص الروابط المحتملة بين المجرمين و دوافع النشاط الإجرامي باعتبار المعهد مؤسسة مجسدة في تحديد السياسة الجنائية المثلى لمكافحة الإجرام من خلال ترقية البحث التطبيقي، ثبوتية التحريات في ميدان الأدلة الجنائية على الصعيد الوطني الدولي مستعينًا بالتقنيات الدقيقة بشأن الاستفادة من النتائج المنوط إليها، بذلك يظل المعهد الوطني من بين المؤسسات الناجحة على عملية المكافحة.

عمدت الدول الأجنبية الغربية إلى تشكيلة الأجهزة المختصة لإجراء التحريات المعلوماتية، تقرير الخبرة الفنية بما في ذلك الولايات المتحدة الأمريكية التي قامت بإنشاء المعمل الإقليمي الشرعي للإعلام الآلي التابع لمباحث الفيدرالية الأمريكية (FBI) خلال 2002 المسمى بـ مكتب البرنامج الوطني **(The Régional computer forensices laboratoy)** الذي يتم بإجراء الفحص الشامل للأدلة الالكترونية نقطة اتصال إقليمية لقضايا الأدلة الإلكترونية، منح خدمات مهنية تقنية في الطب الشرعي

(17) ـ سليمة نواوي، دور الدرك الوطني في محاربة الجريمة الالكترونية (المجموعة الإقليمية للدرك الوطني بالمسيلة أنموذجًا)، مذكرة مكملة لنيل شهادة الماستر في علوم الاعلام والاتصال، كلية العلوم الإنسانية والاجتماعية، قسم علوم الاعلام والاتصال، جامعة محمد بوضياف، المسيلة، الجزائر، 2019، ص48.

الرقمي، فعلى الدول مواصلة جهودها الرامية إلى تطوير الهياكل المختصة في المكافحة داخل هيئات إنفاذ القانون و الجهاز القضائي بشأنها الحصول على المعدات اللازمة ضد التحديات المفروضة على الجريمة السيبرانية في دعم مصداقية الإجراءات الجنائية أمام الجهات القضائية المختصة.(85)

الفرع الثاني
المكافحة المؤسساتية الدولية

أضحت البيئة الرقمية على نقاب حاد إثر مداهمات القراصنة الذين يبتغون ممارسة أعمال تخريبية تقنية من شأنها إلحاق ملامح مخيفة على أمن المعلومات التي تنصب بالمنظمات القانونية الدولية، مما يدفع الحال إلى رصد الآليات المؤسساتية كفيلة في محاربة نماذج الإجرامية ذلك بناءً على توطيد العلاقات الدولية بين الجهاز الأمني القضائي نحو معالجة الإدمان داخل الفضاء الافتراضي، حيث يقتصر ترقية المصالح الأمنية الإدارية على الحيز الإقليمي الدولي لضمان تعزيز التعاون الدولي المشترك في المكافحة، بالمقابل تسخير الموارد البشرية المساهمة في إنجاح الخطة الأمنية على الميدان الدولي لاسيَّما المنظمة الشرطة الجنائية (الإنتربول) باعتبارها مؤسسة شرطية دولية ذات دور اتحادي فعال، أما بالنسبة إلى المؤسسات الإقليمية من الافريبول، اليوروبول،

---

(18) – JANKARI Rachid, *« Les technologie de l'information au Maroc, Algérie et en Tunisie, vers une filière euromaghrébine des TIC »*, études et analyse, l'Institut de prospective économique du monde méditerranéen, France, 2014, p.19

ـ سجلت مصالح الدرك الوطني المختصة في مكافحة الجريمة الالكترونية خلال عامي 2012/2011 بما يقارب 153 إلى 175 قضية. منشور على الموقع الالكتروني الموالي https://www.ons.dz/spip.php?rubrique327

Cybercriminalité : un programme de sensibilisation bientôt lancé par la Gendarmerie nationale, dimanche24 juin2018 à 12:09, disponible sur site : http://www.elmoudjahid.com/fr/actualites/89227

ـ حملة تحسيسية على الفضاء السيبراني راجع في ذلك تصريح السيد قائد الدرك الوطني اللواء مناد نوبة، يومية الجمهورية، العدد 6449، يوم الأربعاء 28 مارس2018 متاح على الموقع الالكتروني الموالي https://www.eldjoumhouria.dz/Images/5abaa9b

ـ تنص المادة الثانية من المرسوم رقم 04-183 ما يلي:**" المعهد مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي يوضع تحت وصاية وزير الدفاع الوطني... يخضع إلى جميع الأحكام التشريعية التنظيمية المطبقة على المؤسسات العسكرية."**

المرسوم الرئاسي رقم 04 -183، المؤرخ في 26 جانفي 2004، المتعلق بإحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج. ر. ج. ج، عدد 41، الصادر في 27 جانفي 2004.

ـ تقرير عن اجتماع فريق الخبراء المعني بدراسة عن الجريمة السيبرانية المنعقد في فيينا من الفترة 27 إلى 29 مارس 2019 المزيد من التفاصيل على قيادة الدرك الوطني الرجوع إلى الموقع الرسمي الالكتروني التالي www.mdn.dz/

الاوروجيست الخاضعة للاتحاد الأوروبي مدعمة على سبيل الاستئناس في ميدان المكافحة، فلا ننسى عقد اتفاقيات ثنائية دولية تنادي بالانسجام على تشجيع روح التعاون سواء بين الدول الشقيقة أم الأجنبية لعلها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة في القاهرة التي صادقت عليها الجزائر في 2010 الهادفة إلى تبني سياسة جنائية متحدة لحماية الأمن العربي ضد التهديد التقني مع إلزامية مراعاة مبادئ المعاهدات و المواثيق العربية الدولية ذات الصلة بالضمانات الشخصية، تنفيذ المساعدات القضائية في تظافر جهود الأمنية عند ملاحقة المجرمين و تسليمهم بأقصى سرعة متناهية، التنسيق في تبادل المعلومات المساعدة في المسائل الجنائية، نقل الإجراءات، الانابة القضائية من آليات التعاون القضائي الدولي.

للإحاطة على النقاط الملموسة في الدراسة يقتضي الإشارة إلى إحدى الآليات الملمة في مكافحة الجريمة التقنية على الصعيد الدولي بما في ذلك التعاون الأمني الدولي التي تقتصر على منظمة الشرطة الجنائية الدولية **(أولا)** ثم الولوج إلى مسألة التعاون القضائي الدولي سوف نلتمس إلى المساعدة القضائية الدولية، تسليم المجرمين **(ثانيا)** بعد ذلك نعرج إلى العقبات الموجهة على التعاون الدولي**(ثالثا).**

أولا: التعاون الأمني الدولي

رغم قصور التشريعات الوطنية في سبيل المكافحة على عواقب المعلوماتية داخل المحيط الافتراضي قد يتطلب ذلك تعاونًا دوليًا لتخطي المشكلات التي تعترض الجهود الوطنية في تعقب مصادر التهديد المعتمدة على شبكات التقنية لارتكاب جرائم عابرة الحدود من قبل محترفين ذات أدمغة ألية يتحدون أيدي الأجهزة الأمنية، مما نتصور هناك تنافس بين القوى الأمنية القانونية في حماية البيئة الرقمية من إنتهاك خصوصية النظام المعلوماتي محلًا لأداء المعاملات الميدانية والشغف للانضمام إلى فضاء الإجرام الذي يعد عائقًا أمام سلطات الأمن في ممارسة التحري لإثبات واقعية الدليل الخفي، تعذر الكشف عن هوية مجرمي المعلوماتية لانعدام رؤيته على المسرح الافتراضي، حيث تسعى الهيئات الدولية في تبادل المشاركة التنسيقية لردع تلك العقبات المؤثرة على سلامة استقرارها الداخلي نظرًا إلى تفاشي حذافير الجريمة، فلابد من اتخاذ تدابير قانونية تدعم سبل التعاون الدولي بمثابة الحبل السري لالتقاء العلاقات الدولية في تفادي مخاطر المعلوماتية على الصعيدين الوطني الدولي و ملاحقة المجرمين بإحالتهم إلى العدالة، فكلما سادت معالم الإجرام بات الجهاز الأمني في تلاشي لفك الخيوط المقيدة على عاتقها، بذلك ننادي على توفيق المعايير التشريعية الدولية لبناء استراتيجية احترازية تحقق حصر

معدلات الجريمة دون استفحالها و السعي في توعية التكامل الأمني بين مؤسسات الشرطة على المستوى الدولي من أجل إنهاء معارض المنظمات الاجرامية، بالمقابل تطوير الإجراءات الفاعلة على سير القضاء الجنائي في إطار المكافحة الدولية، ربط أجهزة الشرطة على قنوات الاتصال لتبادل المعلومات الهادفة بين مصالح الدول.

تطبيقًا على ذلك سوف نحدد الآليات الأمنية المساعدة على المستوى الدولي منها المنظمة الدولية للشرطة الجنائية (الإنتربول) التي تعاهدت إليها أغلبية الدول لاسيَّما التشريع الجزائري المجسدة في أحكام قانون الإجراءات الجزائية، بالمقابل هناك مؤسسات إقليمية نتيجة حتمية في توحيد مجهودات الدول على النطاق الجغرافي ذات دعامة أمنية قوية في المكافحة لعلها الاتحاد الإفريقي للتعاون الشرطي (Afripol) جاءت لأجل مضاعفة رصيد التعاون الشرطي في إفريقيا بالتنسيق مع المؤسسات الدولية الإفريقية المنعقدة في مدينة وهران بالجزائر و الذي سنبينه في النقاط الموالية:[86]

➢ 1. الشرطة الجنائية الدولية (الإنتربول):

عبارة عن آلية التعاون الشرطي في مكافحة الإجرام المنظم على الصعيد الدولي المنعقدة في مدينة باريس الفرنسية عام 1923 التي أُعترفت من قبل الأمم المتحدة عام1971، مما تهدف إلى التنسيق بين مؤسسات الشرطة الدولية بشأن تعقب المجرمين في ملاحقتهم مع مبادرة تكثيف الجهود الإقليمية، الوطنية، الدولية ضد التحالفات الإجرامية، حيث تنقسم شبكة اتصالات الإنتربول إلى ثلاث مدرجات هرمية: المكاتب المركزية الوطنية، المحطات الإقليمية، الأمانة العامة للإنتربول قد تضم المنظمة حوالي 194 دولة عضو لكل منها مكتب مركزي وطني(NCB) متحد بشبكة الإنتربول العالمية.[87]

---

(23) ـ خالد بن مبارك القحطاني، التعاون الأمني الدولي في مواجهة الجريمة المعلوماتية عبر الوطنية، أطروحة لنيل شهادة الدكتوراه في العلوم الجنائي، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2013، ص38.

(24) –ILIANG Jiansheng, *« Criminalité informatique »*, Diplôme professionnel supérieur en Sciences de l'information et des Bibliothèques, Rapport de stage, École Nationale Supérieure des Sciences de l'information et des Bibliothèques, Paris, 2009, Disponible sur le site http://www.eldjazaircom.dz/index.php?id-rubrique=313&id-article=3745 , N° 114-juin2018.

(24) ـ نادية دردار، الجهود الدولية لمكافحة الجريمة، المركز القومي للإصدارات القانونية، القاهرة، 2017، ص150.

ـ للاطلاع على المزيد من التفاصيل يتم الرجوع إلى الموقع الرسمي التالي: Le 17/12/2019 https://www.interpol.int/ar/3/10

INTERPOL, Résolution N° 5, **GA-2018-87-RES-05 : « RAPPELANT ÈGALEMENT la résolution AG-2016-RES-03 qui a approuvé le cadre stratégique 2017-2020 d'INTERPOL, lequel visait notamment à optimiser le rôle d'INTERPOL au sein de l'architecteur de sécurité mondiale, ainsi qu'à renforcer la relation entre INTERPOL, les organisations de police régionales et les autres organisations internationale, pour combler les lacunes et**

عند التمعن في الرابط المشترك بين الدول بالإنتربول لاسيَّما التشريع الجزائري الذي احتضن المنظمة مباشرة بعد الاستقلال مستندًا مبادئ الاتفاقية في قانون الإجراءات الجزائية من خلال انجاز الطلبات الواردة في استمارات الإنتربول، أما بالنسبة لجمهورية مصر العربية قد تم إنشاء المكتب المصري للشرطة الجنائية الدولية بمقتضى قرار وزير الداخلية سنة1948، إذ تتولى الإنتربول مهام مجسدة بين المنظمات العالمية الناجحة في مكافحة الجرائم العابرة للحدود من خلال تأمين الاتصال الرسمي بين رجال الشرطة الدولية بغية تبادل الخبرات لاسيَّما تجميع المعطيات الرقمية من شتى المكاتب المركزية الوطنية في دول الأعضاء، تعقب مجرمي المعلوماتية إلى حين تسليمهم، القيام بعملية التفتيش للأنظمة المعلومات مع شبكات الاتصال لأجل ضبط الأدلة الرقمية، تبادل المعلومات على منصة الاتصالات بغية تسهيل التحقيقات الجنائية التي تجريها وكالات وزارة العدل ووزارة الأمن الوطني، تعزيز العلاقة بين الإنتربول مع منظمات الشرطة الإقليمية لسد الثغرات المنطوية على المكافحة، الحفاظ على القرائن الرقمية، الدعم التكويني الفني لأجهزة الشرطة، تنمية المؤسسات الأمنية الفعالة في الوقاية من جرائم الأنترنت، تشجيع أنشطة الأمن السيبراني.

تتسم المنظمة الدولية على دور حيوي بين شتى أجهزة الشرطة العالمية مع المنظمات الإقليمية الدولية من خلال موقعها الهام الذي يسمح في تنامي القدرة الفاعلة على منع الجريمة وتحديد هوية المجرمين باعتقالهم طالما أنَّ الإدمان التقني من التحديات المكبلة بين الدول، فمازالت المنظمة تسعى إلى بذل مجهودات لمكافحتها على سبيل المثال: تلقت النيابة العامة اللبنانية برقية من الإنتربول في ألمانيا الذي تم على إثرها توقيف أحد الطلبة الجامعيين من قبل القضاء اللبناني على تهمة إرسال صور إباحية لقاصر دون 10 سنوات من موقعه على شبكة الإنترنت.[88]

accroitre la complémentarité. » ; INTERPOL General Secrétariat, GLOBAL CYBERCRIME STRATEGY-200, quai Charles de Gaulle- 69006 Lyon-France- www.interpol.int, February2017,p.03.

(25) – QUEMENER Meriem, *« le rapport sur la cybercriminalité et la protection des internautes »*, la base de donnés juridique des Éditions Dalloz, France, AJ Pénal 2014, p.316.

ـ للإشارة إلى أمثلة نموذجية تدعيمية على الجهود المقدمة من قبل منظمة الإنتربول بين أعضاء الدول المبينة فيما يلي:
قدم الإنتربول مساعدة "لكولومبيا" في شهر مارس 2008 من خلالها قام الخبراء المختصين في الأدلة الجنائية على تحليل معدات حاسوبية تم ضبطها عند مداهمة أحد مخيمات القوات المسلحة الكولومبية في إطار عملية مكافحة المخدرات

➢ 2. الاتحاد الإفريقي للتعاون الشرطي (الآفريبول):

عبارة عن آلية مؤسساتية تقنية إقليمية لمكافحة جرائم العابرة الخاص بالدول الإفريقية التي أنشئت لأجل مضاعفة رصيد التعاون الشرطي في إفريقيا على المستويات الاستراتيجية التكتيكية بين أجهزة الشرطة في إفريقيا لمنع الجريمة العابرة للوطنية بالدعم مع المؤسسات الشرطة الوطنية الإقليمية الدولية، لقد شكلت **الندوة الجهوية الإفريقية الثانية الـ 22 للإنتربول المنعقدة أيام 12/11/10 من سبتمبر 2013 بمدينة وهران(الجزائر)** الانطلاقة الرئيسية لإنشاء الآفريبول الذي تبنى كلا من المدراء، المفتشون العامون للشرطة من دول الأعضاء للاتحاد الإفريقي، مما أعلن في اللقاء المنعقد بالجزائر بتاريخ 11 فيفري 2014 على فكرة إنشاء الآلية الإفريقية للتعاون الشرطي **"آفريبول"**[89]، حيث يؤكد انعقاد الجمعية العامة الأولى لآلية الاتحاد الإفريقي في مجال التعاون الشرطة بمثابة التأسيس الفعلي للآفريبول الذي تم في الفندق الأوراسي بالجزائر العاصمة أيام 16/15/14 من شهر ماي 2017 بعد المصادقة على القوانين المنظمة للآفريبول من قبل قادة الحكومات الإفريقية خلال القمة العادية الـ28 للاتحاد الإفريقي المبرمة بالعاصمة الإثيوبية "أديس أبابا" شهر جانفي 2017.[90]

يسعى الاتحاد الإفريقي " آفريبول" في ظل المبادئ المعلنة من القانون الأساسي لآلية التعاون الشرطي تحقيق غايات ناجعة الواردة بمقتضى المادتين 4/3 منها مساعدة مؤسسات الشرطة في دول الأعضاء على إعداد استراتيجية إفريقية منسقة لمكافحة شتى جرائم العابرة على المستويات الوطنية، الإقليمية، القارية، الدولية تطوير أنظمة الاتصال

والإرهاب، حيث استخدموا تقنيات متطورة أثناء عملية التحليل على كمية هائلة من البيانات المشفرة تحصلوا منها على أدلة رقمية مكنت من إثبات الوقائع الإجرامية، أما خلال 2017 تمت وحدة مكافحة الجرائم المرتكبة ضد الأطفال التابعة لمنظمة الإنتربول عن كشف فيديوهات لاعتداءات جنسية المرتكبة ضد 11 طفلًا دون 13 سنة من قبل شخص يدعى Muntrie salangam المقيم في تايلند صاحب الموقع الرسمي للصور الإباحية ثم خلال شهر جوان 2018 تم الحكم على المجرم أمام القضاء التايلندي لمدة 146 سنة إثر عمليات الاغتصاب الأطفال مع الترويج بالمواد الجنسية و الاتجار بالبشر.
https://www.interpol.int/ar/1/1/2019/50-9

(26) – Déclaration d' Alger relative à la création du mécanisme africain de coopération policière AFRIPOL, Conférence africaine des directeurs et inspecteurs généraux de police sur AFRIPOL, Alger , le 10 et 11 février 2014, sur le site: http://www.peaceau.org/uploads/algiers-declaration-afripol-french.pdf

– قرار رقم 16 (GA-2017-86-RES-16) المتعلق بالتعاون بين الإنتربول وآلية الاتحاد الافريقي للتعاون الشرطي (الآفريبول) الذي تمت المصادقة عليه بالجمعية العامة للإنتربول الدورة الـ 86 ما بين الفترة 26–29 سبتمبر 2017 في بيجين (الصين).

