وزارة التعليـم العالـي والبحـث العلمي
جامعة المجاهد عبد الحفيظ بوالصوف –ميلة
كلية الحقوق

القسم: الحقوق
التخصص: قانون جنائي

الرقم التسلسلي: .....
الرمـــــــز: .....

الجريمة المنظمة العابرة للحدود الوطنية وآليات مكافحتها: العصابات الرقمية نموذجا

مذكرة ضمن متطلبات نيل شهادة الماستر

من إعداد الطالبة:
- **بوجغيم أسمـاء**

إشراف الأستاذة:
د. مزياني صبرينة

السنة الجامعية: 2026/2025

وزارة التعليـم العالـي والبحـث العلمي
جامعة المجاهد عبد الحفيظ بوالصوف –ميلة
كلية الحقوق

القسم: الحقوق
التخصص: قانون جنائي

الرقم التسلسلي: .....
الرمـــــــز: .....

الجريمة المنظمة العابرة للحدود الوطنية وآليات مكافحتها: العصابات الرقمية نموذجا

مذكرة ضمن متطلبات نيل شهادة الماستر

من إعداد الطالبة:
- **بوجغيم أسمـاء**

إشراف الأستاذة:
د. مزياني صبرينة

أعضاء لجنة المناقشة:

اسم ولقب الأستاذ(ة)	الجامعة	الرتبة	الصفة
موسى زينب	جامعة المجاهد عبد الحفيظ بوالصوف ميلـة	أستاذ محاضر ب	رئيسا
مزياني صبرينة	جامعة المجاهد عبد الحفيظ بوالصوف ميلـة	أستاذ محاضر ب	مشرفا ومقررا
منصور نورة	جامعة المجاهد عبد الحفيظ بوالصوف ميلـة	أستاذ محاضر ب	ممتحنا

السنة الجامعية: 2026/2025

ملخص

الجريمة المنظمة العابرة للحدود الوطنية وآليات مكافحتها العصابات الرقمية نموذجا تتمحور حول تصاعد نشاط العصابات الرقمية ومدى خطورتها باعتبارها وجه جديد للجريمة المنظمة العابرة للحدود، والتي تطرح تحديات قانونية وأمنية لصعوبة التتبع والملاحقة القضائية غرارًا عن إجراءات البحث والتحقيق الالكتروني، من خلال تبيان مفهوم العصابات الرقمية وخصائصها التنظيمية وآليات عملها، مع تحليل النصوص القانونية والاتفاقيات الدولية ذات الصلة، وتقييم التعاون الدولي في مكافحتها عبر اعتماد المنهج الوصفي التحليلي في ذلك، حيث أن التطور التكنولوجي ساهم في توسع إجرام العصابات الرقمية مقابل محدودية التنسيق الدولي وضعفه وتفاوت التشريعات الوطنية؛ كما خلصت لضرورة تعزيز التعاون القضائي والأمن الدولي من خلال تبني اتفاقيات دولية ملزمة خاصة بالجرائم السيبيرانية، وتفعيل الولاية القضائية العالمية في الأنشطة الخطيرة الرقمية وتسريع تبادل الأدلة الرقمية الكترونيا، إضافة لتطوير آليات الرصد الرقمي والتكوين المتخصص للأجهزة المختصة.

الكلمات المفتاحية: الجريمة المنظمة؛ العصابات؛ الرقمية.

Abstract:

Transnational Organized Crime And Mechanisms For Combating It Digital Gangs As A Model. This study focuses on the escalating activity of digital gangs and their severity as a new face of transnational organized Crim ,this gange pose and the legal and security challenges making tracking and prosection difficut, similar to electronic search and investigation procedures. The study aimed to clarify the concept of digital gangs, their organizational characteristics, and their operational mechanisms, while analyzing relevant legal texts and international agreements, and evaluating international cooperation in combating them through the adoption of a descriptive-analytical approach. The study showed that technological devlopment has contributed to the expansion of digital gang crim, in contrast to the limited and weak international coordination and the disparity in national legislation. It concluded that it is necessary to strengthen judicial cooperation and international security by adopting binding international agreements specific to cybercrimes, activating universal jurisdiction over serious digital activities, accelerating the electronic exchange of digital evidence, and developing digital monitorin mechanisms and specialized training for relevant agencies.

Keywords: Organized Crime, Gangs, Digital.

شكر وعرفان

قال تعالى: " فاذكروني أذكركم واشكروا لي ولا تكفرون".

وعملا بقوله صلى الله عليه وسلم: " من صنع إليكم معروفا فكافئوه فإن لم تجدوا ما تكافئونه فادعوا له حتى ترو أنكم قد كافأتموه "

الحمد لله رب العالمين فهو السند الأول فلك الشكر والثناء على توفيقي لإتمام رسالتي وعلى كل تسهيل؛ واعترافا مني لأهل الفضل الذين علموني الكثير أتقدم بخالص الحب في شكرهم والثناء العاطر وجميل الوفاء لكل من أسدى لي علما أو أفادني بتجربة أو قدم لي رأيا أو توجيها أو توضيحا؛

يسرني بصدر رحب وقلب ممتن أن أتقدم بأسمى كلمات الشكر والعرفان وأعمق معاني التقدير والامتنان إلى من اخترتها مشرفتي "مزياني صبرينة " فقبلت دعوتي فكانت بذلك نبراسي وهدايتي طوال عمر رحلتي لإعداد لرسالتي؛ شكرا لدعمك ومؤازرتك في إرشادي شكرا فلم تتركيني حين اعترضتني العقبات كنت السلم للنجاة؛ شكرا لنصائحك ولتوجيهاتك التي وضحت لي المسالك عند العثرات؛ شكرا لصبرك فلم تملي من الشرح والتشجيعات، شكرا لكونك قويتي من عزيمتي فبُت تلك الطالبة التي عهدت، أسأل الله أن يجزيك عني كل خير وأن يبارك في علمك وعملك ويجعل ما تقدمينه في ميزان حسناتك؛

كما أتقدم بالشكر إلى السادة الأساتذة أعضاء لجنة المناقشة على تكرمهم بقبول مناقشة هذه المذكرة وإبداء ملاحظاتهم وآرائهم القيمة والتي ستثري هذا العمل المتواضع؛

وقبل أن أمضي لا بد لي أن أتقدم بجزيل الشكر والتقدير والمحبة إلى الذين حملوا أقدس رسالة في الحياة ومهدوا لنا طريق العلم والمعرفة إلى جميع أساتذتنا الأفاضل في قسم الحقوق بجامعة المجاهد عبد الحفيظ بوالصوف ميلة؛ وكل من ساعد من القريب أو البعيد في رسم طريقي لبلوغ حلم طفولتي.