(27) - جوزي صليحة، **"الجزائر تحتضن الجمعية العامة الأولى لآلية الاتحاد الإفريقي في مجال التعاون الشرطي (الآفريبول)"**، **"مجلة الشرطة"**، المجلد 27، العدد 136، الجزائر، 2017، ص09. متاح على الموقع الإلكتروني التالي: https://Afripol.africa-union.org

مع قواعد البيانات بين أجهزة الشرطة في دول الأعضاء بواسطة برامج متطورة من خلال إنشاء مركز الاستخبارات الالكترونية مثلما تم الإشارة إليها في إحدى توصيات أشغال الجمعية العامة الثانية للآفريبول المنعقدة يومي 15/ 16 من شهر أكتوبر 2018 بالجزائر العاصمة التي دعت إلى تفعيل نظام الاتصالات(AFSYCOM) لقوات الشرطة بغية تبادل المعلومات فيما يتعلق التحقيق الجنائي للأدلة الرقمية، تشجيع التكوين المستمر على التدريبات الفنية للأعوان الأمنيين، الوعي الإفريقي لردع القراصنة المعلوماتية على المستوى القارة الإفريقية، التنسيق الأمني بين الإنتربول مع الآفريبول لأجل توفير الاستقرار الاقتصادي ضد الهجمات الالكترونية، تكاد منظمة الآفريبول آلية فعالة في ميدان التعاون الشرطي الذي يضمن ردًا مشتركًا على كافة التهديدات الماسة بالبلدان الإفريقية لاسيَّما الجزائر ذات مقومات نوعية في أمانة القارة الإفريقية التي احتضنت مقر الآفريبول اختيارها لرئاسة المنظمة عهدتين متتاليتين، أما بالنسبة لشرطة الويب الدولية تم انعقادها في الولايات المتحدة الأمريكية عام 1986 مكلفة بتلقي شكاوى مستخدمي الشبكة ملاحقة القراصنة عبر الفضاء الافتراضي معتمدًا شبكات الاتصال الدولية، مما تهدف لإجراءات التعاون مع وكالات إنفاذ القانون بين دول الأعضاء ذلك قد يسهل على فريق العمل تتبع الأنشطة الإجرامية عبر الشبكة العالمية، إذ ارتأينا للإشارة عن المنظمات الأمنية الناجحة التي شاركت فيها الدولة الجزائرية عضو فعال على المستوى الأوروبي للإنتربول بينما المستوى الافريقي منتخبة على رئاسة المنظمة [91]

ثانيا: التعاون القضائي الدولي

عزم الهيئات القضائية الدولية على الحد لإفلات مجرمي المعلوماتية من العقاب ووقف الزيادة غير الطبيعية لمعدلاتها على سلامة الأمن الداخلي الدولي الذي يعد مشروعًا إستباقيا في التقليل واقعية الجريمة نحو البحث على تدابير وقائية يجب مراعاتها لإنجاح عملية المكافحة من خلال تظافر المساعدات المشتركة بين السلطات القانونية القضائية الهادفة إلى الصبغة غير الوطنية للجريمة في سبيل ملاحقة الجناة مع التحري عن الأدلة معتمدًا الآليات التقنية الرقمية، ذلك مالا تملكها الجهات القضائية الوطنية طالما لم تساند الجهود القانونية الدولية التي تمد يد العون في مجابهة الأنشطة غير المشروعة لاسيَّما المرتكبة عبر الإنترنت صعب المنال على عرقلة إجراءات التحقيق الذي يستغرق زمنًا طويلًا نظرًا إلى مرونة الجريمة لارتكابها عبر الشبكات الآلية دون التحكم لأروقتها المتسمة بالبعد الوطني ضف إلى الأدمغة المتسللة في نشوزها، فكلما توحدت المعاهدات

(28) ـ إسكندر غطاس، الندوة العربية حول التعاون الأمني الدولي في المجال الجنائي على العالم العربي، دار القلم، دمشق، 2014، ص21.

الدولية سادت المرجعية القانونية في تجسيد عمود المكافحة نحو إزالة التحديات الشائكة على بصمة التعاون الدولي الفعال لاسيَّما في إطار ضبط الأدلة الرقمية ذات تعقيد في المسائل الجنائية مالا يتعارض ضمانات التعاون الدولي. (92)

علاوة على ذلك قد يثبت الواقع العملي على أنَّ المبادرة الوطنية بشأن القضاء على محدودية الجريمة التقنية غير قادرة على دعامتها مالم يكن هناك توافق بين السياسة الجنائية الداخلية بآلية التعاون الدولي مقدمة ناجحة نحو تحقيق نتائج إيجابية على تصدي الهيمنة الرقمية العالمية.

بناءً على المعطيات المتداولة خلال الدراسة يتعين علينا الإشارة لأهم صور التعاون القضائي الدولي منها المساعدة القضائية ذات فعالية مرشدة في ميدان تعقب المجرمين بملاحقتهم إلى حين تسليمهم للعدالة مما يبدو على دور مرن في المسائل الجنائية لاسيَّما فيما يتعلق تبادل المعلومات، نقل الإجراءات القانونية، الإنابة القضائية إلى جانب آلية تسليم المجرمين بات حاجزًا أمام النطاق الإقليمي بين الدول الذي لا يتجاوز تعدي الحدود في ممارسة تطبيقاتها القضائية على عملية فرار مرتكبيها بل ينبغي اتخاذ الإجراءات داخل رقعتها من شأنها يتم تسليم المجرمين إلى الدولة المختصة لمحاكمتهم مالم تسمح تشريعاتها الوطنية، في هذا السياق سوف نتناول تلك العناصر فيما يلي:

➢ 1. المساعدة القضائية الدولية:

يقصد تلك الإجراءات القضائية المتفاوضة بين السلطات القانونية الدولية فيما يتعلق المسائل الجنائية لاسيَّما المحاكمة الجنائية، الملاحقة القضائية، تسليم المجرمين، مما تتفرع آليات التعاون القضائي في الميدان الجنائي باختلاف المساعدة القضائية المستمدة من المعاهدات الثنائية الدولية بشرط استيفاء الالتزامات المتخذة على العضوية دون إنتهاك ضمانات المحاكمة العادلة أو اتخاذ تدابير إجرائية خارج إطار الاتفاقية، إعمالًا على تجسيد تلك المبادئ المعلنة بين سيادة الدول لابد من تقوية التعاون لاتحاد الإجراءات القضائية على أقاليمها الداخلية لاسيَّما التشريع الجزائري الذي نظم كيفية قبول طلبات المساعدة القضائية فيما يتعلق جمع الأدلة من خلال البريد الالكتروني، أجهزة

(29) ـ أحمد عبد اللاه المراغي، التعاون القضائي في مكافحة الجريمة الالكترونية ودور القانون الجنائي في الحد منها، (دراسة تحليلية تأصيلية مقارنة)، المركز القومي للإصدارات القانونية، القاهرة، 2017، ص126.

الفاكس آلية مضمونة لطلب المساعدة دون المساس بالسيادة الوطنية مع الحفاظ على سرية المعلومات المبلغة بينما اشترط الاستخدام في إطار الغرض المحدد لأجله ثم فعالية التحقيق والملاحقة القضائية في جرائم تقنية المعلومات غالبًا ما تقتضي تتبع أثر النشاط الإجرامي من خلال ربط قناة الاتصالات بالأنظمة الآلية، شبكات الأنترنت تنسيقًا مع مقدمي الخدمات بمثابة وسطاء داخل البيئة الافتراضية ذات دور تقني يساعد تسهيلات عملية التحقيق الجنائي.

حيث تناولت اتفاقية بودابست لمكافحة جرائم المعلوماتية وفق المادة 24 على تحديد شروط تسليم المجرمين ثم فصلت المادة 25 لأحكام المساعدة القضائية في مجال المكافحة، بينما التشريعات الوطنية لاسيَّما القانون الجزائري الذي نص على مبدأ المساعدة القضائية الدولية المتبادلة بمقتضى المادة 16 من القانون رقم 09ـ04 المتعلق بتكنولوجيا الإعلام والاتصال معتبرًا في إطار التحقيقات القضائية لمعاينة الجرائم التقنية قد يتسنى على السلطات المختصة تبادل المساعدة القضائية فيما يتعلق الأدلة الرقمية التي تتحقق بواسطة ثلاث خطوات متتالية: تقديم الطلبات الخاضعة لنطاق الاتفاقية المتعاقدة بين الدولتين، مما يتم الطلب وفق الطرق الدبلوماسية التي تسمح بالاتصال المباشر على الجهات القضائية ثم تقوم الدولة المساعدة بالتحقق من الواقعة المطلوبة بمثابة جريمة طبقًا لقانون الدولة المستنجدة يد المساعدة في ضوء مدى اختصاص دراسة الطلب قد يسري الرد وفقًا لأحكام الاتفاقية المتعاقدة، بينما يتم تنفيذ الإجراء وفق لمقتضيات الاتفاقية الدولية الوسيلة المتبعة لالتزامات التعاون الدولي من ثم انعدام الشروط السارية في الاتفاقية تصبح المساعدة دون جدوى لاعتمادها تلقائيًا، إذ تتخذ المساعدة القضائية صور عديدة مماثلة التي سنبينه فيما يلي:

- **تبادل المعلومات:**

يبنى على تقديم البيانات، الوثائق الاستدلالية، السوابق القضائية المتعلقة بالجناة ذلك في إطار ما تطلبه السلطة القضائية الأجنبية حين الاطلاع على الاتهامات المنسوبة إلى الرعايا الإجرامية في الخارج مع الإجراءات المتخذة بشأنهم، طالما لم تكن الجهة المختصة في رقابتهم بل تتفاعل بين الدولة المساعدة لإقامة محاكمتهم وفق تشريعاتها الداخلية في حدود المساعدة القضائية، أما بالنسبة للسوابق القضائية يقتضي البحث عن الماضي الجنائي لدى المتهم المحال الذي يساعد في تقرير الأحكام المرتبطة على حالات العود، وقف تنفيذ العقوبة بينما تدويل الصحيفة الجنائية مازال يتم إعدادها لرعايا الدول

المبرمة باتفاقية تبادل المعلومات حيث وردت العديد من التشريعات الوطنية الدولية في تطبيقها على قوانينها الداخلية ما يلي: (93)

ـ أقرَّ التشريع الجزائري استنادًا إلى المادة 17 من القانون 09ـ04 لاستجابة طلبات المساعدة القضائية الدولية الرامية في تبادل المعلومات تحت إطار الاتفاقيات الدولية المتعاقدة احترامًا لمبدأ المعاملة الإنسانية.

ـ تؤكد المادة الأولى من معاهدة الأمم المتحدة النموذجية على تبادل المساعدة القضائية في المسائل الجنائية لاسيَّما طلبات المتعلقة بالسوابق القضائية الواردة في البندين (و، ز) من الفقرة الثانية، كذا البند الثالث، الرابع، الخامس من المادة الثامنة لاتفاقية الأمم المتحدة في مكافحة الجريمة المنظمة العابرة للوطنية المستوجبة على الدول تيسير تبادل المعلومات المتعلقة بالنشاط الإجرامي.

ـ وردت المادة الأولى من اتفاقية الرياض للتعاون القضائي العربي بشأن إلزامية تبادل المعلومات بين دول الأعضاء مع التنسيق بين الأنظمة القضائية، بينما صاغ اتفاق شنجن للاتحاد الأوروبي نظام متكامل على فاعلية تبادل المعلومات، أما بالنسبة لمعاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي قد أشارت إليها في البند الأول من المادة الرابعة، إذ قررت الاتفاقية الأوروبية بشأن الجريمة الافتراضية استنادًا إلى المادة 23 الواردة صراحة على إلزامية التعاون الدولي بين دول الأعضاء لأجل التقليل من العوائق الصادة، مما يوفر المرونة في تبادل المعلومات على التنظيم القضائي الدولي.(94)

➢ 2. تسليم المجرمين:

(30) ـ محمد أحمد سليمان عيسى، "التعاون الدولي لمواجهة الجريمة الإلكترونية"، **"المجلة الاكاديمية للبحث القانوني"**، المجلد 14، العدد 2، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميره، بجاية، الجزائر، 2016، ص60.

(31) ـ عادل عبد العال إبراهيم خراشي، إشكالية التعاون الدولي في مكافحة الجرائم الالكترونية وسبل التغلب عليها، دار الجامعة الجديدة، الاسكندرية، 2015، ص235.
ـ للإشارة على أمثلة نموذجية حية بشأن تبادل المعلومات في ميدان التعاون القضائي الدولي المبينة فيما يلي:
تم تقديم الطلب من السلطات الأسترالية إلى وزارة العدل الرومانية عن طريق رسالة إلكترونية يبلغ فيها ارتكاب جريمة السرقة المعلوماتية مع استنساخ البيانات دون تصريح قانوني من قبل جماعة إجرامية رومانية استهدفت ضحايا استراليين، مما ورد في الطلب المقدم تحديد هوية أصحاب البطاقات المستنسخة، العثور على النسخ الالكترونية من الوثائق المستنسخة مع الانتظار بالرد على الطلبية في وقت قياسي، بينما تم إجراء مشاورات مع مكتب النائب العام الملحق بمحكمة النقض العليا من شأنها أرسلت وزارة العدل الرومانية تلك المعلومات، إذ قدمت إيضاحات إضافية بشأن عناصر التحقيق منها حضور الشهود، الخبراء التقنيين من دول الأعضاء ذات دور على المساعدة القضائية في المجال الجنائي الذي يشترط الحضور بمحض اختياره أمام الهيئات القضائية في الدولة المطلوبة استدعاءه طالما يتمتع بالحصانة القانونية ضد أية إجراءات جنائية متخذة بحقه.
متاح على الموقع الإلكتروني الموالي: https://www.unodc.org

عبارة عن تدبير قضائي دولي قد يرمى لإحالة المتهم محلًا للملاحقة الجنائية من نطاق السيادة القضائية لدولة إلى إقليم الدولة الذي تم الفرار إليها في إطار تنفيذ محاكمته أمام العدالة الجنائية، حيث جاءت المعاهدة إثر عولمة تكنولوجيا المعلومات مع شبكات الاتصالات التي تقتصر على اعداد أنشطة إجرامية ناعمة في فضاء افتراضي متاح على الساحة الدولية، مما يخالف لأنظمة التشريعية القانونية على الدول بشأن اختلال الكيان الأمني الداخلي ضد تفاقم الاعتداءات المعترضة أمام عقبة المكافحة الدولية، ذلك ما جدى أغلبية التشريعات الوطنية إلى عقد اتفاقيات تعاونية لأجل إيجاد حلول ناجعة تساهم القضاء على احتمالية معدلات الجريمة، إذ نلتمس هناك تعذر على طبيعة التسليم في ظل الأحكام الوطنية بمثابة عملًا سياديًا قضائيًا بل تفادت تلك النظم على غرار الاتفاقية قد تسري تبعًا لمبادئ العامة المتعلقة بإجراءات التسليم، بينما التشريعات الوطنية تتفاوت حسب خصوصية التنظيم القضائي، بالرغم يستمد التسليم أساسه القانوني تبعًا للمبادئ العامة الواردة في التشريعات الجزائية الداخلية حتى على الاتفاقيات الثنائية التي تنظم القواعد المطبقة بين الأعضاء المتعاقدة بشأن تبادل تسليم المجرمين سواء أكانوا في طور الملاحقة أم المحكوم عليهم ثم يفرض على الأعضاء تنفيذ الاتفاقية المنتجة لآثارها القانونية بعدما يتم التصديق عليها وفقًا للأوضاع الدستورية المقررة ذات سيادة على القانون لاسيَّما الدولة الجزائرية قد تسري الموافقة من قبل رئاسة الجمهورية، بالمقابل شاركت في مؤتمرات دولية قد تدعو لإبرام معاهدات عالمية على قضية تسليم المجرمين منها المؤتمر الأول للشرطة القضائية في موناكو عام 1924، المؤتمر الدولي للعقاب في لندن عام 1945.[95]

ثالثا: العقبات الموجهة على التعاون الدولي

يرتقي التعاون الدولي على دور حقيقي فعال في سبيل المكافحة المعلوماتية إلا قد يعترض العديد من التحديات سواء على الصعيد الوطني الدولي، مما ينادي بإرساء حلول وقائية مجسدة قد تسعى نحو التغلب على العقبات التي تقف عائقًا أمام السيادة الإقليمية للدول من حيث تعذر الاثبات لجرائم المعلوماتية عدم ملائمة التشريعات الجنائية الداخلية، تنوع النظم الإجرائية، تنازع الاختصاص القضائي، إشكالات المتعلقة بالإجراءات الجنائية الدولية لاسيَّما الانابة القضائية، تسليم المجرمين، تعارض المصالح على القانون الواجب التطبيق، حيث انقلب التعاون الدولي في الميدان الجزائي عقبة من تعاون تشريعي

(34) ـ كريمة تدريست، "معوقات نظام تسليم المجرمين كآلية للتعاون القضائي الدولي لمكافحة الجريمة المنظمة عبر الوطنية"، **"المجلة النقدية للقانون والعلوم السياسية"**، المجلد 11، العدد 2، كلية الحقوق والعلوم السياسية، جامعة مولود معمري،
تيزي وزو، الجزائر،2016، 48.

يهتم بتجريم الأفعال الماسة على النظام العام داخل إقليم الدولة إلى تعاون أمني مشترك بين المنظمات الدولية الهادفة في تبادل المعلومات، تحديد هوية المجرمين بشأن تسليمهم ثم يمتد نحو تعاون قضائي لاسيَّما الإنابة القضائية، نقل الإجراءات الجزائية، المساعدة القضائية، الاعتراف بتنفيذ الأحكام الجزائية الأجنبية، تسليم المجرمين، بطبيعة الحال يكتسب التعاون الدولي أهمية جديرة في تكثيف المكافحة لاسيَّما الجرائم التقنية التي تستلزم اتخاذ الإجراءات في الوقت الملائم دون إضاعة الأدلة الرقمية المعتمدة في التحقيقات القضائية.

بذلك يتم عقد المعاهدات الدولية ذات دعامة على التعاون الدولي لاسيَّما معاهدة بودابست لمكافحة جرائم المعلوماتية، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لأجل القضاء على التحديات التعاون الدولي قامت شتى الدول باستحداث تشريعاتها الخاصة بما يخفف عملية المكافحة منها القانون المتعلق بحماية البيانات الشخصية، التوقيع الالكتروني، التجارة الالكترونية على إثر ذلك ورد المشرع الجزائري في الفصل السادس من القانون رقم 09ـ04 على التعاون والمساعدة القضائية الدولية من خلالها تسنى القيام بالإجراءات القانونية المتخذة على التبادل الدولي لمكافحة الجرائم المعلوماتية وفقًا للأطر المبنية قانونًا، لقد ألقت الاتفاقية العربية على عاتق الدول الأعضاء بالتكفل لوضع جهاز متفرغ على مدار الساعة بشأن توفير المساعدة الفورية لغاية إجراءات التحقيق دون توقف الدول لاقتراح حلول راسخة على التعاون الدولي مثلًا تدريب رجال العدالة مرآة عاكسة على التعاون القضائي لإفادتهم بالبرامج التكوينية التي تحسن الكفاءة العلمية الفنية لاسيَّما البرنامج الدولي للتدريب على التحقيق الجنائي(ICITAP) قد تم عقد اجتماع حول مكافحة الجريمة السيبرانية خلال يومي 17-18 فيفري 2020 في إطار البرنامج الأوروبي الذي شارك فيها 9 قضاة في المجال الجزائي التقني مع خبراء المجلس الأوروبي سعيًا إلى تقديم الدعم في مجال التكوين القاعدي، أما بالنسبة لآلية تسليم المجرمين ذات غاية الأهمية في قمع الجريمة قد تطرق إليها المشرع الجزائري بمقتضى المادة 50 من التعديل الدستوري لسنة2020 دعمًا للعلاقة المبرمة في ميدان التعاون القانوني القضائي الرامية إلى المكافحة، كذلك سعت الاتفاقيات الدولية لإيجاد حلًا على قواعد الاختصاص في الجريمة المعلوماتية باتت بغير الكفاية للأساليب التقليدية المعتمدة على عملية المكافحة الذي عالجه المشرع في المادة 15 من القانون 09 -04 ضف إلى قواعد الاختصاص الواردة في قانون الإجراءات الجزائية، الاتفاقية العربية المجسدة بمقتضى المرسوم الرئاسي رقم 14- 252 تم بالذات في المادة 30 من الاتفاقية.