الإهداء

الحمد لله حمدًا كثيرًا طيبًا مباركًا فيه كما ينبغي لجلال وجهه وعظيم سلطانه، والحمد لله الذي هذانا لهذا وما كنا لنتهدي لولا أن هدانا الله، الشكر له سبحانه وتعالى الذي بنعمته وتوفيقه تتم الصالحات ورأفته تيسر الصعاب، فما كان من توفيق فمن الله وحده وما التوفيق إلا بالله عليه توكلت وإليه أنيب؛

إلى نفسي... إلى تلك التي صبرت حين تعبت، وقاومت حين انكسرت، واستعانت بالله في لحظات ضعفها فجبر خاطرها، إلى نفسي التي لم تستسلم وآمنت أن بعد العسر يسرا، وأن الله لا يُضيع أجر من أحسن عملا، إلى من سهرت وبكت في جوف الليالي واحتضنت نفسها ولملمت شتاتها، واتبعت حلمها فرسمت طريقا وتحدت العراقيل لبلوغه، إلى نفسي هذا الإنجاز لك أولا؛

إلى أمي الغالية قرة عيني وجنتي... إلى من جعل الله الجنة تحت قدميها، إلى النبع الصافي الذي لا ينضب، والقلب النابض حبا بلا مقابل، إليك أمي يرجع الفضل بعد الله، فشكرًا بحجم السماء على دعواتك في جوف الليالي التي كانت تفتح لي مغاليق الأبواب وتذلل لي الصعاب، شكرًا لكونك ملجئي وقوتي والسبب الأول في كل نجاح أصل إليه، حفظك الله لي ذخرًا وتاجًا فوق رأسي وأطال في عمرك على طاعته؛

إلى أبي عزيزي وأجمل من خُتم اسمي به... إلى السند الحقيقي وضلعي الثابت، إلى من علمني أن الأهداف لا تُنال إلا بالجد والاجتهاد والتوكل على رب العباد، إلى من كان نبع الحنان وصاحب الكلمة الطيبة والحضن الدافئ به أقتاد، دمت لي نورا يضيء عتمات السير حفظك الله وأطال عمرك ورزقك من واسع فضله؛

إلى أخوتي سندي ومسندي... إلى أختي زينب إلى الصديقة الأولى والروح الأقرب لي، وكتفي الثابت الذي لم يمل يوما، كنت ولا تزالين السند الحقيقي والدفء والأمان الذي يُظل طريقي رزقني الله بك لتكوني بصمة نجاحي وبك أعتز وأقتدي؛ إلى توأمي رقية إلى الجزء الأجمل من روحي ورفيقة الدرب والقلب، التي تقاسمت معي الفرح والتعب، شكرا لكونك نصفي ونبض يدفعني للأمام، والروح التي تفهمني دون كلام نجاحي يكتمل بك؛ إلى أخي يوسف إلى القوة التي أستمد منها الأمان والدرع الذي يحميني، والركن الذي أستند إليه دون خوف والقلب الذي ألجأ إليه دون تردد، منذ الطفولة كنت العون والصديق شكرا ياقطعة من روحي؛ إخوتي شكرًا لأنكم كُنتم ظهري حين وقعت وضحكتي حين انهمرتُ جعلتم ثقل الحياة أخف، أنتم عزوتي وكنزي وفخري الذي أتباها به؛

إلى عمتي وأمي الثانية رحمها الله... إلى الطهر الذي غادرنا إلى من كانت لي أما ثانية بحنانها وعطفها وغابت عن العين لكنها في القلب والذاكرة حية اللهم ارحمها برحمتك الواسعة واجعل قبرها روضة من رياض الجنة واجمعنا بها في فردوسك الأعلى؛

إلى كل من كان له أثر طيب في هذا الطريق... إلى كل من دعمني بكلمة طيبة أو شجعني بابتسامة أو ذكرني بدعوة في ظهر الغيب شكرا لكم؛ وإلى كل من كان له أثر طيب في حياتي وترك بصمة في مسيرتي، من رافقني يوما أو بقي أثره حيا في الذاكرة حاضرًا كان أم غائبًا، ومنهم من رحل عن الدنيا بالموت لكن بقي دعاؤه وأثره حاضرا في قلبي؛

إلى من شاركوني المشاعر بصدق ويفهمن صمتي وكنا سندا لي، هن صديقات القلب والدرب اللواتي يسكنن الوجدان فلا تكفيهم الصحائف للشكر : وئام، مريم، منار، إكرام، ايناس، خديجة، آسيا، جيهان، سارة، حنان، نسرين، آمنة، عبير؛

وحتى لا أنسى الفضل شكرا لمن وجدتهم سندي من أول خطوة لحلمي وأحمد الله على معرفتي بهم كانوا ولا زالوا لي نعم المرشد والناصح ومن يستمع لي قبل أن يحكم عليا، من ضممنني بين دعواتهم قبل أن يشاركنني دربي: طاطا زهية، عمي جمال شكرا من القلب على كل شيء.

قائمة المختصرات:

الكلمات	المختصرات
مجلد	م
عدد	ع
صفحة	ص
طبعة	ط
دون مجلد	د.م
دون طبعة	د.ط
من الصفحة إلى الصفحة	ص ص
Page	P

الفهرس

فهرس المحتويات

عناوين المحتوى	الصفحة
شكر و عرفان	
الإهداء	
قائمة المختصرات	
الفهرس	
مقدمة	2
الفصل الأول: الإطار المفاهيمي للعصابات الرقمية	
تمهيد:	11
المبحث الأول: العصابات الرقمية الوجه المتطور للجريمة المنظمة العابرة للحدود الوطنية.	12
المطلب الأول: مفهوم العصابات الرقمية"Digital bands".	12
الفرع الأول: تعريف العصابات الرقمية.	12
الفرع الثاني: من العصابات التقليدية إلى العصابات رقمية.	15
المطلب الثاني: التنظيم الشبكي للعصابات الرقمية.	19
الفرع الأول: الخصائص المميزة للعصابات الرقمية.	19
الفرع الثاني: الهيكل والبنية المنظمة للعصابات الرقمية.	20
المطلب الثالث: الأسلحة الالكترونية للعصابات الرقمية.	22
الفرع الأول: الأساليب التقنية في جرائم العصابات الرقمية.	22
الفرع الثاني: الهجمات الالكترونية للعصابات الرقمية.	24
المطلب الرابع: دوافع العصابات الرقمية.	27
الفرع الأول: الدوافع الشخصية.	27
الفرع الثاني: الدوافع خارجية.	28
المبحث الثاني: الأنشطة الإجرامية التي تمارسها العصابات الرقمية.	29
المطلب الأول: الهجمات الواقعة على الأموال.	29
الفرع الأول: الاحتيال باستخدام بطاقات الائتمان عبر الانترنت.	29
الفرع الثاني: التصيد الاحتيالي الالكتروني.	30
الفرع الثالث: الاحتيال عبر الانترنت.	31
المطلب الثاني: الهجمات الواقعة على الأشخاص.	31