علاوة على تلك الاقتراحات السائدة في تفاعلية التعاون الدولي مازالت هناك مسألة بشأن الدعوة إلى تنظيم محكمة جنائية دولية لمكافحة الجرائم التقنية إعمالًا لسد الفجوة القانونية من خلالها تم استحداث التقاضي الالكتروني لأجل سير الإجراءات القضائية معتمدًا شبكة الإنترنت بل نأمل من إنشاء محكمة رقمية للفصل في القضايا التقنية الدولية التي تسعى إلى إرساء دعائم المتعلقة بالمنازعات المتقاضين ذلك تحت رعاية الأمم المتحدة، فلابد من عقد دورات تدريبية على القضاة، رجال القانون، المحققين الجنائيين بالتنسيق مع فريق الخبراء الامريكية حتى يتم الالتحاق بالركب التقنية المعلوماتية إلا أنَّ التشريع الجزائري قد ساهم في هذا الإطار إلى تطبيق المحادثة المرئية عن بعد، أما بالنسبة لأداة الإثبات الجنائي التقني لاسيَّما الشهادة عبر مؤتمر الفيديو قد تجيز لظروف استثنائية لدى الشاهد.[96]

رغم التحديات المعترضة على التعاون الدولي إلا هناك آليات يتعين على التشريعات الوطنية الدولية للاعتماد عليها حتى نتفادى العواقب أمام عملية المكافحة ذلك من خلال اتخاذ جملة من التدابير الموضوعية الاجرائية على الصعيد الداخلي، أما على الصعيد الدولي يقتضي التغلب على تحدي القصور التشريعي دون تعارض المصالح، تنازع الاختصاص، بطئ الإجراءات، ميدان التدريب القضائي إلى جانب آليات المتعلقة على تزاحم طلبات تسليم المجرمين، في سياق الدراسة سنبين العقبات الموجهة ثم الآليات المتخذة على التعاون الدولي فيما يلي:

➢ 1. تحديات التعاون الدولي في مكافحة الجريمة المعلوماتية:

تتجلى المعيقات التي تصطدم بآلية التعاون الدولي في مكافحة الجرائم التقنية على الصعيدين الوطني الدولي بما في ذلك تنوع النظم الإجرائية، القصور التشريعي الوطني، تنازع الاختصاص القضائي إلى جانب إجراءات المتعلقة بالإنابة القضائية، تزاحم طلبات تسليم المجرمين، ذلك ما يعترض على أسبقية التعاون الدولي في الميدان الجنائي مادام أمامنا جرائم ترتكب عبر الفضاء الرقمي قد يتعذر الالتحاق بالركب المعلوماتية على سهولة نظرًا إلى معالم الجريمة ذات طبيعة مرنة معقدة عابرة لم يتسنى حتمًا التعامل مع الواقع الافتراضي، مما يقتضي اللجوء إلى حصر تلك العقبات ضمانًا لمبدئية السيادة الدولية التي تعهد اتفاقيات هادفة على التغلب لاحترافية الأنشطة الإجرامية بل عمدت إلى

(38) - لرقط عزيزة، " التعاون الدولي في مكافحة الجرائم المعلوماتية (إشكالاته، آليات التغلب عليها)"، **"مجلة التواصل"**، المجلد 25، العدد 4، كلية العلوم الإنسانية والاجتماعية، جامعة باجي مختار، عنابة، الجزائر، 2019، ص 16.

إرساء حلول ناجعة لإنجاح فاعلية التعاون الدولي ضد الديناميكية الرقمية، حيث سنفصل دراسة تلك التحديات وفق النقاط الآتية:[97]

- **قصور التشريعات الجنائية الداخلية:**

رغم التنافسية السائدة على التكنولوجيا الرقمية المستأثرة في سائر الأعمال الميدانية لاسيَّما على مجرمي المعلوماتية الذين يبتغون لأداء أنشطة تخريبية معتمدًا على التقنيات الآلية المساعدة على استفحال الإجرام من شأنها أدت لاستحالة النصوص القانونية الداخلية على التصدي فضاء المعلوماتية طالما يتطلب محل الارتكاب طبيعة مادية ما يتنافى مع الجريمة التقنية التي تخرج عن المبادئ العامة للتجريم والعقاب، ضف إلى التقليل من جهود الأجهزة الأمنية عند ضبط فاعليها بإحالتهم إلى القضاء التي من شأنها يتم استكمال إجراءات الدعوى الجنائية، إذ لم يسمح على التشريعات الوطنية من مبادرة التحدي ضد عولمة الجريمة حتى لو تم إصدار تعديلات جديدة قد تجرم الأفعال الماسة بالأنظمة المعلوماتية لاسيَّما التشريع الجزائري الذي سارع إلى تعديل قانون الإجراءات الجزائية، قانون العقوبات ثم قام باستحداث قوانين مستقلة تماشيًا بالركب التقني في إطار المكافحة التشريعية الداخلية، ضف إلى الانضمام لاتفاقيات الدولية لعلها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المساعدات القضائية الدولية بشأن تسليم المجرمين بل تظل تلك الجهود المأمولة في عرقلة التصدي لمعالجة الجرائم التقنية أمام التشريع الداخلي.

- **تعذر الإثبات الجنائي على الجرائم المعلوماتية:**

تتسم الطبيعة التقنية بالخفاء طالما هناك الذبذبات الإلكترونية مشفرة غير مرئية ملموسة، مما يتعذر البحث عن الأدلة الرقمية بواسطته يبنى الإثبات، حيث يتم التلاعب على البيانات لإعاقة الوصول إلى آثار الجريمة التي يلجأ الجاني في تشفير تعليمات الحاسب الآلي من شأنه يؤدي إلى طمس الدليل تلقائيًا أم إخفاءه في المستودع السري لدى

(39) ـ محمد الفاضل، **"إشكالات** التعاون الدولي"، "**مجلة المحاماة المصرية"** بتاريخ 26 أفريل 2020 على 13 سا و57 د في الموقع الالكتروني التالي https://www.elmetr.com تم الاطلاع عليه يوم 26 أوت 2023 على 12سا 33د.

النظام المعلوماتي الذي بات عائقًا أمام المحقق الجنائي عند الخوض في عملية التحري لأجل الكشف عن حذافير الجريمة بل ينبغي الدراية الفنية على كيفية استخدامات الشبكة الرقمية حتى يتسنى معرفة التقاط الدليل من مسرح الجريمة نظرًا لاحترافية مجرمي المعلوماتية في التحكم بالأمن البرمجية، بينما يعمدون إلى حجب هويتهم معتمدًا حسابات مستعارة وهمية يتم الدخول إليها عبر مقاهي الإنترنت قد يكلف على المحقق وقت مستغرق في تتبع النشاط الإجرامي بغية ضبط قناع الشبكة المعلوماتية.(98)

- **إشكالية الإنابة القضائية:**

التلاحم على السيادة القانونية يصطدم أمام التعاون الدولي إزاء التذرع بالمصلحة القومية، مما يغتنم مجرمي المعلوماتية على فرص مغرية نحو الفرار من العدالة الذي يقتضي التخلي عن السيادة المطلقة بشأن نجاعة المكافحة دون تقييد من ممارسة الاختصاص لاسيَّما الملاحقة القضائية، التحقيقات الجنائية، المحاكمة، تنفيذ العقاب بناءً على إجراءات الإنابة القضائية المتخذة بواسطة سلطاتها القضائية بدل الدولة المنعقد لها الاختصاص، حيث يحرص على احترام السيادة الدولية في الإقليم الوطني بمقتضى إجراء الانابة القضائية التي تقرر بإتباع الشروط الآتية:

ـ تخضع الإنابة القضائية بناءً على الطلب المقدم من صاحبة الاختصاص الجنائي استنادًا للأسلوب المحدد في الاتفاقية السارية بين الدولة المطلوبة.

ـ فحص الطلب بشأن التأكد من استيفاء موجبات الانابة القضائية تبعًا للاتفاقية المبرمة في ذاك الإطار.

ـ تنفيذ الإنابة القضائية طبقًا لأحكام القانون الدولة المطلوبة على سبيل المثال يتم إرسال إنابة قضائية خارج الإقليم من قاض جزائري إلى قاض أجنبي يسري تنفيذ الإنابة بناءً على المبادئ السارية في قانون دولة القاضي الأجنبي فلا تعني من إنقاص السيادة بل الاشتراك على التعاون، إذ لجأت الدول لإبرام اتفاقيات ثنائية متعددة وفق المساعدة القضائية إلا قد تعرقل مسألة التعاون الدولي في ضوء المكافحة المعلوماتية.(99)

(40) ـ عمرو زكي عبد المتعال، المعاهدة الدولية لمقاومة جرائم الحاسبات، ورقة عمل مقدمة إلى مؤتمر الجوانب القانونية للتجارة الالكترونية، مقر الجامعة العربية، القاهرة، 2001، ص60.

(42) ـ نعيمة بن يحيي،" الإنابة القضائية الدولية كآلية للتعاون الدولي في مجال مكافحة الجرائم"، **"مجلة الدراسات الحقوقية"**، المجلد 4، العدد 1، كلية الحقوق والعلوم السياسية، جامعة الدكتور مولاي الطاهر، سعيدة، الجزائر، 2017، ص30.

➢ 2. سبل التغلب على عقبات التعاون الدولي:

لقد أسفرت المعلوماتية على تخلف المنظومة الجنائية التشريعية ذلك ما يستلزم إنشاد فعالية التعاون الدولي من خلال إقرار المبادئ الاتفاقية في تجسيدها بالآليات الإجرائية نحو الالتحاق بالركب فضاء الرقمنة التي ترمى إلى التصدي التشريعات الوطنية ضد القناع الإجرامي التقني، مما سعى الفقه الجنائي الدولي بالتذليل من العقبات التي تحول دون تكامل التعاون الدولي فيما يتعلق اختلاف النظم القانونية العقابية الاجرائية قد تجتهد المنظمات الدولية إلى تحديث قوانين محلية تماشيًا مع تطور الجرائم بغية سد الفجوة القانونية التي تعاقب آلية المكافحة، ضف إلى إبرام المعاهدات الثنائية لاسيَّما الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة عليها الجزائر، أما بالنسبة لترسانة الصكوك الدولية الصادرة عن الأمم المتحدة قد تشجع دول الأعضاء على السماح باستخدام تقنيات التحقيق الذي يخفف من تطرف النظم القانونية بل يفتح الباب أمام التعاون الدولي الفعال، حيث أكدت الاتفاقية الأوروبية للإجرام المعلوماتي استنادًا إلى المواد 33،30،29 من الاتفاقية على سرية حفظ البيانات المعلوماتية المخزنة للاعتداد عليها في التحقيقات القضائية حتى يتسنى تجميع الأدلة التي يتعذر الوصول إليها مالم تساهم على ود التعاون الدولي الذي يخفف من غلو العقبات الصادة لعملية المكافحة، إذ باتت الحاجة الملحة لإسناد التعاون على عاتق التشريعات العقابية الوطنية الهادفة إلى الموازنة بين متطلبات تصدي الجرائم المعلوماتية مع إلزامية حماية السيادة الوطنية و خصوصية الأفراد، بذلك يقتضي الإشارة للآليات المتخذة على عقبات التعاون الدولي المبينة في النقاط الآتية:[100]

- **التدابير الموضوعية:**

يتوجب على الهيئات الدولية تتبع سياسة تشريعية هادفة إلى التعاون الفعال لأجل الحماية الناجعة من تداعيات الجرائم التقنية التي تتطلب تبني بما يتلاءم الطبيعة المعلوماتية حتى يتسنى التغلب على مخاطر استخدام الإنترنت الدافعة لارتكاب الأعمال التخريبية من خلال التسلل على الأدلة المتعلقة بالجريمة معتمدًا شبكات الاتصال الدولي بل يتعين على الدولة تقرير التدابير التشريعية اللازمة في الكشف عن عمليات الدخول

(45) ـ أحمد بورازم، أساليب التعاون الدولي في القضاء على الجرائم الالكترونية، ورقة بحث مقدمة إلى أعمال الندوة الوطنية، كلية الحقوق والعلوم السياسية، جامعة حمه لخضر، الوادي، الجزائر، منشور على الموقع الالكتروني www.courdebatna.majustice.dz بتاريخ 15 جوان 2022، تم الاطلاع عليه يوم 26 أوت 2023 عل سا19 و55د.

للأنظمة المعلوماتية تبعًا لما تقضيه قوانينه الداخلية حتى لو حققت حماية نسبية بغية في درء الهاجس التقني إلى جانب ادراك للاستيلاء غير القانوني باعتباره جريمة جنائية طبقًا للأحكام الصادرة في القانون الوطني، فلابد من اشتمال أفعال الاعتداء (الاتلاف، المحو، الإعاقة، التعديل) على البيانات المخزنة في النظام الآلي قد يقتضي على التشريع الداخلي اتخاذ قواعد متعلق بالعقاب لتلك الأفعال الإجرامية مع اتاحة المساءلة الجنائية على الأشخاص المعنوية في إطار الوظيفة، أما بالنسبة لصلاحية تطبيق القواعد التقليدية على الجرائم المعلوماتية عاجزة تمامًا نظرًا لما تتطلب من طبيعة مادية قد تتنافى الجريمة التقنية إذ لو هناك مآل في ملائمة النصوص التقليدية على الطبيعة التقنية ما استدعى التشريعات إلى معالجة قوانينها من خلال إثراء تعديلات جديدة على المنظومة الجنائية مع الإحاطة لكافة الأنماط الإجرامية دون تناقض لمبدأ الشرعية الجنائية حتى على القاضي مقيد في تنفيذ القانون، رغم ذلك يجدى تعديل القواعد الموضوعية لتصبح صريحة على تجريم الاعتداءات الماسة بالمنظومة المعلوماتية بدلًا من النصوص التقليدية دون تلاشي يد القانون على عقبة المعلوماتية.[101]

- **التدابير الإجرائية:**

البعد الإجرائي الفني لجرائم الإنترنت ينطوي من إشكاليات المنفردة على التعاون الدولي ذات أهمية خالدة التي قطعت أنفالًا صادة على المكافحة المعلوماتية قد يجدر التفكير لاتخاذ التدابير التشريعية الملائمة في التغلب على تلك الأصداف أمام الميدان لاسيَّما إنعدام قنوات الاتصال بين السلطات الأمنية الدولية بغية تبادل المعلومات عنصرًا حاسمًا في إجراء التحقيقات الجنائية، فلابد من ربط شبكات الاتصال تؤمن بين الهيئات الدولية حتى يتسنى تعقب جرائم الحاسبات الآلية، حيث أشارت إليها الترسانة القانونية الدولية لعلها اتفاقية الأمم المتحدة الاتفاقية الأوروبية لمكافحة الاجرام المعلوماتي الواردة في المواد 35/27 من الاتفاقية، أما بالنسبة للمساعدات القضائية قد أوصت مؤتمرات الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية على فعالية تعزيز السلطات المركزية المعنية للارتقاء بالمساعدة القانونية بغية تنفيذ الطلبات القضائية إلى جانب عقبات التعاون الدولي في مجال التدريب القضائي يستدعي التوعية بين الهيئات القضائية الدولية على اكتساب الكفاءات المستهدفة في مجال المعلوماتية لاسيَّما إيجاد برامج تكوينية تطبيقية تنسيقية تتناسب لكافة المستهدفين، القيام بعمليات صقل المهارة التقنية بين الخبراء لأجل تقريب الرؤى على القائمين، الحرص على دعم إجراءات التحقيق الجنائي (المعاينات الفنية،

(46) ـ منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الأنترنت والحاسب الآلي، دار الفكر الجامعي، الإسكندرية، 2014، ص137.

تفتيش النظم المعلوماتية، فحص البيانات المخزنة)، صلاحية الدولة على تخويل سلطاتها القضائية في ملاحقة مجرمي المعلوماتية، إضفاء صفة الضبطية القضائية على العاملين في ميدان المعلوماتية لاسيَّما مزودي الخدمات ذات دور تقني يساعد على تأمين الفضاء السيبراني لحماية الأمن المعلوماتي مع المراقبة للاتصالات الالكترونية، التحفظ على الأدلة إلى حين حضور رجال الضبط القضائي مبادرة الهيئات الدولية في الحصول على النسخ البيانات ذات الحفظ السريع.[102]

الفرع الثالث
مكافحة الجمعيات على الجريمة التقنية

الملامح الإجرامية مرآة عاكسة على الطابع الأمني الاجتماعي نظرًا لتفاقم معدلاتها الماسة بالكيان العام بينما تلحق آثارًا حاثة تطال لانتهاك الحق في المعلومات حتى سادت على منافذ التهديد بكافة المنظمات الدولية الهادفة لحماية الأمن المعلوماتي من مخاطر البيئة الرقمية مهما تواصلت من بوادر مأمولة على المكافحة إلا أنَّ دائرة الآليات التشريعية الاجرائية أو المؤسساتية العملية لن تكمل الدور الوقائي حتى تتلقى التدابير العائدة إلى تعزيز أساليب المكافحة لاسيَّما الاستعانة بما تؤديه الجمعيات الأهلية في عملية تنشيط التوعية القانونية ضد السلاح التقني، بينما يستفاد من معالجة الإدمان الافتراضي التي تنادي القراصنة إلى الإغراء في عالم الإجرام، حيث باتت على كيد الإعاقة في المعاملات الالكترونية بين سائر الأمم، مما حرصت جمعيات الوقاية على تنمية الحس الأمني لدى المواطنين من عواقب الإنترنت، التفاعل مع رجال الشرطة حال التحقيق عن لغز الجريمة، استطاعة الإبلاغ حال العلم بوقوع الجريمة، التعاون بين الهيئات القضائية فيما يتعلق الإدلاء بالشهادة الاشتراك في البرامج الاجتماعية الثقافية بغية إعادة اصلاح الجناة نحو الادماج في البيئة المجتمعية، إذ تلعب دورًا حاسمًا في التوعية الارشادية على الأطفال ضد الأضرار الناجمة عن الوسائط الالكترونية بالذات مواقع التواصل الاجتماعي بل يقتضي تنظيم الأنشطة التوعوية بغرض تحصين الشباب ضد الآفة الخبيثة من خلال

(47) ـ حسين الغفاري، الجهود الدولية في مواجهة جرائم الأنترنت، دار النهضة العربية، القاهرة، 2015، ص14، متاح على الموقع الالكتروني www.cip.org.sa/vb/sharthread.plp3697

ـ الإشارة إلى نماذج تطبيقية عن آفاق التكوينية بين الهيئات القضائية الدولية المبينة ما يلي:

تجسيدًا على التعاون القضائي قد تم تنظيم ست دورات تكوينية لصالح 150 قاض جزائري من تنشيط القضاة الأمريكيين في مجال المصنفات الرقمية، أما بالنسبة لفرنسا قد استفاد قطاع العدالة بـ 12 منحة، حيث انطلق التكوين خلال شهر سبتمبر 2005 في المدرسة العليا للقضاء بينما يدوم الفوج الأول 10 أيام Bordeaux ثم يتبعه الفوج الثاني خلال اللاحقة تكوين Dijon من عشر قضاة متاح على الموقع الالكتروني الخاص بوزارة العدل الجزائرية
https://ww Power Off w.majustice.dz/tableaux-dgrh-ar/tableau3.pdf

التوجيه إلى منحى الأمة الفاعلة، فلا ننسى إحياء الحقبة التقنية التي تفرض القائمين على التأقلم لانتهاج سبل كفيلة في محاربة الجرائم الناتجة عن الفضاء الالكتروني مادام المجتمع وسيط بين مسؤولية علاج المجرمين من الانحراف حال ما إذا جسَّدت تلك الأولوية على الجمعيات ضد الوقاية من معدلات الإجرام.(103)

فلا تكفي السياسة الردعية على المشرع الجنائي لصد الجريمة المعلوماتية بينما اعتدت الهيئات الدولية إلى رسم سياسة وقائية تحت تسمية **الثقة الرقمية**، إذ لجأت إلى سن قوانين مستندة على محفزات تقنية بغية تشجيع أنشطة الجمعية، إشراك القطاع المدني التطوعي في التصدي العقبات الطارئة على الأمن القومي قد باتت عاملًا حاسمًا لفعالية النجاح من خلال تنمية الوعي الاجتماعي بغية فض السلبيات على دوام الإيجابيات، حيث نسلط الدور لتلك الجمعيات في سبيل الاستدلال المبينة ما يلي:

ـ عقد البروتوكول التعاوني مع المؤسسات التعليمية بغية تثقيف الوعي الفكري بين الطلبة التدريب التأهيلي على السادة القضاة، أعضاء النيابة العامة، الأساتذة المحاميين، العاملين في القطاعات القانونية بغية اكتساب الكفاءات العلمية الفنية المعتمدة على الصعيد الوطني الدولي حتى يتسنى مناقشة الإشكاليات المتلقة في فضاء المعاملات الالكترونية.

ـ إعداد الأبحاث الدراسية حول العلاقة الرقمية بالقاعدة الموضوعية الإجرائية في القانون الجنائي ثم الحث على التطوير للأجهزة الوقائية في مجال المكافحة.

(48) ـ أمال عزري، جمال بن زروق، "استخدام جمعيات المجتمع المدني في الجزائر للشبكات الاجتماعية الالكترونية"، (دراسة ميدانية على جمعيات المجتمع المدني في ولاية سكيكدة)، **"مجلة آفاق للعلوم"**، المجلد 2، العدد 7، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، 2017، 235.

ـ الإشارة إلى نماذج ميدانية عن جمعيات مكافحة الجريمة الالكترونية في التشريعات العربية المبينة فيما يلي:

انشاء الجمعية التونسية في مقاومة الجريمة الالكترونية، الجمعية التونسية للإنترنت، بينما بدأ الاهتمام بمكافحة الجريمة الالكترونية على الجمعية المصرية بعد انعقاد المؤتمر التأسيسي الأول لجمعيات قانون الانترنت بالقاهرة خلال شهر سبتمبر 2004، المؤتمر الدولي لقانون الإنترنت بالغردقة خلال شهر أوت 2005 حينئذ تم تأسيس الجمعية العربية لقانون الإنترنت، بالمقابل هناك الجمعية الأردنية المتخصصة في الجرائم الالكترونية الهادفة إلى إنتاج التوعية الفكرية للحد من جرائم الحاسب الآلي، أما الجزائر قد استحدث بما يقارب 108940 جمعية ناشطة في شتى الميادين إلا مجال القانون الجنائي المتعلق بمكافحة المعلوماتية دون الجدوى على إنشاء برامج التوعية على الجمعية بلا غاية ناجحة مستقبلًا، هنالك الجمعية الدولية لمكافحة الجريمة الالكترونية بفرنسا(Association internationale de Lutte Contre la Cybercriminalité) المستهدفة إلى تقليص حجم ارتكاب الجرائم المعلوماتية عبر الانترنت.

انظر/ المنظمة العربية للتنمية الإدارية، جامعة الدول العربي، المؤتمر الدولي الأول لقانون الإنترنت (CYBERLAW) " نحو علاقات قانونية إدارية اقتصادية سياسية اجتماعية جديدة"، المنعقدة يومي 21ـ25 أوت 2005، الغردقة، جمهورية مصر العربية.

ـ الموقع الرسمي لوزارة الداخلية والجماعات المحلية http://www.interieur.gov.dz/images/pdf/listeassossaciation-ar.pdf بتاريخ 2020/04/25.

ـ تنظيم الورشات العملية، الملتقيات بالتنسيق مع الهيئات الوطنية الدولية بغية تبادل الرؤية الفكرية في انتقاء حلول سليمة تتوافق الجسامة الاجرامية مع الإفادة على الخبرة المستنقعة من ذوي الاختصاص.

ـ اعتداد الشركات التقنية على التعاون الوقائي في حذف المحتوى المتطرف من خلال حجب المواقع الالكترونية بواسطة آلية الذكاء الاصطناعي بغية القضاء على الإرهاب المعلوماتي بينما تمت بإزالة حوالي 377.000 حساب من شهر جويلية إلى ديسمبر عام 2016. [104]

(49) ـ عبد الله دغش العجمي، المشكلات العلمية القانونية للجرائم الالكترونية، (دراسة مقارنة)، مذكرة لاستكمال الحصول على درجة الماجستير في القانون العام، جامعة الشرق الأوسط، الأردن، 2014، ص 104.
ـ طرحت قضية جنحية مسجلة لدى المحكمة الابتدائية في القضاء المغربي تحت رقم 04/385 الصادر في 02/18/ 2005 التي تتلخص الوقائع فيما يلي:
أُدين أحد التقنيين على جنحة الدخول إلى نظام المعالجة الآلية إثر التعطيل عن التشغيل، بينما أحدث موقع الكتروني خاص لاتصاله بمقاهي الانترنت من خلالها بدا يراسل أشخاص ذاتية معنوية عبر الشبكة، حيث تسلم على إثر ذلك بريد الكتروني حقق له منفعة مالية دون حق قانوني مما أُلحق ضرر لإحدى الشركات الامريكية.
انظر/ صليحة حاجي، "الآليات القانونية لتكريس الأمن المعلوماتي"، **"مجلة العلوم الجنائية"**، العدد الثاني، المطبعة الأمنية الرشاد، المغرب، 2015، ص10.

المطلب الثاني
الجهود التشريعية الدولية في مواجهة الجريمة المعلوماتية

بادر التشريع الدولي في تكثيف جهود ناجعة من خلال إعداد استراتيجية قانونية هادفة إلى مجاراة للاعتداءات الواقعة على النظم المعلوماتية إلى إرساء بلورة قانونية كفيلة للمواجهة اسهاما على المواجهة يتطلب وعي دولي بأهمية الخطورة مما ساير المشرع الجزائري اسهامات المجتمع الدولي من خلال وضع استراتيجية متكاملة تتجلى في التعديلات التي أدخلها على منظومته القانونية ذلك بما يتلاءم الطبيعة المعلوماتية في مجال المكافحة، فلا مناص من البحث عن آليات تساعد على إيجاد تعاون دولي يتفق الطبيعة المعلوماتية، بينما يخفف الفوارق لأنظمة القانونية الأمنية الدولية من خلال تحديث التشريعات الوطنية المعنية بالجرائم الالكترونية مع عقد الاتفاقيات الثنائية، الصكوك الدولية الصادرة عن الأمم المتحدة

التعاون الدولي الآلية الفعالة على المكافحة الذي يقتضي التخفيف من غلو الفوارق بين الأنظمة العقابية الداخلية التي تقيد على المجرم المعلوماتي البحث عن فرص مغرية، لذا ابرمت العديد من الاتفاقيات الدولي في مجال التعاون الدولي بينما تبرز معالم التقارب لاسيَّما قبول حالات تفويض الاختصاص القضائي، اتخاذ إجراءات التحقيق الجنائي المتعلق في جمع الأدلة، الاعتراف بالأحكام الأجنبية، فلا ينال القانون الدولي من السيادة الإقليمية بل التعاون على فاعلية المكافحة بمثابة خطوة مسايرة على تدويل القانون الجنائي طالما هناك قواعد موضوعية إجرائية تهيمن التشريعات الوطنية ضد الحقبة، مما يعتبر من قبيل التدابير المانعة لارتكاب ذاك النوعية على غرار المجرم المعلوماتي سوف يجد نفسه محاطًا بسياج مانع من الإفلات في المسؤولية الجنائية من شأنه يكاد يعزف عن سلوك سبيل الجريمة.

المطلب الثالث
الحلول التشريعية المقترحة لمكافحة الجريمة المعلوماتية

أثبت الواقع العملي على إلزامية وضع الحلول القانونية لمواجهة التحديات التي تعرقل الجهود الدولية في مجال مكافحة المعلوماتية رغم تدارك التشريعات الجنائية تلك الثغرات الناجمة عن قصور القواعد الموضوعية الاجرائية من خلال إدراج نصوص التجريم والعقاب ذات الصلة بتكنولوجيا الاعلام والاتصال، فلا ينبغي التوقف حائلًا عند الحد بل حتمية الالتحاق بالركب التقني تبعًا لما ستهيئ البيئة الرقمية من العواقب قد تتعلق أساسًا بمدى استطاعة السلطات الأمنية القضائية على المسايرة معتمدًا سبل ناجعة لسد الفجوات التي مازالت غامضة لدى التشريعات العربية مقارنةً بالدول الأجنبية ذات دراية مُحكمة في ميدان تقنية المعلومات، مما يتسنى تنظيم المعاملات الالكترونية تحت المراقبة الدورية لكي يسمح بمعرفة نوعية الخدمات المقدمة مستعينًا على مقاهي الأنترنت المتحدة بين قنوات الاتصال الدولية تسهيلًا لإثبات أنماط الجرائم المعلوماتية التي تكفل على الحماية الجنائية للأنظمة المعلوماتية بمراعاة مبادئ الخصوصية الشخصية.

بينما يحتم على المشرع الجزائري مراجعة المنظومة القانونية لاستيعابه جوانب تشريعية تارة ثم يغفل على تنظيم تلك النصوص الجنائية في توازن قياسي بل يسمح في تعقب تلك الاعتداءات الماسة على النظم المعلوماتية التي تخلف آثار صادة بالمؤسسات التابعة لسيادة الدولة مادام أغلبية مجرمي المعلوماتية يسعون لارتكابها عن خفاء مستترة تمامًا دون القدرة على كشف معالم الجريمة بل يتعذر الوصول الى حقيقة الواقعة علةً في احترافية التسلل بمادة الجريمة ذات عامل جوهري على التنبؤ السلطات القانونية في البحث عن الطبيعة الإجرامية ذلك بناءً على الإجراءات التقنية المتبعة فلا ننسى استقطاب الخبراء التقنيين ذات دور فعال للإفصاح عن نقاب الجريمة من خلالها يتم ملاحقة محترفي الشبكات الآلية إيمانًا في الحماية الوقائية على ردع السلاح التقني.[105]

انطلاقًا على المعطيات المتداولة سوف نعرض لأهم التوصيات المقترحة في ميدان مكافحة المعلوماتية بين الاستراتيجية الوطنية **(الفرع الأول)** ثم نعرج للإشارة على الاستراتيجية الدولية **(الفرع الثاني)** بعد ذلك نبين التدابير الوقائية على مكافحة المعلوماتية **(الفرع الثالث).**

(51) ـ مخلد إبراهيم الزعبي، " فاعلية التشريعات القانونية في مكافحة الجرائم الالكترونية"، **" المجلة العربية للنشر العلمي"** المجلد 20، العدد 37، كلية الشرطة، قطر، 2021، ص 2669، متاح على الموقع الالكتروني التالي www.ajsp.net

الفرع الأول
الاستراتيجية الوطنية

بعدما أشارنا لمسألة تكثيف الجهود الدولية المنتهجة على المكافحة لاسيَّما التشريع الجزائري الذي يواكب المستجدات العلمية التقنية في المجال المعلوماتي بغية القضاء على التهديدات الرامية لإساءة النظم المعلوماتية الذي يعد القلب النابض في ميدان الأعمال، حيث عمَّد المشرع الجزائري على إدخال تعديلات مستحدثة بما يتوافق الطبيعة المعلوماتية ذلك من الناحية الموضوعية المتعلق بالشق التجريم والعقاب لكافة صور المساس بأنظمة المعالجة الآلية للمعطيات استنادًا إلى القانون رقم 06 ـ 23 المعدل لقانون العقوبات.

أما من الناحية الإجرائية بمقتضى القانون رقم 06ـ 22 قد تتعلق أساسًا على قواعد التفتيش داخل البيئة الرقمية، مشروعية الأدلة، الإثبات الجنائي التقني للإفادة أمام الجهات القضائية، الخبرة الفنية المساعدة على سير التحقيقات الجنائية لدى الأجهزة الأمنية، أساليب التحري الخاصة المرتبطة بعملية الحفظ و الإفشاء العاجلان للمعطيات الالكترونية، حجز المعطيات المعلوماتية، مراقبة الاتصالات الالكترونية تبعًا لأحكام القانون رقم 09ـ04 المستهدفة إلى بناء الأطر القانونية التي تتلاءم خصوصية الجريمة المعلوماتية بينما جاء القانون رقم 09ـ04 جامعًا بين القواعد الإجرائية المكملة لقانون رقم 06ـ 22 مع القواعد الوقائية التي تسمح برصد الاعتداءات المحتملة، حينئذ تسارع المشرع إلى حصر تلك الانتهاكات لأجل تحديد المصدر الإجرامي كذا فاعلية القبض على مجرمي المعلوماتية في سبيل تحقيق حماية جنائية على المعطيات المعلوماتية، ضف إلى استصدار قوانين داخلية مستقلة المتعلق بمعالجة المعطيات الشخصية استنادًا إلى القانون رقم 18ـ 07 إعمالًا على احترام الضمانات الفردية عند معالجة تلك المعطيات دون التسريب الافشاء، الاطلاع على الغير إلا في إطار قانوني مرخص، بينما اعترف لإقرار الحماية الجنائية على المصنفات الرقمية لاسيَّما البرامج المعلوماتية قواعد البيانات وفقًا لقانون رقم 03ـ05 المتعلق بحقوق المؤلف، تطبيقًا على ذلك ساهم المشرع إلى تطوير تقنيات التعامل مع القناع الرقمي من شأنها يعزز ثقة الكيان العام نحو التشجيع لاستخدام النظم المعلوماتية.[106]

(52) ـ فضيلة عاقلي، الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، بحث مقدم إلى المؤتمر الرابع عشر المنظم بأكاديمية الدراسات العليا المنعقد يومي 24- 25 مارس، طرابلس، 2017، ص14.
ـ قانون رقم 06ـ23، المؤرخ في 20 ديسمبر، يعدل ويتمم الأمر رقم 66ـ156 المتعلق بقانون العقوبات، ج. ر. ج. ج، عدد 84 الصادر في 24 ديسمبر 2006.

بناءً على ذلك سنبين المقترحات المماثلة لدى التشريعات الوطنية قابلة إلى الردع والتطوير في التصدي المعلوماتية المتعلق بالشق الموضوعي **(أولا)** ثم نحدد بعد ذلك الشق الاجرائي **(ثانيا).**

أولا: الشق الموضوعي

يستنير على التشريعات الجنائية الوطنية سن قانون المعلوماتية بمثابة مرشد قانوني مستقل في مجال المكافحة، مما يساعد السلطات القضائية الإلمام بكافة المعايير الموضوعية تحت قسم **" الأحكام المتعلقة بالتجريم الاعتداء على الأنظمة الآلية"** إذا ما تم تحريره من القيود الواردة في قانون العقوبات حتى تبدو تلك النصوص القانونية واضحة تمامًا قد تتماشى الخصوصية التقنية لكي نتفادى الثغرات المعيبة على القانون الجنائي إلا سيفقد فعاليته أمام المواجهة لتلك الجرائم المتلاحقة من خلال مراعاة الحلول القانونية المقترحة لدى التشريعات الداخلية التي سنفصله فيمايلي:[107]

- تحقيق التوازن الفعلي بين حماية التكنولوجيا الرقمية والخصوصية الشخصية.
- سن تقنين المعلوماتية والأنترنت مكملًا لقانون العقوبات ذلك بإدخال قواعد مرنة ردعية تستوعب لكافة الأنماط المتصلة بالنظم المعلومات والاتصال مستقبلًا.
- إعداد مشروع قانون التوقيع الالكتروني والوثائق الالكترونية فيما يتعلق بالمسائل الجنائية مستبعدًا الأحكام المتعلقة بالتقنين المدني شرط دون تناقض بين مبادئ القانون مع الاعتماد على شهادات التوثيق الرقمي تأكيدًا على الهوية في إطار التعاملات المصرفية مع الخدمات الحكومية الالكترونية.
- السعي إلى تعديل قانون التجارة الالكترونية لمنع المتاجرة عبر الأنترنت في السلع المحظورة النشر الالكتروني على الخدمات غير المشروعة، تنظيم

(53) ـ الإشارة إلى نماذج تدعيمية عن القوانين العربية الصادرة لمكافحة الجريمة المعلوماتية المبينة فيما يلي:
ـ قانون مكافحة الجرائم الالكترونية رقم 14 لسنة 2014 الصادر لدولة قطر، قانون رقم 63 لسنة 2015 المتعلق بمكافحة جرائم تقنية المعلومات لدولة الكويت، الصادر بتاريخ 7 جويلية 2015، القانون الاتحادي رقم 05 لسنة 2012 المتعلق بمكافحة جرائم تقنية المعلومات لدولة الامارات العربية المتحدة، نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم 17، المؤرخ في 1428/3/8ه لمملكة العربية السعودية، قانون مكافحة جرائم تقنية المعلومات رقم 12 الصادر في 6 فيفري 2011 لدولة عمان.
-

جباية الضرائب والرسوم لإتمام الصفقة في المعاملات الالكترونية بغية تأمين البيئة الافتراضية على السير القانوني لتلك الخدمات المقدمة مع احترام حقوق مزودي الخدمة، المورد الالكتروني، المستهلك.