الفرع الأول: الابتزاز الالكتروني.	31
الفرع الثاني: سرقة الهوية.	33
الفرع الثالث: الملاحقة والتشهير الالكترونية.	34
المطلب الثالث: الهجمات الواقعة على الشبكات الالكترونية.	34
الفرع الأول: هجمات الاختراق.	35
الفرع الثاني: التجسس الالكتروني.	36
الفرع الثالث: التوقيع الالكتروني.	37
المطلب الرابع: الهجمات الواقعة على أمن الدولة.	39
الفرع الأول: الاتجار بالبشر عبر الانترنت.	39
الفرع الثاني: الاتجار بالمخدرات عبر الشبكات الالكترونية.	42
الفرع الثالث: هجمات الإرهاب الالكتروني.	44
ملخص الفصل الأول	46
الفصل الثاني: الإطار القانوني الدولي للعصابات الرقمية	
تمهيد:	48
المبحث الأول: استراتيجيات الأمن السيبيراني لمكافحة العصابات الرقمية.	49
المطلب الأول: الجهود الإقليمية في مواجهة العصابات الرقمية.	49
الفرع الأول: اتفاقية بودابست 2001 لمكافحة الجرائم السيبيرانية.	49
الفرع الثاني: اتفاقية الجامعة العربية لمكافحة الجريمة السيبيرانية.	52
المطلب الثاني: دور اتفاقية الأمم المتحدة لمكافحة الجرائم الالكترونية 2024.	54
الفرع الأول: اعتماد الاتفاقية.	55
الفرع الثاني: مبررات الأهمية الإستراتيجية للاتفاقية.	55
الفرع الثالث: الإطار القانوني الدولي لمكافحة الجريمة السيبيرانية عبر الاتفاقية.	56
المطلب الثالث: المحاكمة الإجرائية في الاتفاقيات الدولية.	58
الفرع الأول: معاينة مسرح الجريمة.	59
الفرع الثاني: إجراءات تفتيش نظام المعلومات وضبطها.	60
المطلب الرابع: آليات التعاون القضائي الدولي.	64
الفرع الأول: تعزيز التعاون القضائي الدولي.	64
الفرع الثاني: تعزيز تبادل المعلومات والإنذار المبكر.	67

الفرع الثالث: تعزيز التعاون التقني والفني.	70
المبحث الثاني: سبل تعزيز الجهود الدولية في مواجهة العصابات الرقمية.	72
المطلب الأول: التحديات القانونية لمكافحة العصابات الرقمية.	72
الفرع الأول: إشكالية الاختصاص القضائي.	72
الفرع الثاني: صعوبات الإثبات الرقمي.	74
الفرع الثالث: دور الذكاء الاصطناعي في استشراف ورصد العصابات الرقمية.	77
المطلب الثاني: الإجراءات الجنائية والتحقيقية.	78
الفرع الأول: إجراءات الجهات المعنية بالمواجهة.	79
الفرع الثاني: استراتيجيات جمع الأدلة الرقمية وتحليلهاDigital Forensics.	82
الفرع الثالث: إجراءات الضبط والحجز الإلكتروني.	85
المطلب الثالث: الأجهزة الدولية للتصدي للعصابات الرقمية.	87
الفرع الأول: المنظمة الدولية للشرطة الجنائية (الأنتربول).	87
الفرع الثاني: جهود المنظمات الإقليمية.	90
المطلب الرابع: آليات الوقاية والمواجهة المستقبلية للعصابات الرقمية.	92
الفرع الأول: التوعية كآلية قبلية للوقاية.	93
الفرع الثاني: سبل الوقاية والعلاج للقضاء على الصعوبات.	95
ملخص الفصل الثاني	98
الخاتمة	100
قائمة المصادر والمراجع.	104

مقدمة

مقدمة

شكلت الظاهرة الإجرامية منذ فجر التاريخ البشري حقيقة اجتماعية وسلوكا بشريا منحرفا رافق تطور المجتمعات في مختلف مراحلها، إذ تعد الجريمة واحدة من أقدم الظواهر الاجتماعية حيث تعكس في بداياتها انحرافات فردية أو اجتماعية عن الأعراف والقواعد السائدة، وقد شكلت اعتداءاتها خروجا عن تلك القواعد المنظمة للعيش المشترك وانتهاكا صارخا للنظام العام، وتتنوع وفقا للظروف الاقتصادية والسياسية والثقافية لكل عصر.

وفي مراحل تاريخية مبكرة كانت الجرائم تمارس في أغلبها على نحو مباشر وضمن إطار محلي وفي نطاق جغرافي ضيق ومحدود، حيث كانت الأدلة المادية وسلطات التحقيق التقليدية قادرة إلى حد ما على تتبع الجناة وملاحقتهم، ومع تطور المجتمعات وتنامي التعقيد قي العلاقات الاجتماعية والاقتصادية، أدرك العقل الإجرامي أن العمل الفردي لم يعد كافيا لتحقيق العوائد غير المشروعة المرجوة، فأخذت الأشكال الإجرامية تتطور وانتقلت من جرائم فردية بسيطة إلى أشكال أكثر تنظيما، مما مهد الطريق لظهور ما يعرف بالجريمة المنظمة.

أدى تزايد الترابط الاقتصادي العالمي وتوسع حركة البضائع والأشخاص ورؤوس الأموال لتحول الجريمة المنظمة إلى ظاهرة عابرة للحدود الوطنية، فقد باتت المجموعات الإجرامية قادرة على استغلال الفجوات التشريعية بين النظم القانونية المختلفة، واعتمادها على شبكات لوجستية معقدة ووسائل اتصال متطورة، وأساليب تمويل دولية بما يتيح لها العمل في أكثر من ولاية قضائية، دون أن تلتزم بسيادة دولة واحدة أو بأطر إنفاذ القانون المحلية. وقد تجلى هذا التحول بوضوح في أنشطة الاتجار غير المشروع وغسيل الأموال، أيضا تهريب المخدرات والجرائم المرتبطة بالتهريب والفساد، حيث أصبحت الملاحقة الفعالة تتطلب تعاونا قضائيا وأمنيا دوليا متقدما وغالبا ما يتجاوز القدرات الإجرائية التقليدية.