- فعالية دور الحكومة العربية في إحداث برامج تقنية مساهمةً لإغلاق المواقع المرتبطة بالإباحية الإرهاب المعلوماتي، التجسس المعلوماتي، العنف عبر الانترنت تخفيفًا للأنشطة الإجرامية.

- وضع برامج متطورة مضادة لحماية الشبكات المعلوماتية ضد مكافحة الفيروسات، القرصنة الخبيثة مع تجنب تحميل برامج مجهولة المصدر.

- الاعتماد على التقنيات الألية للكشف عن هوية مجرمي المعلوماتية حتى يتسنى تتبع آثر الأنشطة الإجرامية عبر الفضاء الافتراضي.

- الحفاظ على سرية المعلومات الحكومية دون إرسالها إلى العناوين الالكترونية تفاديًا من المخترقين.

- تنظيم مقاييس على إطلاق التقنية تحت المراقبة الأمنية الافتراضية لاسيَّما كيفية إعمال مقاهي الأنترنت المتحدة على قنوات الاتصال الدولي.

- التوعية القانونية على عقد ندوات تحسيسية، المؤتمرات بين السلطات الأمنية القضائية العربية تفاديًا على مخاطر الانترنت.

- اقتراح مشروع تنظيمي بين الوزارة التربوية، التعليم العالي، العدل بشأن تدريس مادة الأخلاقيات لاستخدام الانترنت المقررة على النهج التربوي لرفع الوعي الحسي بين الأطفال، أما على المستوى الجامعي لاسيَّما كليات الحقوق نأمل في تنظيم مقياس الحماية القانونية على المعلوماتية مع السماح للطلبة بالتكوين النظري التطبيقي في مجال تقنية المعلومات، اعداد ملتقيات بالتنسيق بين الأساتذة والطلبة بغية تبادل المناقشة في المسائل القانونية التقنية، بينما نطمح من وزارة العدل السماح لطلبة الكفاءة المهنية للمحاماة، طلبة المدرسة العليا للقضاء الحرص على فاعلية التدريبات الدورية في الميدان الفني المعلوماتي قبل انتهاء التكوين باعتباره تمارين تطبيقية بإدخال الشغف لدى الطلبة الذي يساعد في تحسين الوعي الفكري العلمي مع الحصول على شهادات معتمدة في المجال التقني إلى جانب أداء التربص مع

الخبراء التقنيين بغض النظر عن رجال القانون(المحامين، القضاة، النيابة العامة) حتى يصبح مؤهلًا على الميدان المهني.

ثانيا: الشق الإجرائي

بعدما عالجنا الحلول التشريعية الوطنية من الناحية الموضوعية سوف نحدد الحين على الاقتراحات الاجرائية العملية المبينة ما يلي:

- تنظيم الأحكام الإجرائية المتعلقة بالأساليب التحري المستحدثة بمقتضى القانون رقم 09ـ04 تحت قسم **"أساليب التحري التقني"** من الفصل الثالث تحت عنوان **" القواعد الإجرائية"** من خلال حصر تلك الأحكام في إطار جامع مانع حتى يتسنى باستيعاب لكافة الآليات التقنية التي تسمح باللجوء إليها بغض النظر عن مراقبة الاتصالات الالكترونية، تفتيش المنظومة المعلوماتية، حجز المعطيات المعلوماتية بل يستوجب على المشرع إدخال القواعد المرتبطة بالحفظ والإفشاء العاجلان للمعطيات المعلوماتية شاملًا (التحفظ العاجل على البيانات المخزنة، امر تسليم المعلومات، ضبط المعلومات المخزنة، الجمع الفوري لمعلومات تتبع المستخدمين).

- تعديل الإجراءات الجنائية فيما يتعلق قواعد تفتيش النظم المعلوماتية حتى يتم هناك مشروعية للأدلة مع السماح لسلطات التحقيق ضبط البريد الالكتروني أو أية تقنية تفيد للإثبات الجنائي التقني.

- تطوير المؤسسات الأمنية العربية للالتحاق بالتكنولوجيا الرقمية لاسيَّما التحقيق الجنائي عن بعد مع وضع ضوابط مجسدة في احترام قوانين حماية المعلومات عند الجمع وتبادلها.

- عملية ضبط الأدلة الرقمية المأخوذة من البيئة الافتراضية وليدة إجراءات مشروعة قد يسمح مناقشته داخل المحكمة مع استطاعة القاضي الجنائي الاستعانة بمدى حجية الدليل من خلال تقرير الخبرة الفنية.

- تشجيع تبادل المعلومات بين قوات الشرطة الجنائية مع الوكالات التقنية تسهيلًا على طرق التحقيق في مجال الإجرام المعلوماتي من خلال توفير التكنولوجيات المستخدمة لملاحقة المجرمين في آجال محددة.

- تطوير أنظمة التشغيل الآلي **" نظام لينكس"** على المستوى الوطني بغية حماية البيانات المتداولة بين الهيئات الحكومية من هواجس الجوسسة الاقتصادية،

العسكرية، الأمنية مستبعدًا الأساليب التقليدية المسهلة على القراصنة في الوصول إلى المعلومات السرية.

- تعزيز الموارد المادية البشرية في عمليات التحقيق، الادعاء، المحاكمة بشأن التصدي على الجرائم المتصلة بتكنولوجيا المعلومات والاتصال.
- دعم هيئات الدولة على إنشاء شرطة افتراضية حرصًا على تأمين حماية الأنظمة المعلوماتية.
- إتاحة فرصة على المواطنين في المشاركة لمكافحة الجرائم المعلوماتية من خلال فتح خط الكتروني يتلقى البلاغات الناشئة في إطار ممارسة اللاأخلاقية عبر الأنترنت، الابتزاز الالكتروني، الاحتيال على بطاقات الدفع الالكتروني مع التحفيز لمؤسسات المجني على القيام بالتبليغ دون الإحجام حتى يتسنى من السلطات الأمنية تتبع تلك الجرائم.
- تأهيل الخبراء على البحث في استراتيجية تكنولوجيا المعلومات بغية الالتحاق إلى معايير أمنية تنسيقية للحد من السلاح التقني.
- تفعيل دور المجتمع المدني لاسيَّما الجمعيات الأهلية على وقاية الشباب من الوقوع في السلوك الضار إثر سلبية الانترنت.
- فاعلية دور السلطات الحكومية العربية على إرساء نظام الأمن الوقائي بغية حماية المعلومات المتداولة.[108]

الفرع الثاني
الاستراتيجية الدولية

(54) ـ رابح سعاد، "ضوابط مكافحة الجريمة المعلوماتية"، **"مجلة القانون العام الجزائري والمقارن"**، المجلد 7، العدد 1، كلية الحقوق والعلوم السياسية، جامعة الجيلالي ليابس، سيدي بلعباس، الجزائر، 2021، ص 269.
ـ طرحت العدالة الجزائرية عددًا من القضايا لسنة 2005 دون الوحي لاستفحال الإجرام حسب احصائيات مركز البحوث القانونية القضائية لوزارة العدل الجزائرية الذي لم يتجاوز 38 قضية توبع من خلالها 88 متهم، مما ارتفع معدل مستخدمي الأنترنت في الجزائر حوالي 4,5 مليون إلى غاية 2013 سببًا للاعتماد على البطاقات المصرفية مع الاستعداد لتطوير الكفاءات القضائية الأمنية في مجال المكافحة، بينما تتنوع تلك الجرائم بين هجمات المواقع الالكترونية، الدعاية الإرهابية، سرقة المعطيات الشخصية رغم ذلك جاءت الاحصائيات المقدمة من المركز على النحو الآتي:
الدخول غير المشروع لأنظمة المعالجة الآلية: 11 قضية مفصلة، اتلاف المعطيات المعلوماتية:13 قضية، ادخال المعلومات بطريق الغش:8 قضايا، حيازة المعطيات عن الدخول غير المشروع: 3 قضايا، نشر صور للاستغلال الجنسي: 01 قضية.
انظر/ مداخلة مدير المركز البحوث القانونية القضائية لوزارة العدل أثناء الملتقى الدولي حول محاربة الجريمة المعلوماتية المنعقد بالجزائر في 5 ماي 2010، متاح على الموقع الالكتروني https://crjj.mjustice.dz

التعاون الدولي عماد المواجهة المعلوماتية طالما ترتكب على الفضاء الافتراضي بمثابة البؤرة المركزية للاتصال العالمي من خلال اتحاد الشبكات الآلية الدولية باستخدام تقنية الأقمار الاصطناعية التي فتحت قنوات لاستنفار الأدمغة المحترفة على استفحال الإجرام عبر الدخول للأنظمة المعلوماتية المتصلة بالقطاعات الميدانية لكافة الدول، مما سادت العواقب على الامن العام قد تقتصر التشريعات القانونية الدولية لإرساء التدابير الناجعة بغية الحد من المخاطر اللاحقة بسيادة الدول تزامنًا على ذلك قد تمت تكثيف جهودًا مبادرة من خلال إبرام المعاهدات المتعددة الأعضاء في السعي نحو المكافحة مع تعزيز دور التعاون الدولي الفعال على الوفاء بالالتزامات المعاهدة حسبما أكدت عليها اتفاقية مجلس أوروبا بشأن الإجرام السيبراني ما يلي:" **ضرورة التزام الدول الأعضاء بتسليم المجرمين والمساعدة المتبادلة في التحقيق وجمع الأدلة واتخاذ كافة التدابير التشريعية"** بينما جاءت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات طبقًا المادة 1/32 ما يلي:" **على جميع الدول الأطراف تبادل المساعدة فيما بينها بأقصى مدى ممكن لغايات التحقيق أو الإجراءات المتعلقة بجمع الأدلة الالكترونية في الجرائم المرتكبة بواسطة تقنية المعلومات".**(109)

إذ أسفرت المصالح الدولية على تطوير البنية التشريعية المحلية سعيًا للالتحاق في ميدان تكنولوجيا المعلومات إلا هناك تفاوت جدير من حيث سبل المكافحة بين مناهج القانونية المتخذة لأية دولة لاسيَّما الولايات المتحدة الأمريكية قد أصدرت القانون المتعلق بإساءة استخدام الحاسب الآلي الذي يعالج القواعد الموضوعية المرتبط بالتجريم والعقاب تماشيًا مع الطبيعة المعلوماتية، بينما هناك من الدول اعتدت على التعديلات المستحدثة بشأن مسايرة الرقمنة رغم السرعة الحادة في تطور الجريمة المعلوماتية لاسيَّما فرنسا التي ساهمت على التعديل للأحكام العامة الواردة في قانون العقوبات مرارًا يتبعه التشريع الجزائري الذي استحدث قسم مستقل في قانون العقوبات تحت عنوان " **تجريم المساس بأنظمة المعالجة الآلية للمعطيات"** من الناحية تم اصدار القانون رقم 09-04 المتعلق بتكنولوجيا الاعلام و الاتصال ذلك ما نلاحظ على المشرع قد خطى التشريعات الدولية في مجال المكافحة بل مازال يتصادف ثغرة قانونية فيما يتعلق تجريم الاعتداء على المال المعلوماتي الذي بات قاصرًا على مرجعية النصوص الجنائية التقليدية لجرائم الأموال ذلك يتنافى الخصوصية التقنية بل يقتضي على المشرع مراجعة المنظومة المعلوماتية

(55) ـ الاطلاع على الموقع الالكتروني الخاص بالمجلس الأوروبي بشأن مكافحة الإجرام السيبراني:
http://www.conventions.coe.int/treaty/EN/treaties/html/185.htm
ـ المرسوم الرئاسي رقم 14ـ 252، المؤرخ في 08 سبتمبر 2014، المتعلق بالتصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، (ج. ر. عدد 57)، مرجع سابق.

بشأن تعديل القواعد المتعلقة بجرائم الأموال ذات الطبيعة المعنوية غير المادية، أما بالنسبة إلى الدول التي مازالت على قيد المبادئ التقليدية لمواجهة تلك الجرائم التقنية لاسيَّما الدول العربية قد تثير من مسائل متناقضة تتعلق بالإخلال لمبدأ الشرعية الجنائية غالبًا ما يؤدي لإفلات المجرمين على العقاب إثر انعدام التكييف القانوني العقابي بين الدول بما يتوافق ذاك الإجرام المستجد، حيث أجريت دراسة استطلاعية على الآليات المعتمدة من المشرع الدولي حال التعامل مع الواقع المعلوماتي لاسيَّما تقرير الحماية الجنائية للأنظمة المعلوماتية على عاتقها الولايات المتحدة ذات دراية فيدرالية تتولى اهتمام جوهري بحماية المعلومات ذاته فيما يتعلق الخصوصية الشخصية، المعلومات السرية المرتبط بأمن الدولة، بالمقابل نلاحظ على فرنسا اعتمدت موقفًا قانونيًا ملمًا لكافة المعايير التشريعية المقارنة بشأن الحماية الجنائية على المعلوماتية في حين الدول العربية قد عمدت إلى تطوير قوانينها الداخلية لمواكبة الدول السباقة في المجال التزاما بالمعاهدات المبرمة. **(110)**

رغم ذلك بيَّنت التجارب العربية الرؤية الجادة على جسامة ذلك السلاح الرقمي أمام الفضاء الافتراضي ربما يرجع السبب إلى اختلاف الاستراتيجية المعتمدة على استخدامات الحاسب الآلي مع شبكة الأنترنت لتلك الدول بينما نلاحظ هناك من الدول الرائدة في التشريع على مكافحة المعلوماتية لاسيَّما الإمارات العربية المتحدة المملكة العربية السعودية ذات قوى آلية ناجحة حينئذ هناك من الدول لازالت تبادر جهودًا بشأن تكييف القوانين التقليدية لمعاصرة التطور المعلوماتي رغم صدور **" القانون العربي الموحد للأنترنت"** ذات مرشد تقني قانوني لدى مرجعية التشريعات العربية التي ظلت من غير تطوير البنى القانونية الرادعة على المعلوماتية. **(111)**

(56) – RUSSEL Hon Fox, « *justice in the Twenty first Century* », Cavendish Publishing, London, 2000, p.22.

(57) ـ محمد الأمين البشري، محسن عبد الحميد أحمد، الإطار القانوني لمكافحة المعلوماتية على المستوى الدولي، بحث مقدم إلى أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2002، ص 19.

تأسيسًا على ذلك سنحاول دراسة التجارب الدولية المؤطرة في الميدان المعلوماتي معتمدًا الحلول التشريعية المتخذة لمكافحة الجريمة المعلوماتية بدايةً في الولايات المتحدة الأمريكية**(أولا)** ثم الإمارات العربية المتحدة**(ثانيا)** بعد ذلك فرنسا**(ثالثا).**

أولا: الولايات المتحدة الأمريكية

شاء القانون الفدرالي لجرائم الحاسب الآلي (Federal computer fraud and Abuse Acte) أول مرجع تشريعي قائم لمواجهة المعلوماتية الصادر عام 1984 بينما تعرض لتعديلات متكررة إلى غاية 1996 شاملًا سبعة فصول جوهرية متعلق بالقواعد الموضوعية على التجريم والعقاب لاسيَّما الدخول غير المصرح إلى النظام الآلي الواردة في المادة (A1-1030،A4-1030)، اتلاف المعطيات المعلوماتية في المادة(A5-1030)، الحصول غير المشروع على الشفرات المتعلقة بالدخول إلى النظام، الابتزاز المعلوماتي الوارد في المواد (A6-1030،A7-1030)، مما حدد مقدار العقاب بناءً على النية الاجرامية لدى المتهم إلى جانب جسامة الضرر اللاحق بالضحية، ظروف التشديد لاسيَّما حالة العود، حيث باتت قضية الطالب الأمريكي روبرت موريس مثالًا حيويًّا على حرص التشريع الأمريكي لإثبات النية القانونية في مكافحة المعلوماتية بينما هناك ثغرة قانونية ذات الصلة باستخدام البرامج الخبيثة على تعطيل أجهزة الحاسب الآلي دون مطابقة السلوك الإجرامي المرتكب من قبل الطالب مع فحوى المادة (A-1030) التي تسري بالعقاب على الدخول العمدي غير المصرح دون اتجاه الإرادة إلى إعاقة الأنظمة المعلوماتية، بالمقابل جرمت المادة على الدخول العمدي لأنظمة الحماية الأمنية متى ترتب ضرر حاد من خلالها تكيَّف جناية ففي حال وقوع الاتلاف نتيجة الإهمال تكيَّف جنحة.[112]

أما بالنسبة للاحتيال المستندة على بطاقات الممغنطة، الاحتيال المعلوماتي الواردة في المواد (A4-1030،A-1029)، إذ أقرت المسؤولية الجنائية للأشخاص المسموح لهم بالدخول إلى النظام في إطار أعمال الاتلاف إلا إذا تمت عمدًا، حينئذ طرحت وزارة العدل الأمريكية لسنة 2000 تصنيفًا قيَّما على جرائم الكمبيوتر المبينة فيما يلي:(السطو على البيانات المخزنة، الاتجار بالمفتاح السري، حقوق الطبع لاسيَّما المصنفات الرقمية،

(58) –Totty Richard & Hardcastle Antony, « *Computer-Related Crime in information technology and the law* », Macmillan Publishers, U.K, 2005, p.92.

الأفلام، التسجيلات الصوتية، عملية القرصنة، تزوير العلامات التجارية، العملة المشفرة، نشر المواقع الإباحية، الاستغلال الجنسي للأطفال، الاتجار بالأسلحة، غسيل الأموال عبر الانترنت في سنة 1986 صدر المشرع الأمريكي قانون عام لمكافحة جرائم الكمبيوتر الوارد على مصطلحات تقنية استيفاء الشروط المفروضة لدى الدستور الأمريكي بشأن تطبيق القانون على الجرائم المعلوماتية. (113)

حيث بادر التشريع الأمريكي على تظافر الجهود الدولية خلال عقد المؤتمر الثامن لمنع الجريمة ومعاملة السجناء بشأن التصدي لإساءة استعمال الأجهزة الآلية بإدخال تلك الأفعال الجنائية في نطاق التجريم مع اتخاذ هاتيه الإجراءات متى دعت الحاجة باللجوء إليها: (حرص الدول الأعضاء من مضاعفة الأنشطة المبذولة على الصعيد الدولي في إطار تبادل طلبات المساعدة القضائية، تسليم المجرمين، فاعلية دور مركز الاستخبارات الأمنية على التحقيق الجنائي المتعلق في تبادل المعلومات المستفادة للإثبات أمام العدالة، دعم الخبرات الفنية بين سلطات الضبط القضائي)، مما ترصد رؤية ناجعة على تطوير معايير دولية لأمن المعالجة الآلية، إرساء تدابير ملائمة على حل إشكالية الاختصاص القضائي المثارة أمام واقعية الجريمة المعلوماتية ابرام اتفاقيات ثنائية بشأن تنظيم إجراءات التفتيش مع الضبط المباشر على الأنظمة المعلوماتية المتصلة بين الشبكات الدولية، التعاون الفعال بين مؤسسات المجني مع الشاهد المعلوماتي لإتاحة استخدام تلك المعلومات على الأغراض القضائية، اعتراض الاتصالات داخل أنظمة الحاسب الآلي مع تقييم دور الرقابة الأمنية لحماية البيئة الرقمية، تنظيم الإسعافات الأولية التقنية عند الكشف عن جريمة معلوماتية لإعداد نسخ احتياطية من أسطوانات البيانات، البرامج المعلوماتية، ضف إلى اقتراح مشاريع قانونية تدعو لمكافحة المعلوماتية، عقد معاهدات دولية بغية تعزيز التعاون الأمني القضائي.(114)

ثانيا: الإمارات العربية المتحدة

باتت دولة الامارات العربية من التشريعات العربية الرائدة في ميدان حماية النظم المعلوماتية، حيث اعتدت إلى استحداث القانون الاتحادي لسنة 2006 بشأن مكافحة جرائم المعلوماتية، مما أورد المشرع الاماراتي سلسلة من المصطلحات ذات الدلالة القانونية الدقيقة شاملًا على نموذجية الجرائم المعلوماتية بشتى الأنماط المستحدثة لاسيَّما

(59) – CORNWALL (Hugo), « *Computer Fraud Industrial Espionage and Information crime* », Heinemann, London, 2003, p.57.