وفي خضم هذا المسار المتصاعد شهد العالم في أواخر القرن العشرين وبدايات القرن الحادي والعشرين ثورة تكنولوجية ورقمية غير مسبوقة، مواكبة لذلك حدث انتشار واسع للانترنت والحوسبة الرقمية والأنظمة المالية الالكترونية، أدى هذا إلى ظهور الفضاء السيبيراني كبيئة افتراضية لا تعترف بحدود السيادة، وكعادتها في استغلال كل تطور بشري سارعت التنظيمات الإجرامية إلى استثمار هذا الفضاء الجديد، مما أدى إلى استحداث جيل جديد من الجرائم عرف بالجرائم الالكترونية والسيبيرانية، تتميز بطابعها الفوري واللامحدودية الجغرافية، تستهدف البيانات والأنظمة المعلوماتية، وهذا ما شكل تحديا جسيما أمام

الترسانة القانونية الجنائية الكلاسيكية التي صممت أساسا للتعامل مع الجريمة في بيئتها المادية، فزاد هذا من تعقيد آليات التحقيق والإثبات الجنائي.

إن هذا التزاوج الحتمي بين الفكر الإجرامي المنظم ذي الطابع العابر للحدود من جهة والبيئة التكنولوجية من جهة أخرى، لم يقتصر على تغيير أسلوب ارتكاب الجريمة فحسب بل برزت عنه عصابات رقمية تختلف عن العصابات التقليدية في الجريمة المنظمة، فهذه الكيانات لم تعد مجرد أفراد قراصنة يعملون بشكل معزول بل تبلورت كمنظمات إجرامية متكاملة الأركان، وتستخدم أدوات أكثر تطورا مثل البرمجيات الخبيثة وبرامج الفدية والعملات المشفرة، إضافة لامتلاكها هياكل تنظيمية مرنة وموارد مالية ضخمة تكسبها قدرة فائقة على الخفاء، متخذة من العالم الافتراضي مسرحا حصريا لعملياتها كالاحتيال المالي، والابتزاز الرقمي وسرقة البيانات الحيوية.

أضحت العصابات الرقمية اليوم تشكل التهديد الأبرز للأمن القومي والاقتصادي في العصر الرقمي، ويطرح هذا الأمر إشكالات قانونية وإجرائية معقدة، فيتطلب لفهم تلك الظاهرة مقاربة قانونية وأمنية متكاملة تجمع بين التحليل الجنائي التقليدي والتقنيات الحديثة في التحقيق وجمع الأدلة الرقمية، وعمليات التفتيش الالكتروني وأيضا المحاكمات في الجرائم الواقعة في العالم الافتراضي، إلى جانب تعاون دولي فعال يعالج التحديات الفريدة التي تفرضها الجريمة الرقمية عبر عصابات رقمية منظمة في عالم افتراضي مترابط بشكل مشفر وغير مسبوق.

إشكالية الدراسة:

أفرزت الثورة التقنية تحولا جذريا في بنية الجريمة المنظمة العابرة للحدود الوطنية، حيث انتقلت من طابعها المادي الكلاسيكي إلى بيئة افتراضية لا مادية، وقد تمخض عن هذا التطور ظهور العصابات الرقمية كجيل مستحدث وأكثر خطورة، فهذه الكيانات تخلت عن العنف المادي والهرمية التقليدية معتمدة على هياكل شبكية لامركزية وأدوات تقنية معقدة لممارسة أنشطة تخريبية عابرة للقارات في أجزاء من الثانية.

وبناء على هذا التعارض بين تطور الظاهرة الإجرامية وقصور الاستجابة التشريعية، تتبلور الإشكالية الجوهرية في التساؤل الآتي:

إلى أي مدى استطاعت المنظومة الجنائية والآليات الدولية استيعاب ظاهرة العصابات الرقمية باعتبارها الأسلوب الأكثر تطورا للجريمة المنظمة؟

الأسئلة الفرعية:

ولتفكيك هذه الإشكالية وفق منهجية قانونية نطرح الأسئلة الفرعية الآتية:

– فيما تتمثل ماهية العصابات الرقمية من حيث المرتكبين والخصائص والأدوات المنظمة والأنشطة الإجرامية المستحدثة؟

– ما هي الإستراتيجيات القانونية والأمنية المتخذة لمكافحة العصابات الرقمية؟

فرضيات الدراسة:

في ضوء الأسئلة الفرعية الواردة في الإشكالية المتعلقة بالعصابات الرقمية بوصفها نمطا متطورا عن الجريمة المنظمة العابرة للحدود الوطنية، تتبنى هذه الدراسة فرضيات بحثية منهجية التي يسعى البحث إلى إثباتها أو نفيها، وتتمثل في الآتي:

– كلما تسارعت وتيرة التحول الرقمي للبنية التحتية للجريمة المنظمة التقليدية، وتطورت الأنشطة الإجرامية التي تمارسها العصابات الرقمية من حيث التعقيد التقني وتنوع الأساليب، أدى ذلك إلى زيادة فعالية عملياتها الإجرامية وتوسع نطاق تأثيرها عالميا، مما يعمق من التحديات المفاهيمية والتشريعية التي تواجهها أجهزة إنفاذ القانون ومواكبة هذا التحول الرقمي.

– كلما تطورت استراتيجيات الأمن السيبيراني وتكاملت مع الآليات الوقائية، وتعمقت سبل تعزيز الجهود الدولية من خلال توحيد التشريعات وتبادل المعلومات الاستخباراتية والقضائية بين الدول، أدى ذلك لترسيخ إطار قانوني دولي رادع ومتماسك قادر على سد الثغرات التشريعية في مواجهة العصابات الرقمية، بتضييق هوامش الإفلات من العقاب وتفكيك المنظومة الهرمية والبنى التحتية لشبكاتها الإجرامية.

أهمية الدراسة:

تكمن أهمية هذه الدراسة في أنها تسلط الضوء على إحدى أخطر الأنشطة الإجرامية غير التقليدية التي – تواجه العالم، والمتمثلة في العصابات الرقمية من خلال تناولها كعامل تهديد للأمن السيبيراني، وهذا ضمن مقاربة شاملة تربط بين الأبعاد النظرية والاستراتيجية والقانونية، وتزداد هذه الأهمية بالنظر إلى ما يلي:

أ- أهمية علمية:

-إثراء المكتبة الجامعية بموضوع جديد في مجال الأمن السيبيراني خاصة في تخصص القانون الجنائي.

- رفع الوعي المجتمعي والمؤسساتي والحكومي بأثر هذه العصابات، ودور الدولة والمجتمع في التصدي لها ومواجهتها.

ب- أهمية عملية:

- الطابع المستحدث والمعقد للعصابات الرقمية والتي تختلف تهديداتها عن التهديدات الكلاسيكية في عدم مركزيتها، وغموض مصدرها وجناتها مع سرعة انتشارها وتنفيذها.

- الحاجة لبناء إستراتيجية دولية متكاملة للتصدي لمخاطر العصابات الرقمية في الفضاء السيبيراني، بما يعزز الأمن الوطني والدولي على حد سواء.

أهداف الدراسة:

تسعى هذه الدراسة إلى تحقيق جملة من الأهداف العلمية المعرفية والعملية المرتبطة بفهم وتحليل العصابات الرقمية كأداة تهديد أمن سيبيراني، من أبرزها:

- فهم الخلفيات التاريخية لنشوء العصابات الرقمية وتطورها مع الإحاطة بالمفاهيم النظرية المتعلقة بها وتحديد خصائصها.

- دراسة الهيكل التنظيمي الذي تعمل به هذه العصابات وأبرز الدوافع التي تسعى لتحقيقها.

- الكشف عن طبيعة الأنشطة الإجرامية التي تمارسها العصابات الرقمية وأنواعها ومختلف مصادرها، وتحليلها عبر أبعادها القانونية والمجتمعية والدولية.

- تقييم الاستراتيجيات الإقليمية والدولية المتمثلة في الاتفاقيات الخاصة بالجرائم الالكترونية لمواجهة العصابات الرقمية.

- تقييم آليات التعاون القضائي الدولي التي تسعى لتبني رؤية موحدة لضبط أنشطة العصابات الرقمية الإجرامية.

– إبراز مختلف التحديات القانونية والجزائية والميدانية التي تواجه السلطات المختصة في ملاحقة العصابات الرقمية وأثناء المحاكمة القضائية.

– تقييم دور الأجهزة الدولية في التصدي للعصابات الرقمية وكيفية تعزيز آليات الوقاية القبلية والمواجهة المستقبلية لهجماتها.

أسباب اختيار الموضوع:

تم اختيار موضوع العصابات الرقمية كأحد الأنماط المستحدثة للإجرام المنظم العابر للحدود منها الذاتية والموضوعية، يمكن ذكرها كالتالي:

أ– أسباب موضوعية:

– حداثة ظاهرة العصابات الرقمية وخطورتها المتزايدة في العالم مع التطور التكنولوجي المتسارع.

– طابع الموضوع العملي والآني، ما يمنحه أهمية مضاعفة على صعيد البحث العلمي بصياغة سياسات وقائية واستباقية لحماية الأمن الدولي والوطني، ووضع سياسات عامة موحدة لمكافحة العصابات الرقمية، فتكون مجال للبحث والتفكير الخصب في ظل بيئة رقمية متسارعة.

– تزايد حجم وخطورة التهديدات السيبيرانية التي تمارسها العصابات الرقمية والساعية لتحقيقها على المدى القريب، والموجهة ضد الأشخاص والمؤسسات والحكومات ما يفرض الحاجة إلى دراسات تحليلية معمقة لفهم طبيعتها وآليات مواجهتها.

ب– أسباب ذاتية:

– الفراغ الأكاديمي في دراسة موضوع العصابات الرقمية من منظور استراتيجي من حيث جوانبها التنظيمية والإجرائية القانونية.

– الرغبة في المساهمة العلمية في إثراء حقل دراسات الجريمة المنظمة باستحداث العصابات الرقمية عنها على مستوى الفضاء الرقمي، واستكشاف تقاطعاتها مع التكنولوجيا والقانون والسياسة، بما يعزز من الأدبيات العربية حول الموضوع.

الدراسات السابقة:

ومن أبرز الدراسات السابقة التي تم الاعتماد عليها في هذه المذكرة، ما يلي:

– دراسة محمد أرزقي نسيب (سبتمبر2000) بعنوان "المافيا أداة للجريمة المنظمة"، الصادرة عن مجلة كلية–أصول الدين–الصراط بجامعة الجزائر، العدد03، سعى الكاتب للتعرض إلى مفهوم "المافيا" انطلاقا من جذورها التاريخية، وتطورها في الوقت الحاضر إلى عصابات منظمة يمارسها أشرار ومجرمون في منظومة سرية وخطيرة، من خلال تسليط الضوء على المافيا في دولتي إيطاليا، و.م.أ فقط، حيث خلصت الدراسة إلى أن المافيا ظهرت فكرتها البدائية في أوروبا خلال القرون الوسطى، وهذا ما يؤكد أن الحضارة الغربية هي مصدر العصابات المنظمة وأصل الإجرام الخطير والمقلق للمجتمعات البشرية، ثم انتقلت لبلدان أخرى بدرجات متفاوتة الخطورة.

– دراسة أحلام بن شريف، بوغرارة الصالح (جوان2012) بعنوان "القرصنة الالكترونية: أنواعها أشكالها وطرق التصدي لها"، الصادرة عن المجلة الجزائرية للعلوم السياسية والعلاقات الدولية، المجلد 05، العدد 01، هدفت الدراسة إلى التعريف بجريمة القرصنة الالكترونية، والأسباب التي تدفع للقيام بهذه الجريمة، ومحاولة التصدي لهذه الظاهرة عبر الحماية القانونية والمعلوماتية من القرصنة الالكترونية، وعلى ضوء ذلك برزت عدة وسائل للحماية منها من خلال التوعية والتثقيف من مخاطرها عبر دورات توعوية، وتقديم إرشادات بعدم الدخول لأي موقع مشبوه والتحفظ بالمعلومات الشخصية.

– دراسة ميرفت محمد حبايبة (2023) بعنوان "مكافحة الجريمة الالكترونية: دراسة مقارنة في التشريع الجزائري والفلسطيني"، الصادرة عن دار اليازوري العلمية للنشر والتوزيع بالأردن، هدفت الكاتبة إلى إبراز مدى خطورة الجريمة الالكترونية كونها عابرة للحدود والقارات، بتسليط الضوء على تعريف الجريمة الالكترونية وأهم سماتها، ومرتكبيها بما يمتازون به من خصائص معينة واعتمادهم على وسائل وأدوات تقنية مستحدثة، كما استعرضت الكاتبة آليات الوقاية من الجريمة الالكترونية والأساليب الوقائية منها، أما الباب الثاني منها فخصص للحديث عن مدى فعالية التشريعات الوطنية والاتفاقيات الدولية في مكافحة الجريمة الالكترونية، فقد كشفت الدراسة عن أن التطور التكنولوجي والانتشار الواسع للأنظمة المعلوماتية قد أسفرا عن ظهور وتطور الجريمة الالكترونية كظاهرة إجرامية متجددة تتسم بالعابرة للحدود والسيادة، مما يخلق صعوبات بالغة في التحقيق والملاحقة القضائية نظرا لسرعة انتشارها وتوزعها الجغرافي الرقمي، وفي سبيل مواجهة هذه التحديات توصي الكاتبة بضرورة إنشاء محاكم دولية محايدة متخصصة لتسوية إشكاليات الاختصاص وتنازع القوانين، والعمل المستمر على تطوير التشريعات الوطنية وتعزيز القدرات المؤسسية والإجرائية للنيابة العامة والقضاة لمواكبة التقدم.