(60) ـ ليندة شرابشة، السياسة الدولية الإقليمية في مجال مكافحة الجريمة الالكترونية، دار البدر للطباعة والنشر، الجزائر، 2018، ص ص 244– 249.

المعلومات الالكترونية، البرنامج المعلوماتي، نظم المعلومات الالكتروني، الشبكة المعلوماتية المستند الالكتروني، وسيلة تقنية المعلومات، البيانات الحكومية بينما جرم الأفعال الجنائية المتصلة بالإجرام المعلوماتي بما في ذلك تجريم اختراق المواقع، الأنظمة الالكترونية بواسطة الإلغاء، الحذف، التدمير على المعطيات المعلوماتية مع تشديد العقاب إذا ما ترتب لانتهاك المعلومات الشخصية، تجريم تزوير المستندات المعالجة آليًّا مع استعمال المستند المزور، تعطيل الوصول إلى البرامج المعلوماتية، العبث على الشبكة المعلوماتية عن طريق الإيقاف لأداء الوظيفة الآلية، اتلاف البيانات المخزنة تجريم العبث بالفحص الطبي عبر الوسائط الرقمية، عملية التنصت و اعتراض المراسلات عبر الشبكة المعلوماتية، الابتزاز الالكتروني القرصنة، السرقة، الاحتيال، الاستيلاء على السندات المعلوماتية، بيانات البطاقات الالكترونية، التحريض على الدعارة طالما لم يغفل القانون الاتحادي عن تجريم الاتجار بالأعضاء البشرية المخدرات غسيل الأموال عبر الانترنت الترويج للأعمال الإرهابية، التجسس على المؤسسات الحكومية انشاء المواقع، نشر المعلومات بإحدى الآليات التقنية تسهيلًا على ترويج البرامج المخلة بالنظام العام، حينئذ تعرض القانون لانتقادات أثناء حلقة نقاشية المنظمة في معهد التدريب و الدراسات القضائية بالإمارات العربية بشأن وقوع تلك القواعد العقابية إلى تناقض حاد غير ملائم لتلك النصوص الجنائية بينما تم تجريم الوصول إلى بيانات البطاقات الالكترونية باستخدام الانترنت، اصطناع الحسابات الالكترونية الزائفة، الاعتداء على وسائل الدفع الالكتروني، العبث بالأدلة الرقمية التحريض على المساس بأمن الدولة.[115]

أعطت تكنولوجيا الاتصال طابعًا دوليًا لتلك الجرائم التي ترتكب على النطاق الداخلي المعاقب في إطار التشريعات الوطنية بعدما سادت احترافية مجرمي المعلوماتية نحو الفرار عبر الحدود الإقليمية مع استطاعة التحكم بالآلات الرقمية التي تؤدي إلى تمادي فضاء الإجرام، مما أعلن عن الحصار التقني بين إغراء القراصنة مع القوى الأمنية بغية فك الحزام المهدد على الكيان القانوني الدولي، حيث انبثقت التشريعات الجنائية لاسيَّما الامارات العربية إلى انتقاء الحلول القانونية الوقائية في معالجة المعلوماتية تفاديًا من حذافير الإجرام بغية تدعيم الحماية الفاعلة على الأنظمة المعلوماتية الماسة بسيادة الأعمال عاملًا حيوي في بناء الدولة الرائدة، بذلك أقرَّ التشريع الاماراتي نحو الولوج لإبرام معاهدات دولية مضمونة بشأن توحيد تلك الجهود المكثفة على الصعيد الإقليمي الدولي في إطار المكافحة المعلوماتية لكي تعزز الشراكة مع المجتمع الدولي من خلال

(61) ـ ياكر الطاهر، "مكافحة الجرائم الالكترونية بين التشريعات الوطنية والاتفاقيات الدولية"، **"مجلة الصدى الدراسات القانونية والسياسية"**، المجلد 4، العدد 4، مخبر النظام القانوني للعقود والتصرفات في القانون الخاص، جامعة الجيلالي بونعامة، خميس مليانة، عين الدفلى، الجزائر، 2022، ص36.

نجاعة الدور الاستراتيجي المنتهج نحو رسم سياسة تشريعية رادعة على المجابهة بينما تدعو إلى الإشادة بالخطة العملية التي تتطلب تظافر الجهود الدولية الحثيثة تأكيدًا على الوفاء بالالتزام في ضوء المكافحة من خلال تنفيذ شتى برامج التوعية الارشادية ضد المخاطر السلبية للإنترنت، صون تدابير احترازية في حماية المنظومة المعلوماتية مع تأمين الرقابة الجادة داخل الفضاء الافتراضي ضد جوسسة القراصنة، تطبيق نظام الرقيب على الخدمات الموزعة في إطار التجارة الالكترونية، تحقيق التوازن بين مصالح الأفراد اثناء تنظيم المعاملات الالكترونية لاسيَّما المالية.

التعاون على إيجاد قاعدة بيانات دولية لمجرمي المعلوماتية، عقد مؤتمرات دولية بشأن اقتراح مشروع قانون دولي في حماية النظم المعلوماتية، تكريس البحث العلمي العربي لإرساء الحلول الوقائية على الميدان المكافحة، إدراج محاور الاستراتيجية الأمنية العربية بشأن إحداث منظمة الشرطة الجنائية العربية في مكافحة جرائم تقنية المعلومات المقررة في تجسيد فعالية التعاون القضائي لاسيَّما آلية التحقيق الجنائي للأدلة الرقمية معتمدًا على تقنيات متطورة للكشف عن حقيقة الإجرام، ملاحقة المجرمين مع تسليمهم إلى المحاكمة القيام السلطات الأمنية على عمليات تدريبية مشتركة في تبادل الخبرات الفنية بغية رفع الكفاءة العلمية المؤهلة على الميدان المعلوماتي، تفعيل سبل معالجة على الحد من المشكلات المثارة بالضحايا جرائم الحاسب الآلي عبر الاتصال بالمنصة الالكترونية للإبلاغ، خدمة أمان الهادف إلى توفير حماية قانونية على الأمن العام الحفاظ على البنية التحتية للمعطيات السرية مع احترام الحقوق الشخصية في ظل جودة الحياة الرقمية من الجرائم السيبرانية، مما بادرت على تأسيس ضوابط عملية هادفة إلى تأمين البنى التحتية لقطاع الاتصالات مع تقنية النظم المعلوماتية من اختراقات الانترنت بغية توفير بيئة الكترونية آمنة.[116]

الفرع الثالث
التدابير الوقائية المستحدثة في التشريع الجزائري

تبنى القانون رقم 09- 04 المتعلق بتكنولوجيا الاعلام والاتصال حوصلة من التدابير الوقائية المتخذة من قبل المصالح المعنية تفاديًا على وقوع الاعتداءات اللاحقة بالمعلوماتية، مما صاغت إلى بناء استراتيجية طوعية على حماية الفضاء الرقمي ضد

(62) ـ مدني سالم، نحو قانون دولي موحد لمكافحة الجرائم المعلوماتية، ورقة بحث مقدمة إلى مؤتمر الأمن العربي للدراسات والبحوث الجنائية، ابوظبي، 2015، ص 12. متاح على الموقع الالكتروني https://www.dubaipolice.gov.ae

التهديدات التقنية القاصرة لدى التشريعات الوطنية في المواجهة من خلال رصد سبل ناجعة التي سنبينه فيما يلي:

- مراقبة الاتصالات الالكترونية المخولة على سلطات الأمنية فيما يتعلق المراسلات الالكترونية، شبكات الاتصالات بغض النظر إلى التهديدات المحتملة.
- تنفيذ طلبات المساعدة القضائية المتبادلة فيما بين الدول الأعضاء.
- الزامية التعاون مع مصالح الأمن المكلف بالتحقيق القضائي عند الجمع أو التسجيل المعطيات المتعلقة بالاتصالات شرط مراعاة سرية الإجراءات.
- إنشاء مركز البحث التقني القانوني بغية دراسة تطبيقية إحصائية المساهمة في تطوير الإجراءات الكفيلة للحد من الجريمة المعلوماتية.
- الاشتراك في المحافل الدولية للاستفادة من التجارب الميدانية على المجال المعلوماتي الهادفة إلى تحسين الآليات المكافحة.
- إرساء القواعد الاجرائية المرتبطة بمسألة التنازع الاختصاص القضائي الدولي.
- بلورة النصوص الجنائية الدولية المتعلق بالتجريم والعقاب على مجرمي المعلوماتية مع تعزيز الإجراءات الوقائية المكافحة للأنشطة الإجرامية.
- فعالية مؤسسات العدالة الجنائية من خلال عقد دورات تدريبية على رجال إنفاذ القانون في الميدان الفني مع استقطاب الخبراء تدعيمًا على الوعي القانوني.
- بناء الإطار التشريعي الوطني لأمن الفضاء السيبراني بغية حماية الهوية الرقمية.
- الدعم السياسي المؤسساتي التنفيذي على إعداد الخطط الاستراتيجية التقنية.[117]

(65) ـ مهدي رضا، " الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري"، **"مجلة إيليزا للبحوث والدراسات"**، المجلد 6، العدد 2، كلية الحقوق والعلوم السياسية، المركز الجامعي إليزي، الجزائر، 2021. ص118.

ـ قضية نموذجية عن المحادثة المرئية المعروضة أمام القضاء الجزائري التي تتلخص ما يلي:

استجواب المتهم المحبوس داخل مؤسسة إعادة التربية والتأهيل بمدينة القليعة عن طريق الشاشة الالكترونية بعد الاعتراف بالوقائع المنسوبة إليه بعد تقديم النيابة العامة طلباتها، مما أصدرت المحكمة حكمًا علنيًا ابتدائيًا حضوريا وجاهيا بإدانة المتهم. انظر الحكم القضائي الصادر عن محكمة القليعة، قسم الجنح، قضية رقم 17982 بتاريخ 07 أكتوبر 2015 على الموقع الالكتروني الرسمي لوزارة العدل https://www.mjustice.dz

ـ للإشارة إلى الأمثلة النموذجية الميدانية للتعاون الدولي في مجال تسليم مجرمي المعلوماتية المبينة ما يلي:

- عملية Shadow Web لسنة 2018 التي تمت بالاستيلاء على أحد المنتديات الاجرامية المزعومة تحت اسم In Fraud الذي يتعامل في معلومات بطاقات الائتمان المسروقة، انظر تقرير الأمين العام، الجمعية العامة للأمم المتحدة، مكافحة استخدام تكنولوجيات المعلومات للأغراض الإجرامية (القرار رقم187/73)، الدورة 74، البند 109 من جدول الأعمال المؤقت (A/74/130) بتاريخ 30 جويلية 2019، ص09.

خاتمة

في ظل التحول الالكتروني التي افرزتها تقنية المعلومات مصدر ملح ومعيارًا بناء بين الأمم من خلال بروز مجتمع افتراضي يسير ماله، أعماله عبر الفضاء الرقمي عابرًا على الحدود، طالما هناك محاسن متفاعلة إلا جلبت مخاطر من الناحية جراء الاستخدام غير الواعي للأجهزة الآلية من قبل محترفي النظم المعلوماتية الذين يبتغون اعمال تخريبية الماسة بالكيان العام على الدولة لاسيَّما المنظومة القانونية ستفقد مصداقيته في مواجهة هذا السلاح التقني، مما أضحت عائقًا بين مختلف مظاهر الحياة الأمنية الاقتصادية الاجتماعية يهدد الطاقم الدولي، إيمانًا على المشرع الجزائري من مواكبة التشريعات للحد من مخاطر الجريمة المعلوماتية في خضم عصرنة الرقمنة لكافة أجهزة الدولة، بينما أولى أهمية في التصدي الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يستحق التشجيع على تلك الجهود المبادرة في تعقب من يثبت أي محاولة لانتهاك حق المعلومات، إذ احدث تعديلات جديرة في نصوصه الجنائية العقابية الوقائية بمقتضى القانون 04-15 ضف إلى القانون 09-04 مما حرص على إجراءات التحري التقني فيما يتعلق التحقيق في الشبكات المعلوماتية مع ضبط الأدلة الرقمية ذات دور جوهري على الاثبات امام القضاء سعيا على ذلك بالحفاظ للأنظمة المعلوماتية مع حماية البيئة الرقمية من اغراء مجرمي المعلوماتية لم ينال هذا التعديل مسايرته الفعالة على الالتحاق بالركب المعلوماتي لاسيَّما على جرائم الأموال التي مازالت معتمدة على النهج التقليدي دون احداث تعديل لتلك القواعد التجريمية التي تتنافى مع الطبيعة المعلوماتية دون استجابة تطبيق تلك النصوص القانونية على المعلوماتية.

حيث تناولنا في الفصل الأول على الجوانب التقنية للأنظمة المعلوماتية من خلال مكونات المادية المعنوية للأجهزة الآلية ذات علاقة وطيدة على النموذج القانوني للتجريم والعقاب مع مدى كيفية المعالجة الآلية على البيانات ثم تعرضنا الى الجوانب القانونية فيما يتعلق مسألة أشكال الاعتداء على النظام الآلي بين الخصوصية الشخصية إلى الاعتداءات الماسة بالمال المعلوماتي بينما أوضحنا دراسة العناصر التجريمية مع رصد العقاب على تلك الأفعال الجنائية أما في الفصل الثاني قد تعرضنا إلى النواحي الاجرائية فيما يتعلق التحري على الجرائم الماسة بالنظم المعلوماتية لاسيَّما المعاينة الفنية على المسرح الافتراضي، تفتيش النظم المعلوماتية، التحقيق الجنائي مع الاثبات للأدلة الرقمية أما المحاكمة قد اعتد

المشرع الجزائري الى انشاء القطب الجزائي المتخصص في جرائم تكنولوجيا المعلومات و الاتصال ثم بيَّنا على دور المشرع الجزائري في بذل الجهود المكثفة من خلال ابرام اتفاقيات دولية بغية التعاون الفعال بين السلطات الأمنية القضائية.

من الاستنتاجات المتوصلة إليها خلال الدراسة:

ـ مراجعة المشرع الجزائري على تعديل النصوص المتعلقة بجرائم الأموال

ـ ضرورة الاهتمام بسن تشريعات ردعية نظرًا على جسامة الجريمة المعلوماتية

ـ التعجيل بوضع استراتيجية ناجحة على مؤسسات الأمنية بغية الوقوف على التصدي لمعالم الجريمة.

من الاقتراحات التي سنطرح في الدراسة البحثية ما يلي:

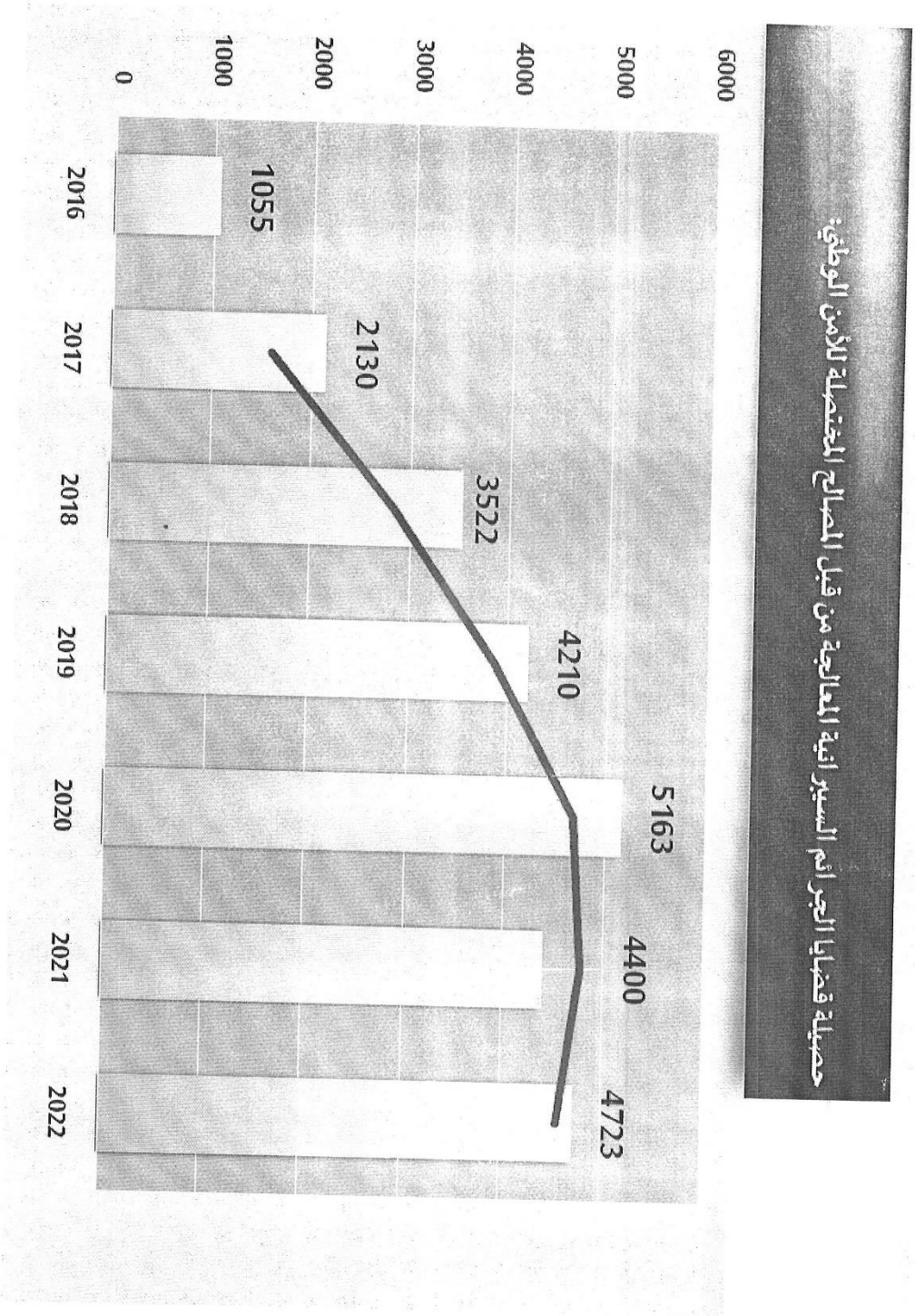
ـ انشاء منصات الكترونية للإبلاغ عن الجرائم المرتكبة عبر الفضاء الافتراضي

ـ اقتراح مشروع قانون المعلوماتية لإدخال الجرائم المتعلق بالتكنولوجيا حسب التطور الملحوظ

ـ عقد مؤتمرات دولية بين أجهزة الأمنية القضائية بغية اكتساب الخبرة التقنية في الميدان المعلوماتي.