– دراسة محمد السعيد بوفليح (جويلية2024) بعنوان "أطر التعاون الدولي للتصدي للتهديدات السيبرانية"، الصادرة عن مجلة الدراسات القانونية التطبيقية، المجلد01، العدد02، سعى الكاتب إلى تسليط الضوء على هذا النمط الجديد من التهديدات على المستوى الدولي، وكيف تعاملت معه المؤسسات الدولية من خلال هيأتها المختصة، حيث اعتمدت في إنجاز ورقته البحثية على المنهج الوصفي في تعداد أنماط التهديدات السيبرانية وصورها وأطرافها، أما المنهج التحليلي في باقي الجوانب الأخرى، لذلك خلص للتوصية بتكليف لجنة القانون الدولي لإعداد مشروع اتفاقية ملزمة للحد من انتشار التهديد السيبيراني على المستوى الدولي، وتعزيز الأمن السيبيراني المشترك وتحديد المسؤوليات الدولية.

ركزت كل هذه الدراسات على الجانب النظري المفاهيم للجرائم الالكترونية والتهديدات السيبرانية مع إبراز طرق للتصدي لها، وأهملت جانب البحث والتحري وجمع الأدلة الرقمية لإثبات الأنشطة الإجرامية الرقمية التي تقوم بها العصابات الرقمية، كما لم يتطرقوا للعصابات الرقمية كعناصر مستقلة، وهذا ما حاولت دراستنا الموسومة بالجريمة المنظمة العابرة للحدود الوطنية العصابات الرقمية نموذجا التركيز عليه.

منهج الدراسة:

نظرا للطبيعة المركبة والمتعددة الأبعاد للعصابات الرقمية فقد تم الاعتماد على منهجين متكاملين بما يتوافق مع الإشكالية المطروحة للوصول لنتائج دقيقة.

تم الاعتماد على المنهج الوصفي نظرت لتلاؤمه مع طبيعة الموضوع حيث تم توظيفه لعرض الإطار المفاهيمي للعصابات الرقمية، إلى جانب إعطاء نظرة عن خصائصها والأدوات المستعملة في أنشطتها، ودراسة أهدافها التي تسعى لتحقيقها.

أما المنهج التحليلي فقد تم استخدامه في تحليل الأنشطة الإجرامية التي تقوم بها العصابات الرقمية وتأثيراتها على جميع الأصعدة، إضافة لتحليل مختلف الاتفاقيات التي نظمت لمكافحة هذه الظاهرة.

أما المنهج التاريخي فقد تجلى في تبيان مراحل ظهور العصابات الرقمية تاريخيا، مما أدى إلى تحول الترسانة القانونية الكلاسيكية إلى ترسانة مواكبة للتطور التكنولوجي الحديث.

صعوبات الدراسة:

من بين الصعوبات التي واجهتنا في إعداد هذه المذكرة، مايلي:

– نقص الكتب المحلية التي تختص بموضوع العصابات الرقمية بشكل مباشر.

_ صعوبة الوصول لبعض المراجع عبر الانترنت لعدم توفرها ورقيا على مستوى المكتبات.

– اختلاف المصطلحات المفسرة لظاهرة العصابات الرقمية من حيث الفاعلين فيها.

– النقص في الدراسات المحلية في هذا الموضوع مقارنة بالاهتمام الأكاديمي العربي والدولي.

تقسيم الدراسة:

لمعالجة موضوع العصابات الرقمية والإجابة عن الإشكالية المطروحة تم اعتماد خطة ثنائية بتقسيم الدراسة إلى فصلين، وكل فصل لمبحثين رئيسيين بمطالب وفروع.

يتعلق **الفصل الأول** بالإطار المفاهيمي للعصابات الرقمية الذي يشمل بدوره مبحثين أساسين، المبحث الأول بعنوان العصابات الرقمية الوجه المتطور للجريمة المنظمة أما المبحث الثاني معنون بالأنشطة الإجرامية التي تمارسها العصابات الرقمية.

الفصل الثاني تم تخصيصه للإطار القانوني الدولي للعصابات الرقمية حيث قسم لمبحثين، المبحث الأول بعنوان استراتيجيات الأمن السيبيراني لمكافحة العصابات الرقمية، أما المبحث الثاني فكان تحت عنوان سبل تعزيز الجهود الدولية في مواجهة العصابات الرقمية

الفصل الأول:

الإطار المفاهيمي

للعصابات الرقمية

تمهيد:

تعد العصابات الرقمية مصطلحا حديث النشأة، ظهر تزامنا مع بروز الجرائم الالكترونية المرتبطة بالتطور التكنولوجي والمعلوماتي، فبعد أن كانت هذه العصابات في السابق تقتصر على أشكال تقليدية من الجريمة المنظمة العابرة للحدود الوطنية، شهدت تحولا تدريجيا نحو الفضاء الرقمي لتتبنى أنماطا إجرامية أكثر تعقيدا وتطورا، وقد اختلفت المقاربات الفقهية في تحديد مفهوم العصابات الرقمية باعتبارها مفهوما مستقلا عن كل من الجرائم الالكترونية والجريمة المنظمة التقليدية، لكونها تمتاز بجملة من الخصائص التي اكتسبتها نتيجة هذا التحول، لاسيما اعتمادها على الوسائل والتقنيات الالكترونية الحديثة التي مكنتها من تنفيذ هجمات تستهدف الأموال والأشخاص، وحتى أمن الدول والشبكات المعلوماتية.

فضلا عن اتسام أنشطتها بدرجة من النعومة(غياب الركن المادي) والسلاسة في التطبيق مما جعلها أقل وضوحا مقارنة بالجرائم التقليدية، وهو ما يزيد من صعوبة كشفها وتعقبها، كما تعتمد هذه العصابات على طيف واسع من الوسائل، فتجمع بين الأساليب التقنية المتقدة كالروبوتات وتقنية البلوك تشين، وبين الهجمات الالكترونية مثل البرمجيات الخبيثة وهجمات استهداف البنى التحتية والشبكة المعلوماتية، الأمر الذي يعزز من خطورتها ويعقد من سبل مكافحتها.

وعليه، سيتم دراسة هذا الفصل من خلال مبحثين رئيسيين، حيث نخصص المبحث الأول لدراسة العصابات الرقمية باعتبارها الامتداد المتطور للعصابات التقليدية، بالتطرق إلى تعريفها، مراحل تطورها متأثرة بالتطور التكنولوجي، خصائصها، بنيتها التنظيمية، وكذا الأدوات المستخدمة في نشاطها الإجرامي. أما المبحث الثاني فسنخصصه لأهم الأنشطة الإجرامية التي تمارسها العصابات الرقمية في الفضاء الرقمي الالكتروني.

المبحث الأول: العصابات الرقمية الوجه المتطور للجريمة المنظمة العابرة للحدود الوطنية.

المبحث الثاني: الأنشطة الإجرامية التي تمارسها العصابات الرقمية.

المبحث الأول: العصابات الرقمية الوجه المتطور للجريمة المنظمة العابرة للحدود الوطنية.

أدى التطور التكنولوجي إلى نتاج وظهور خدمات جديدة في مجالات عدة، مما ساهم في استفادت الجماعات الإجرامية المنظمة من التنامي المتزايد في مجال وسائل العمل وتقنية المعلومات، فأصبحت تمتاز بالخطورة والتشكيل المنظم العابر للحدود الوطنية، معتمدة في ذلك على عدة استراتيجيات حديثة ومتطورة كأجهزة الكومبيوتر وأنظمة الشبكات والبرمجيات، ذلك تحقيقا لأهداف مختلفة قد تكون شخصية لتراكم أحقاد دفينة أو اقتصادية لتحقيق مكاسب مالية ضخمة أو سياسية لوجود إغراءات توفرها حكومات.

وعليه، سيتم في سياق هذا المبحث التطرق إلى تحديد مفهوم العصابات المنظمة للجرائم الالكترونية الموسومة بالعصابات الرقمية، إلى جانب التنظيم الشبكي لها ومختلف الأدوات المسيرة لها، و ابرز الدوافع التي تسعى للوصول إليها بتنفيذها لمختلف الهجمات والعمليات.

المطلب الأول: مفهوم العصابات الرقمية"Digital bands".

يشهد العالم المعاصر تحولا جذريا بفعل الثورة التكنولوجية في مجال المعلومات والاتصال، حيث أفرزت هذه الطفرة بيئة رقمية متشابكة أتاحت فرصا غير مسبوقة للتفاعل وتبادل البيانات، غير أن هذه التطورات لم تخل من أثار سلبية، إذ استغلتها بعض الجماعات الإجرامية لتطوير أنماط جديدة من النشاط الإجرامي كالعصابات الرقمية التي ساعدها التطور التكنولوجي على بناء صفوف هياكلها، فبدأت ظاهرت القرصنة والاختراق مع بداية ظهور الحاسبة الالكترونية، وازدادت باستخدام تقنية الشبكات الحديثة لتصبح في الأخير جماعات إجرامية منظمة عبر الفضاء السيبراني[1].

الفرع الأول: تعريف العصابات الرقمية.

في ظل التحول الرقمي المتسارع الذي يشهده العالم، لم تعد الجريمة تقتصر على صورتها التقليدية، بل امتدت لتشمل أنماطا مستحدثة تستغل الفضاء الالكتروني كبيئة خصبة لممارستها، وقد أدى هذا إلى بروز فاعلين جدد في المجال الإجرامي، يتمثلون في ما يعرف بالعصابات الرقمية التي تعتمد على التقنيات الحديثة ووسائل الاتصال المتطورة لتنفيذ أنشطتها غير المشروعة.

[1] أحلام بن شريف، الصالح بوغرارة، "القرصنة الالكترونية: أنواعها أشكالها وطرق التصدي لها"، **المجلة الجزائرية للعلوم السياسية والعلاقات الدولية**، م05، ع01، جوان 2012، ص26.

ومن هذا المنطلق تبرز أهمية تحديد مفهوم العصابات الرقمية وضبط عناصرها المميزة، باعتبار ذلك خطوة أساسية لفهم طبيعتها القانونية، لذلك، سنقوم أولا بتحديد تعريف لغوي واصطلاحي للعصابات المنظمة الرقمية.

أولا: تعريف العصابات الرقمية لغة.

العصبة والعصابة: بضم العين الأولى، وكسر العين في الثانية، أي جماعة ما بين العشرة إلى الأربعين[1].

يبدوا أن لفظ "مافيا" الذي يعرف لمصطلح "العصابات"، جاء من الكلمة اللاتينية TOSCAN وتعني البؤس، ولا يعني هذا اللفظ بصقلية الدالة على اسم مكان(مدينة)[2]، ويمكن إرجاع أصل الكلمة إلى القرن التاسع للميلاد(9م)، حيث ظهر تنظيم سري و مسلح لمواجهة الغزاة، وهؤلاء الآخرون هم الذين وصفوا أولئك المقاومين بالمافيوزي، أي الخارجين عن قانونهم(قانون الغزاة)، كما يمكن أن يعود أصل لفظ "مافيا" إلى كلمة MAHIAS أي متبجح متباه[3].

تشير بعض المصادر إن أصل كلمة "مافيا" يوجد في الصيغة الايطالية الشهيرة المعادية لفرنسا(الفرانكية)، ذلك في القرن الثالث عشر 1280م: Morte alla frençais Italie,anela، وتعني باللغة العربية الموت لفرنسا، هو صراخ الايطاليين[4].

عام 1933م أكد MOSCA [5] وجود معنيين للفظ "مافيا": احدهما يشير إلى موقف عزيز على الطبقات الشعبية لمدينة صقلية القديمة، وهو موقف الدفاع عن الوطن[6]. أما المعنى الثاني يشير إلى عصابات

---

[1] **معجم لسان العرب**، ابن منظور، دار صبح و إديسوفت، بيروت، لبنان، 2006، ص227.

[2] محمد أرزقي نسيب، " المافيا أداة للجريمة المنظمة"، **مجلة كلية_أصول الدين_الصراط**، ع03، سبتمبر 2000، ص232.

[3] المرجع نفسه، ص232.

[4] المرجع نفسه، ص233.

[5] MOSCA GAETANO " موسكا غايتانو 1858-1941": بعد دراسة القانون والعلوم السياسية، درس غايتانو موسكا هذين التخصصين في جامعة تورينو، ثم في روما، والى جانب عمله الأكاديمي، انخرط في العمل السياسي وانتخب لعضوية مجلس النواب ثم لمجلس الشيوخ، في كتابه الأول ركز على دراسة تكوين وتنظيم الطبقية الحاكمة المعروفة في ايطاليا بالطبقة السياسية (Sulla teorica dei governmenti e sul governento parlamentare ;1884)، https://www.universalis.fr/encyclopedie/gaetano-mosca/، اطلع عليه بتاريخ 2026/04/25، الساعة22:07.

[6] راجع Encyclopédie Universalisé.P 286.

صغيرة محلية، تستعمل العنف في علاقاتها الخاصة بهدف تسوية نزاعاتها، أو ضمان الهيمنة الاجتماعية والسياسية لزبائنها أو أصدقائها[1].