مـــلاحـق

إحصائيات القضايا المنجزة على المستوى الوطني من 2012 إلى 2022
2012
47
48
2013
108
91
2014
246
296
2015
567
543
2016
1055
946
2017
2130
2036
2018
3522
3328
2019
4210
4228
2020
5163
5312
2021
4400
4783
2022
4723
5578
المنجزة
الواردة


حصيلة قضايا الجرائم المسيرة آنية المعالجة من قبل المصالح المختصة للأمن الوطني
6000
5000
4000
3000
2000
1000
0
1055
2130
3522
4210
5163
4400
4723
2016
2017
2018
2019
2020
2021
2022

قائمة المراجع

أوّلاً: اللغة العربية

أ: الكتب

01. ـ لیندة شرابشة، السياسة الدولية الإقليمية في مجال مكافحة الجريمة الالكترونية، دار البدر للطباعة والنشر، الجزائر، 2018.

02. أحمد خليفة المالط، **الجرائم المعلوماتية (دراسة مقارنة)**، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، 2012.

03. أحمد عبد اللاه المراغي، التعاون القضائي في مكافحة الجريمة الالكترونية ودور القانون الجنائي في الحد منها، (دراسة تحليلية تأصيلية مقارنة)، المركز القومي للإصدارات القانونية، القاهرة، 2017.

04. إسكندر غطاس، الندوة العربية حول التعاون الأمني الدولي في المجال الجنائي على العالم العربي، دار القلم، دمشق، 2014.

05. أمين عبد الرحمن محمود عباس، الإنابة القضائية في مجال الإجراءات الجزائية، (دراسة مقارنة)، دار الفكر الجامعي، الإسكندرية، 2014.

06. الحفناوي فاروق، **موسوعة قانون الكمبيوتر ونظم المعلومات**، دار الكتب الحديث، مصر، 2001.

07. خالد دودي، **الجريمة المعلوماتية**، دار الإعصار العلمي، الجزائر، 2017.

08. خالد ممدوح ابراهيم، **الجرائم المعلوماتية**، دار الفكر الجامعي، الإسكندرية، 2009.

09. الزعبي محمد، الزعبي سهير، **الحاسوب والبرمجيات الجاهزة**، دار وائل للنشر والتوزيع، عمان، 2002.

10. سعيدي سليمة، حجاز بلال، **جرائم المعلومات والشبكات في العصر الرقمي**، دار الفكر الجامعي، الإسكندرية، 2017.

11. السيد علي والسيد محمد، **الجرائم الإلكترونية (ماهيتها، صورها، اثباتها، مكافحتها)**، دار التعليم الجامعي، الإسكندرية، 2020.

12. عادل عبد العال إبراهيم خراشي، إشكالية التعاون الدولي في مكافحة الجرائم الالكترونية وسبل التغلب عليها، دار الجامعة الجديدة، الاسكندرية، 2015.

13. عبد الفتاح بيومي حجازي، الأحداث والانترنت (دراسة متعمقة عن اثر الانترنت في انحراف الاحداث)، دار الفكر الجامعي، الاسكندرية، 2004.

14. عبد الفتاح بيومي حجازي، **مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي (دراسة قانونية متعمقة في القانون المعلوماتي)**، دار الفكر الجامعي، الإسكندرية، 2006.

15. عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت (دراسة مقارنة)، منشورات الحلبي الحقوقية، بيروت، 2007.

16. محمد علي العريان، الجرائم المعلوماتية (الجهود الدولية المبذولة في مكافحة الجرائم المعلوماتية)، دار الجامعة الجديدة، الإسكندرية، 2011.

17. محمد علي العريان، **الجرائم المعلوماتية**، الطبعة الرابعة، دار الجامعة الجديدة، الإسكندرية، 2004.

18. محمود أحمد عباينة، محمد معمر الرازقي، **جرائم الحاسوب وأبعادها الدولية**، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005.

19. مغبغب نعيم، **حماية برامج الكمبيوتر (الأساليب والثغرات "دراسة مقارنة في القانون المقارن")**، منشورات الحلبي الحقوقية، بيروت، 2006.

20. منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الأنترنت والحاسب الآلي، دار الفكر الجامعي، الإسكندرية، 2014.

21. **نادية دردار، الجهود الدولية لمكافحة الجريمة، المركز القومي للإصدارات القانونية، القاهرة، 2017.**

22. نبيل صقر ، **موسوعة الفكر القانوني (جرائم الكمبيوتر والأنترنت في التشريع الجزائري)**، دار الهلال للخدمات الإعلامية، القاهرة، 2005.

23. نسرين عبد الحميد نبيل، **الجريمة المعلوماتية والمجرم المعلوماتي**، منشأة المعارف، الإسكندرية، 2008.

24. نسرين محسن نعمة الحسيني، محمد حسن مرعي، الجرائم **الواقعة على الأموال (دراسة مقارنة)**، دار الكتب والوثائق القومية، القاهرة، 2020.

25. نهلا عبد االقادر المومني، **الجرائم المعلوماتية**، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2008.

26. يزيد بوحليط، الجرائم الالكترونية والوقاية منهافي القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، قانون العقوبات، قانون الاجراءات الجزائية، كلية الحقوق والعلوم السياسية، جامعة 8ماي1945، قالمة، الجزائر، 2019.

ب: الأطروحات والمذكرات الجامعية

1. أطروحات الدكتوراه

01. براردي نعيمة، الاتصال بين الشرطة والمواطن ودوره في مكافحة الجريمة في الجزائر (دراسة تحليلية استطلاعية بالجزائر العاصمة)، رسالة لنيل شهادة الدكتوراه في علوم الاعلام والاتصال، كلية العلوم السياسية والاعلام، جامعة الجزائر 3، 2014.

02. خالد بن مبارك القحطاني، التعاون الأمني الدولي في مواجهة الجريمة المعلوماتية عبر الوطنية، أطروحة لنيل شهادة الدكتوراه في العلوم الجنائي، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2013

03. شنتير خضرة، "الآليات القانونية لمكافحة الجريمة الالكترونية (دراسة مقارنة)"، اطروحة مقدمة لنيل شهادة الدكتوراه الطور الثالث ل.م.د، تخصص: القانون الجنائي، كلية الحقوق والعلوم السياسية ، جامعة أحمد دراية، الجزائر، 2021.

04. محمد عبد الفتاح عبد المقصود علي، القواعد الإجرائية للجرائم الواقعة عبر شبكة الإنترنت، رسالة مقدمة للحصول على درجة الدكتوراه، قسم القانون الجنائي، كلية الحقوق، جامعة طنطا، مصر، 2015.

05. مصطفوي عبد القادر، "الآليات الجزائية الموضوعية لمواجهة الجرائم المتصلة لتكنولوجية الإعلام والاتصال"، اطروحة لنيل شهادة الدكتوراه ل.م.د في القانون العام، تخصص: القانون الجنائي وعلم الإجرام، كلية الحقوق، جامعة الجزائر بن يوسف بن خدة، الجزائر، 2022.

2. الرسائل الجامعية

-مذكرات الماجستير

01. عبد الرحمان جميل محمود حسين، الحماية القانونية لبرامج الحاسب الآلي (دراسة مقارنة)، رسالة لنيل شهادة الماجستير في القانون الخاص، كلية الدراسات العليا، جامعة النجاح الوطنية، فلسطين، 2018.

02. -مذكرات الماستر

01. سليمة نواوي، دور الدرك الوطني في محاربة الجريمة الالكترونية (المجموعة الإقليمية للدرك الوطني بالمسيلة أنموذجًا)، مذكرة مكملة لنيل شهادة الماستر في علوم الاعلام والاتصال، كلية العلوم الإنسانية والاجتماعية، قسم علوم الاعلام والاتصال، جامعة محمد بوضياف، المسيلة، الجزائر، 2019.

ج: المجلات العلمية

01. - أمال بن صويلح، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الالكتروني في الجزائر، ورقة بحثية مقدمة في إطار الملتقى الدولي الموسوم حول الإجرام السيبراني، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي، برج بوعريريج، الجزائر، يومي 11- 12 أفريل 2017.

02. ـ مجدوب نوال، " الأليات الإجرائية للكشف عن الجريمة المعلوماتية"، **" مجلة البحوث القانونية والاقتصادية"**، المجلد 6 العدد 3، كلية الحقوق والعلوم السياسية، المركز الجامعي أفلو، الأغواط، الجزائر، 2023.

03. -محمد الأمين البشري، محسن عبد الحميد أحمد، الإطار القانوني لمكافحة المعلوماتية على المستوى الدولي، بحث مقدم إلى أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2002.

04. - نشله مصطفى، رابحي لخضر، " جريمة استهداف الأنظمة المعلوماتية للبنوك والمصارف"، **" مجلة العلوم القانونية والاجتماعية"**، المجلد 8، العدد 2، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، 2023.

05. ابراهيم السيد، حسانين الزايد، "الاختلاس المعلوماتي"، المجلة القانونية للدراسات **والبحوث العلمية، المجلد11، العدد09، القاهرة، 2021.**

06. أمال عزري، جمال بن زروق، "استخدام جمعيات المجتمع المدني في الجزائر للشبكات الاجتماعية الالكترونية"، (دراسة ميدانية على جمعيات المجتمع المدني في ولاية سكيكدة)، **"مجلة آفاق للعلوم"**، المجلد 2، العدد 7، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، 2017.

07. امين حماشي، "ماهية الجريمة المعلوماتية"، مجلة دراسات وأبحاث، المجلد01، العدد01، كلية العلوم الانسانية والاجتماعية، جامع زيان عاشور، الجلفة، الجزائر، 2016.

08. بركان فضيلة، "حماية حقوق المؤلف والحقوق المجاورة في الجزائر"، مجلة الدراسات القانونية، المجلد08، العدد01، كلية الحقوق والعلوم السياسية، جامعة يحيى فارس، المدية، الجزائر، 2022.

09. بكوش محمد أمين، هروال نبيلة هبة، "خصوصية المجرم الالكتروني: مجرم الانترنت نموذجا"، مجلة البحوث في الحقوق والعلوم السياسية، المجلد07، العدد01، كلية الحقوق والعلوم السياسية، جامعة بن خلدون، تيارت، الجزائر، 2021.

10. بلعيد الهام، "الجرائم المستحدثة"، مجلة الباحث للدراسات الاكاديمية، الملجد09، العدد02، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر، 2022.

11. بوبعاية كمال، والي عبد اللطيف، "الإشكالات التي تعترض تنسيق التعاون الدولي لمكافحة الجريمة المنظمة عبر الوطنية"، **"مجلة الدراسات والبحوث القانونية"**، المجلد 6، العدد 1، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف المسيلة، الجزائر، 2021.

12. بوقرين عبد الحليم، "حتمية إنشاء ضبطية خاصة بالجرائم الالكترونية"، **"مجلة العلوم القانونية والسياسية "**، المجلد 5، العدد 1، كلية الحقوق والعلوم السياسية، جامعة حمه لخضر، الوادي، الجزائر، 2016.

13. بوهرين فتيحة، "الجريمة المعلوماتية في التشريع الجزائري"، مجلة الحقوق والعلوم الانسانية، المجلد14، العدد04، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، 2021.

14. حزام فتيحة، "الحماية المؤسساتية للأنظمة الرقمية في الفترة التشريعية الممتدة بين 2009-2020"، **" مجلة الأكاديمية للدراسات الاجتماعية والإنسانية"**، المجلد 13، العدد 2، كلية العلوم الإنسانية والاجتماعية، جامعة حسيبة بن بوعلي، الشلف، الجزائر، 2021.

15. حفيظة رفاس، "الحماية الجزائية من جرائم المعلوماتية في القانون الجزائي الجزائري"، مجلة البحوث القانونية السياسية، المجلد02، العدد10، كلية الحقوق والعلوم السياسية، جامعة الدكتور مولاي الطاهر، سعيدة، الجزائر، 2018.

16. درياد مليكة، "التعاون الدولي في مكافحة الجرائم المعلوماتية"، "**مجلة الأستاذ الباحث للدراسات القانونية والسياسية**"، المجلد 4، العدد 1، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، الجزائر، 2019.

17. رابح سعاد، "ضوابط مكافحة الجريمة المعلوماتية"، "**مجلة القانون العام الجزائري والمقارن**"، المجلد 7، العدد 1، كلية الحقوق والعلوم السياسية، جامعة الجيلالي ليابس، سيدي بلعباس، الجزائر، 2021.

18. رستم هشام محمد فريد، "قانون العقوبات ومخاطر تقنية المعلومات: بحث مقدم لمؤتمر الامم المتحدة التاسع لمنع الجريمة ومعاملة المجرمين"، مجلة الامن العام، العدد15، الاردن، 2003.

19. رشيد بلفكرات، "الجريمة الالكترونية كتهديد للأمن الوطني الجزائري"، "**مجلة العلوم القانونية والاجتماعية**"، المجلد 4، العدد 1، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، 2019،.

20. رمزي حوحو، "مواجهة الجريمة المعلوماتية في الجزائر"، مجلة الحقوق والحريات في الانظمة المقارنة، المجلد02، العدد02، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، 2014.

21. سهام خليلي، "خصوصية المجرم الاكتروني"، مجلة المفكر، المجلد12،العدد02، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2017.

22. سهيلة بوزبرة، "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: بين سرية المعطيات الشخصية الالكترونية ومكافحة الجرائم الالكترونية"، "**المجلة النقدية للقانون والعلوم السياسية**"، المجلد 17، العدد 2، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2022.

23. شيخي عائشة، عياشي بوزيان، "الجرائم المتصلة بتكنولوجيا الاعلام والاتصال واشكالها الاقتصادية وآليات مكافحتها"، مجلة الدراسات الحقوقية، المجلد02، العدد02، كلية الحقوق والعلوم السياسية، جامعة الدكتور مولاي الطاهر، سعيدة، الجزائر، 2015.

24. صليحة بوجادي، "الاطار المفاهيمي للجريمة المعلوماتية"، مجلة الدراسات القانونية المقارنة، المجلد07، العدد01، كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بو علي، الشلف، الجزائر، 2021.

25. عثمان خرشي، فتيحة عمارة، " تسليم المجرمين كآلية دولية لمكافحة الجرائم المعلوماتية"، **"مجلة البحوث القانونية والسياسية"**، المجلد 2، العدد 10، كلية الحقوق والعلوم السياسية، جامعة الدكتور مولاي الطاهر، سعيدة، الجزائر، 2018.

26. عزالدين عثماني، "إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية"، **"مجلة دائرة البحوث والدراسات القانونية والسياسية"**، المجلد 2، العدد 4، معهد الحقوق والعلوم السياسية، المركز الجامعي مرسلي عبد الله، تيبازة، الجزائر،2018.

27. عطاء الله فشار، "مواجهة الجريمة المعلوماتية في التشريع الجزائري"، بحث مقدم الى الملتقى المغاربي حول المعلوماتية المزمع عقده بأكاديمية الدراسات العليا بليبيا، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، 2009.

28. عفاف خذيري، " الجريمة الإلكترونية والأمن الوطني"، **"المجلة الجزائرية للدراسات السياسية"**، المجلد 4، العدد 2، قسم العلوم السياسية والعلاقات الدولية، المدرسة الوطنية العليا للعلوم السياسية، الجزائر، 2017.

29. علي قابوسة، "الجريمة الالكترونية في القضاء الالكتروني: المفهوم والأسباب، سبل المكافحة مع التعرض لحالة ليبيا"، مجلة افاق البحوث والدراسات، المجلد02، العدد04، كلية العلوم الاقتصادية، جامعة اليزي، الجزائر، 2019.

30. عمرو زكي عبد المتعال، المعاهدة الدولية لمقاومة جرائم الحاسبات، ورقة عمل مقدمة إلى مؤتمر الجوانب القانونية للتجارة الالكترونية، مقر الجامعة العربية، القاهرة، 2001.

31. عمري فيصل، "الحماية الجنائية للمعلوماتية في التشريع الجزائري"، مجلة آفاق العلوم، المجلد07، العدد01، كلية العلوم الانسانية والاجتماعية، جامعة زيان عاشور، الجلفة، الجزائر، 2022.

32. العيداني محمد، يوسف زروق، " حماية المعطيات الشخصية في الجزائر على ضوء القانون رقم 18-07"، **"مجلة معالم للدراسات القانونية والسياسية"**، المجلد 2، العدد 3، معهد الحقوق والعلوم السياسية، المركز الجامعي تندوف، الجزائر، 2018.

33. غريبي بشرى، "خصوصية المجرم المعلوماتي ودوافعه"، مجلة نوميروس الاكاديمية، المجلد02، العدد02، كلية الحقوق والعلوم السياسية، جامعة ابوبكر بلقايد، تلمسان، الجزائر، 2021.

34. فضيلة عاقلي، الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، بحث مقدم إلى المؤتمر الرابع عشر المنظم بأكاديمية الدراسات العليا المنعقد يومي 24- 25 مارس، طرابلس، 2017.

35. كريمة تدريست، "معوقات نظام تسليم المجرمين كآلية للتعاون القضائي الدولي لمكافحة الجريمة المنظمة عبر الوطنية"، **"المجلة النقدية للقانون والعلوم السياسية"**، المجلد 11، العدد 2، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر،2016.

36. لرقط عزيزة، " التعاون الدولي في مكافحة الجرائم المعلوماتية (إشكالاته، آليات التغلب عليها)"، **"مجلة التواصل"**، المجلد 25، العدد 4، كلية العلوم الإنسانية والاجتماعية، جامعة باجي مختار، عنابة، الجزائر، 2019.

37. لموسخ محمد، "تنازع الاختصاص في الجرائم الالكترونية"، **"مجلة دفاتر السياسة والقانون"**، المجلد 2، العدد 2، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، الجزائر، 2009.

38. لوجاني نورالدين، "دور رجال الضبطية القضائية في مكافحة الجريمة الالكترونية"، مداخلة في يوم دارسي حول علاقة النيابة العامة بالشرطة القضائية ـ احترام حقوق الانسان ومكافحة الجريمة، بالتنسيق مع المديرية العامة للأمن الوطني، المنعقد في إليزي يوم 12 ديسمبر 2009.

39. محمد أحمد سليمان عيسى، "التعاون الدولي لمواجهة الجريمة الإلكترونية"، **"المجلة الاكاديمية للبحث القانوني"**، المجلد 14، العدد 2، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميره، بجاية، الجزائر، 2016.

40. محمد السعيد زناتي، أحمد بنيني، "دور الشرطة الجزائرية في الوقاية من الجريمة الالكترونية ومكافحتها"، **"مجلة تحولات"**، المجلد 2، العدد 1، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، الجزائر، 2019.

41. مراد دمشوش، شول بن شهرة، "السيمات الخاصة للجريمة المعلوماتية"، مجلة المستقبل للدراسات القانونية والسياسية، معهد الحقوق والعلوم السياسية، المركز الجامعي افلو، الاغواط، الجزائر، 2020.

42. مريم لوكال، "الحماية القانونية الدولية الوطنية ذات الطابع الشخصي في الفضاء الرقمي"، **"مجلة العلوم القانونية والسياسية"**، المجلد 10، العدد 1، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر، الوادي، الجزائر،2019.

43. مهدي رضا، " الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري"، **"مجلة إيليزا للبحوث والدراسات"**، المجلد 6، العدد 2، كلية الحقوق والعلوم السياسية، المركز الجامعي إليزي، الجزائر، 2021.

44. موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية، بحث مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 2016.

45. نشناش منية، "مداخلة حول الركن المفترض في الجريمة المعلوماتية"، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، 2016.

46. نعيمة بن يحيي،" الإنابة القضائية الدولية كآلية للتعاون الدولي في مجال مكافحة الجرائم"، **"مجلة الدراسات الحقوقية"**، المجلد 4، العدد 1، كلية الحقوق والعلوم السياسية، جامعة الدكتور مولاي الطاهر، سعيدة، الجزائر، 2017.

47. هشام بشير، "الاليات الدولية لمكافحة الجريمة الالكترونية"، بحث مقدم الى المركز الدولي للدراسات المستقبلية والاستراتيجية (قضايا محاولة لبلورة تطورات جارية)، مصر، 2004.

48. ياكر الطاهر، "مكافحة الجرائم الالكترونية بين التشريعات الوطنية والاتفاقيات الدولية"، **"مجلة الصدى الدراسات القانونية والسياسية"**، المجلد 4، العدد 4، مخبر النظام القانوني للعقود والتصرفات في القانون الخاص، جامعة الجيلالي بونعامة، خميس مليانة، عين الدفلى، الجزائر، 2022.

49. يعيش تمام شوقي، "الجريمة المعلوماتية: دراسة تأصيلية مقارنة"، مخبر اثار الاجتهاد القضائي على حركة التشريع، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، 2019.

د: الملتقيات

01. ذياب موسى البداينة، الجرائم الالكترونية (المفهوم والاسباب)، الملتقى العلمي حول الجرائم المستحدثة في ظل التغيرات والتحولات الاقليمية الدولية، كلية العلوم الاستراتيجية، عمان، الاردن، 2014.

ه: النصوص القانونية

1-النصوص التشريعية

01. القانون رقم 04/09، المؤرخ في 5 اوت 2009 يتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، ج.ر.ج.ج عدد47، الصادر في 10نوفمبر2004، ج.ر.ج.ج عدد71، الصادر في 7فيفري 2004، يعدل ويتمم الامر رقم 66-156، المؤرخ في 8يونيو1966، المتضمن لقانون العقوبات.

02. قانون رقم 06-23، المؤرخ في 20 ديسمبر، يعدل ويتمم الأمر رقم 66-156 المتعلق بقانون العقوبات، ج. ر. ج. ج، عدد 84 الصادر في 24 ديسمبر 2006.

03. قانون مكافحة الجرائم الالكترونية رقم 14 لسنة 2014 الصادر لدولة قطر، قانون رقم 63 لسنة 2015 المتعلق بمكافحة جرائم تقنية المعلومات لدولة الكويت، الصادر بتاريخ 7 جويلية 2015، القانون الاتحادي رقم 05 لسنة 2012 المتعلق بمكافحة جرائم تقنية المعلومات لدولة الامارات العربية المتحدة، نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم 17، المؤرخ في 1428/3/8ه لمملكة العربية السعودية، قانون مكافحة جرائم تقنية المعلومات رقم 12 الصادر في 6 فيفري 2011 لدولة عمان.

2-النصوص التنظيمية

01. المرسوم الرئاسي رقم 19-172، المؤرخ في 06 جانفي 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها وتنظيمها وكيفية سيرها، ج. ر. ج. ج، عدد 37، الصادر في 09 جانفي 2019.

02. المرسوم الرئاسي رقم 20-05، المؤرخ في 20 جانفي 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج. ر. ج. ج، عدد 04، الصادر في 26 جانفي 2020.

03. المرسوم الرئاسي رقم 19– 278، المؤرخ في 20 أكتوبر 2019، المتعلق بالمهام معهد الدراسات العليا في الأمن الوطني وتنظيمه وسيره، ج. ر. ج. ج، عدد 65، الصادر في 24 أكتوبر2019.

04. المرسوم الرئاسي رقم 04 -183، المؤرخ في 26 جانفي 2004، المتعلق بإحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج. ر. ج. ج، عدد 41، الصادر في 27 جانفي 2004.

05. المرسوم الرئاسي رقم 20–183، المؤرخ في 13 جويلية 2020، المتعلق بإعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج. ر. ج. ج، عدد 40، الصادر في 18 جويلية 2020.

و: المراجع الالكترونية

01. يونس عرب، جرائم الكمبيوتر و النترنت (المعنى والخصائص والصور واستراتيجيات المواجهة القانونية، تم الاطلاع عليه يوم: 2023/04/14، على الساعة 12:30د، على الموقع:

http://www.arblaw.org

02. دائل نعيم، مقال منشور بتاريخ: 2018/03/02 على الموقع:

http://www.albayam.ae/across-the-vaee/accdents/2018-30201-3200109

03. محمد المرسي زهرة، "مراحل عملية معالجة البيانات في الحاسب الالكتروني"، مجلة التكنولوجيا والعلوم التطبيقية ، بتاريخ 2018/10/12، على الساعة 10:57د.

04. ABDE Kader, *« la loi Algérienne et le cyber criminalité »*, El Watan économie supplément N°18, 24/05/2005, Disponible en ligne à l'adresse suivante :

http://elwatan.com

05. FIC2020 : ANSSI calls for Européen sovereingnty in cyber Security, in the web site :

https://www.ssi.gouv.fr/uploads/2020/01/anssi-press-release-fic-2020.pdf

06. عثمان بكر عثمان، "المسؤولية عن الاعتداء على البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي"، " مجلة روح القوانين "، المجلد 11، العدد 6، كلية الحقوق، جامعة طنطا، القاهرة، 2016، ص 10، بحث متاح على الموقع الإلكتروني الموالي: http://law.tanta.edu.eg/files/conf4/

07. مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC)، كوفيد-19، تحليل التهديدات الإلكترونية، برنامج مكافحة الجرائم الإلكترونية بالمكتب الإقليمي للشرق الأوسط وشمال إفريقيا، 01 ماي 2020 على الموقع الالكتروني الموالي:

https://www.unodc.org/documents/middleeastandnorthafrica/2020/COVID19MENA-Cyber-Report-AR2.pdf

08. **La sécurisation du cyber space .14/.4/2005 disponible en ligne à l'adresse suivante**

http://www.premier-minister.gouv.fr

09. تقرير عن اجتماع فريق الخبراء المعني بدراسة عن الجريمة السيبرانية المنعقد في فيينا من الفترة 27 إلى 29 مارس 2019 المزيد من التفاصيل على قيادة الدرك الوطني الرجوع إلى الموقع الرسمي الالكتروني التالي

www.mdn.dz/

10. ILIANG Jiansheng, *« Criminalité informatique »*, Diplôme professionnel supérieur en Sciences de l'information et des Bibliothèques, Rapport de stage, École Nationale Supérieure des Sciences de l'information et des Bibliothèques, Paris, 2009, Disponible sur le site

http://www.eldjazaircom.dz/index.php?id-rubrique=313&id-article=3745

11. **Déclaration d' Alger relative à la création du mécanisme africain de coopération policière AFRIPOL, Conférence africaine des directeurs et inspecteurs généraux de police sur AFRIPOL, Alger , le 10 et 11 février 2014, sur le site:** http://www.peaceau.org/uploads/algiers-declaration-afripol-french.pdf

12. جوزي صليحة، "الجزائر تحتضن الجمعية العامة الأولى لآلية الاتحاد الإفريقي في مجال التعاون الشرطي (الآفريبول)"، "مجلة الشرطة"، المجلد 27، العدد 136، الجزائر، 2017، ص09. متاح على الموقع الإلكتروني التالي: https://Afripol.africa-union.org

13. ـ محمد الفاضل، "إشكالات التعاون الدولي"، "مجلة المحاماة المصرية" بتاريخ 26 أفريل 2020 على 13 سا و57 د في الموقع الالكتروني التالي https://www.elmetr.com تم الاطلاع عليه يوم 26 أوت 2023 على 12سا 33د.

14. ـ أحمد بورازم، أساليب التعاون الدولي في القضاء على الجرائم الالكترونية، ورقة بحث مقدمة إلى أعمال الندوة الوطنية، كلية الحقوق والعلوم السياسية، جامعة حمه لخضر، الوادي، الجزائر، منشور على الموقع الالكتروني

www.courdebatna.majustice.dz بتاريخ 15 جوان 2022، تم الاطلاع عليه يوم 26 أوت 2023 عل سا19 و55د.

15. حسين الغفاري، الجهود الدولية في مواجهة جرائم الأنترنت، دار النهضة العربية، القاهرة، 2015، ص14، متاح على الموقع الالكتروني www.cip.org.sa/vb/sharthread.plp3697

16. مخلد إبراهيم الزعبي، " فاعلية التشريعات القانونية في مكافحة الجرائم الالكترونية"، " المجلة العربية للنشر العلمي" المجلد 20، العدد 37، كلية الشرطة، قطر، 2021، ص 2669، متاح على الموقع الالكتروني التالي www.ajsp.net

17. ـ مدني سالم، نحو قانون دولي موحد لمكافحة الجرائم المعلوماتية، ورقة بحث مقدمة إلى مؤتمر الأمن العربي للدراسات والبحوث الجنائية، ابوظبي، 2015، ص 12. متاح على الموقع الالكتروني https://www.dubaipolice.gov.ae

ثانيا: اللغة الأجنبية

1- livre

01. CHAWKI Mohamed , La Cyber Criminalité combattre, edition2, paris, 2009.

02. BAILLYE Milie , MMANUL Daoud, Cybercriminalité et réseaux sociaux la repense pénale, la base de données juridique , éditions Dalloz, France, 2012.

03. AZZOUZI Aliel, la cybercriminalité au Maroc, bishop solution, Maroc, 2010.

04. SEMLALI RDOUANE , cybercriminalité : menaces et contremesures, digital Maghreb, Maroc, 2013.

05. LUCAS leyssac marie Paul, encyclopédie juridique, Dalloz, paris,2003.

06. CLOUAG mango, approching zero data and the criminel under world,2003.

07. JANKARI Rachid, *« Les technologie de l'information au Maroc, Algérie et en Tunisie, vers une filière euromaghrébine des TIC »*, études et analyse, l'Institut de prospective économique du monde méditerranéen, France, 2014.

08. QUEMENER Meriem, *« le rapport sur la cybercriminalité et la protection des internautes »*, la base de donnés juridique des Éditions Dalloz, France, AJ Pénal 2014.

09. RUSSEL Hon Fox, *« justice in the Twenty first Century »*, Cavendish Publishing, London, 2000.

10. Totty Richard & Hardcastle Antony, « *Computer-Related Crime in information technology and the law »*, Macmillan Publishers, U.K, 2005.

11. CORNWALL (Hugo), *« Computer Fraud Industrial Espionage and Information crime »*, Heinemann, London, 2003.

12. CHAMOUX(Françoise), *« la loi sur la fraude Informatique de nouvelles incriminations »*, J.C.P, Université Québec à Montréal, 2006.

2-Article

01. KHELOUFI Rachid, *« Les institutions de régulation »*, "Revenue Algérienne de sciences juridique, économiques et politiques", volume 41, N° 02, Alger.

02. La Cyber sécurité, Revue de la Gendarmerie Nationale avec la collaboration du centre de recherche de l'école des officiers de la Gendarmerie nationale, 4 trimestres, Edition esprit du livre, paris, 2012.

03. BOUDER Hadjira, *« Les dispositifs légaux de lutte contre la cybercriminalité, Bulletin d'information trimestriel, Centre de recherche sur l'information scientifique et technique- CERIST »*, N° 3, Alger, 2015.

مقدمة 1

الفصل الأول الإطار التقني القانوني للنظام المعلوماتي.....1

المبحث الأول الجانب الموضوعي للشبكة المعلوماتية الرقمية.....4
المطلب الأول التعريف التقني للحاسب الآلي 5
الفرع الأول المقصود بالحاسب الآلي (تقنية المعلومات) 6
أولا: مكونات الحاسب الآلي 8
ثانيا: مراحل تقنية المعالجة الآلية(البيانات) 10
الفرع الثاني المقصود بالإجرام المعلوماتي 12
أولاً: خصائص الجريمة المعلوماتية 16
ثانيا: دوافع الإجرام المعلوماتي.....19
ثالثا: أثار الإجرام المعلوماتي.....23
الفرع الثالث تمييز الجريمة المعلوماتية عن الجريمة المادية 25
المطلب الثاني الطبيعة القانونية للجريمة المعلوماتية.....28
الفرع الأول الطبيعة الذاتية للمعلومات.....29
أولا: المعلومة ذات نوعية خاصة 31
ثانيا: المعلومة ذات قيمة مستحدثة.....33
الفرع الثاني محل الجريمة المعلوماتية.....35
أولا: المعلومات.....35
ثانيا: الأجهزة 36
ثالثا: الجهات 37
الفرع الثالث صلاحية الحماية على الأموال المعنوية من الجرائم المعلوماتية.....37
المطلب الثالث المجرم المعلوماتي 41
الفرع الأول سمات المجرم المعلوماتي 42
أولا: الاحترافية.....43
ثانيا: التخوف على كشف الجريمة 43
الفرع الثاني أصناف المجرم المعلوماتي 45
أولا: صغار نوابغ المعلوماتية(the Criminally Négligence/LESBLAGUEURS) 45
ثالثا: مجرمي المعلوماتية في الجريمة المنظمة (Personnel problème subers).....46
الفرع الثالث الضحية في الجريمة المعلوماتية 47
المبحث الثاني أشكال الاعتداء على النظام الآلي 49
المطلب الأول الجرائم الواقعة بواسطة النظام المعلوماتي.....50
الفرع الأول الجرائم المعلوماتية الواقعة على المعطيات الشخصية 51
أولا: الاعتداء على المعطيات الشخصية 53
ثانيا: الاعتداء الالكتروني على الحياة الخاصة 61

الفرع الثاني الجرائم المعلوماتية الواقعة على المال المعلوماتي.....64
أولا: إتلاف المعطيات المعلوماتية.....65
ثانيا: سرقة المال المعلوماتي.....71
الفرع الثالث الجرائم المعلوماتية الواقعة على المصنفات الرقمية.....77
المطلب الثاني الجرائم الواقعة على النظام المعلوماتي.....79
الفصل الثاني الإطار الإجرائي التطبيقي في البيئة الرقمية.....82
المبحث الأول تكريس قواعد المتابعة الجزائية في البيئة الرقمية.....83
المطلب الأول التحري عن الاستدلالات.....84
الفرع الأول الأجهزة المكلفة في التحري عن الجرائم الماسة بالنظم المعلوماتية.....85
أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.....87
ثانيًا: أجهزة الضبط القضائي.....89
الفرع الثاني إجراءات التحري التقني في البيئة الرقمية.....90
المبحث الثاني الآليات التشريعية العملية في مكافحة الجريمة المعلوماتية.....92
المطلب الأول دور المؤسسات العملياتية في التصدي الجريمة المعلوماتية.....93
الفرع الأول المكافحة المؤسساتية الوطنية.....94
أولا: المنظومة الوطنية لأمن الأنظمة المعلوماتية.....95
ثانيا : وحدات الأمن الوطني المختصة في مكافحة الجريمة المعلوماتية.....98
الفرع الثاني المكافحة المؤسساتية الدولية.....103
أولا: التعاون الأمني الدولي.....104
ثانيا: التعاون القضائي الدولي.....109
ثالثا: العقبات الموجهة على التعاون الدولي.....113
الفرع الثالث مكافحة الجمعيات على الجريمة التقنية.....121
المطلب الثاني الجهود التشريعية الدولية في مواجهة الجريمة المعلوماتية.....124
المطلب الثالث الحلول التشريعية المقترحة لمكافحة الجريمة المعلوماتية.....125
الفرع الأول الاستراتيجية الوطنية.....126
أولا: الشق الموضوعي.....127
ثانيا: الشق الإجرائي.....129
الفرع الثاني الاستراتيجية الدولية.....131
أولا: الولايات المتحدة الأمريكية.....134
ثانيا: الإمارات العربية المتحدة.....135
الفرع الثالث التدابير الوقائية المستحدثة في التشريع الجزائري.....138
خاتمة.....137

قائمة المراجع **139**
الفهرس **156**
ملخص

ملخص

أمام الانتشار الواسع للمعاملات الالكترونية في بيئة افتراضية بدأت تبرز أفعال غير قانونية تسبب اضرار فادحة للافراد و الشركات و الدول برمته قد تملصت من العقاب لانعدام استيعاب النصوص التقليدية الجزائية على الطبيعة المعلوماتية ، هنا ادركت الكثير من التشريعات على غرار القواعد التقليدية غير ملائمة في التطبيق ذاك النوع من الجرائم من بينها المشرع الجزائري الذي مازال على حد القواعد التقليدية لجرائم الأموال خاصة بينما نظم قواعد المتعلقة بالنظم المعلوماتية في قانون العقوبات مع القانون 09ـــ 04 المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيا الاعلام و الاتصال، أعطت أحكاما مكملة قصد التصدي للجرائم المعلوماتية، في هذا الاطار سنحاول حصر الجريمة المعلوماتية وفق القانون 04ـــ 15 و 09ـــ 04 مع تبيان مدى سلامة المعلوماتية من الردع.

الكلمات المفتاحية: الفضاء الافتراضي ـــ المجرم المعلوماتي ـــ بيئة رقميةـــ تقنية المعلومات.

Résumé

A la lumière de la propagation généralisée des transactions électroniques dans un environnement virtuel, des actes illégaux ont commence a apparaitre causant des dommages dévastateurs aux individus aux entreprises et aux pays dans leur ensemble qui ont échappe aux sanctions en raison du manque de compréhension des textes pénaux traditionnels sur le sujet nature de linformation ici je me suis rendu compte que de nombreuses législations similaires aux regles traditionnelles ne sont pas appropriees pour appliquer ce type de droit parmi les délits le législateur algerien adhere toujours aux réglés traditionnelles pour les délits financier surtout lorsquil a organise des regles lees a l'information system dans le code pénal avec la loi 0109 relative a la prévention des délits liés aux technologies.

Mots-clés : espace virtuel – information criminelle – environnement numérique – technologie de l'information.