أيا كان الأصل اللغوي و الاصطلاحي لرجل المافيا، فهو ينعت بأنه(Le mafiose)، أي رجل غاضب ومتغطرس، ماهر في الاختباء داخل المغاور.

ثانيا: تعريف العصابات الرقمية اصطلاحا.

يدخل مفهوم العصابات الرقمية تحت ما يسمى بلفظ القراصنة المنظمون، وقد عرفهم يوسف أبوراوي: "**القراصنة المنظمون (Organized Hackers) المعروفون أيضا باسم مجموعات القراصنة (hacker groups or hacker collectives)، هؤلاء المتسللون هم مجموعة من الأفراد الذين يعملون معا لشن هجوم ضد هدف معين لتحقيق هدف مشترك، من المهم ملاحظة أن هذه الجماعات غير قانونية و أن أفعالها قد تسبب ضررا جسيما لأفراد والمنظمات والحكومات[2]، أشهر هذه المجموعات نجد، مجموعة Anonymous و Lizard Squad و APT**".

كما يمكن تعريفهم بأنهم جماعات منظمة إرهابية أو متطرفة أو قراصنة، يكونوا مخترقون أو متطفلون أو محترفون أو حاقدون، لديهم أفكار اجتماعية أو سياسية أو دينية يرغبون في عرض أفكارهم مستغلين في ذلك اعتماد المؤسسات المختلفة وأجهزة الدولة على أنظمة الحاسبات الآلية، أو السياسية، أو الدينية، أو الاجتماعية وقد تكون دوافع انتقامية بدافع الثار[3].

نستنتج مما سبق أن المجرمون الإلكترونيون(العصابات الرقمية) هم جماعات إجرامية يمارسون أنشطة غير قانونية باستخدام أجهزة الحاسوب والشبكات وغيرها من التقنيات الرقمية، باستخدام أساليب وأدوات متنوعة لارتكاب جرائمهم كالقرصنة، والتصيد الاحتيالي، تختلف دوافعهم كالمكاسب المالية وغيرها، يستغلون الثغرات الأمنية للأنظمة وشبكات الحاسوب.

---

[1] محمد أرزقي نسيب، مرجع سابق، ص233.

[2] يوسف أبوراوي، **القرصنة الأخلاقية: جريمة أم فضيلة ؟**، 2024/01/27، https://blogs.lamah.com/%D8%A7%D9%84%D9%82%D8%B1%D8%B5%D9%86%D8%A9-%D8%A7%D9%84%D8%A3%D8%AE%D9%84%D8%A7%D9%82%D9%8A%D8%A9/، اطلع عليه بتاريخ2026/04/19، الساعة20:00.

[3] ميرفت محمد حبايبة، **مكافحة الجريمة الالكترونية: دراسة مقارنة في التشريع الجزائري والفلسطيني**، الأردن: دار اليازوري العلمية للنشر والتوزيع، ط01، 2023، ص73.

الفرع الثاني: من العصابات التقليدية إلى العصابات رقمية.

يعد تطور العصابات الرقمية امتدادا طبيعيا لتطور الجريمة الالكترونية، إذ يرتبط هذا التحول ارتباطا وثيقا بالتقدم التكنولوجي المتسارع وما افرزه من تقنيات حديثة في مجالات الاتصال والمعلومات، مما دفع بالجماعات الإجرامية المنظمة لإتباع مناهج وجوانب آلية متطورة، وعليه سيتم في سياق هذا الفرع التطرق إلى العصابات الرقمية الشكل الجديد للعصابات القديمة.

أولا: محطات تاريخية في تطور العصابات رقمية.

مر تطور واستحداث العصابات الإجرامية بعدة مراحل هي:

1- مرحلة الخمسينيات من القرن الماضي.

تعد بدايات صناعة الحواسيب وانطلاق تكنولوجيا المعلومات الالكترونية ظاهرة مستقلة عن وسائل الاتصال التقليدية، إذ ترجع إلى أربعينيات القرن الماضي وهو ما يجعل ظهور الجرائم الالكترونية مرتبطا تاريخيا بتطور الحاسوب وانتشار استخدامه. فقط طرح أول جهاز حاسوب للبيع في الولايات المتحدة الأمريكية سنة 1954، ثم استخدم تجاريا خلال الخمسينيات، وخلال هذه الفترة بدأت بوادر جرائم الحاسوب في الظهور، غير أنها كانت تقتصر آنذاك على إساءة استخدامه من الناحية الأخلاقية إلى أن سجلت أول جريمة الكترونية سنة 1958م.

خلال تلك الفترة كانت الأنشطة الإجرامية المتعلقة بالحاسوب تصاغ وفق مدلول أخلاقي أكثر من كونه قانوني، مما أحدث خللا في التمييز بين الجرائم المستهدفة لماديات الحاسوب أو المستهدفة لمعطياته، والتكييف القانوني للجريمة تعاملوا معهم معاملة الجرائم التقليدية إما السرقة أو الإتلاف أو الاحتيال[1].

2- مرحلة الستينيات والسبعينيات من القرن الماضي.

شاعت خلال هذه الفترة استخدامات الحاسوب بكثرة، فساء استعمال الكمبيوتر والعبث في بياناته مطلع الستينيات، فبدأت الصحف تنشر لأول مرة عن ذلك الأمر مقالات تناقش فكرة التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر والاستخدام غير المشروع للبيانات[2].

[1] ميرفت محمد حبايبة، مرجع سابق، ص ص25، 26.

[2] المرجع نفسه، ص26.

تزايد استخدام الحاسوب في مرحلة السبعينيات فظهر عدد من الدراسات القانونية والمسحية المتحدثة عن جرائم الكمبيوتر، إذ تم وصفها بأنها ظاهرة إجرامية لا مجرد سلوكيات مرفوضة، وبدأت ملامح الجرائم الالكترونية تروح في الأفق[1].

3- مرحلة الثمانينيات من القرن الماضي.

اعتبرت فيها الجرائم الالكترونية جديدة نسبيا، وكان القراصنة الإلكترونيون يميلون لاستكشاف الأنظمة الرقمية من باب الفضول أو لإثبات مهاراتهم التقنية، أما عمليات الاختراق فارتكزت على استغلال الثغرات الأساسية في الأنظمة مثل كلمات المرور الضعيفة، إذ كانت تعتبر حسب دراسة أندرسن "محاولات صغيرة لاختبار حدود الأنظمة الرقمية"، فحال الأمر لعدم استيعاب مخاطرها، مما جعلها تبدو اقل تهديدا[2].

4- مرحلة التسعينيات التطور مع الانترنت.

أدى انتشار الانترنت في التسعينيات لبداية الجرائم الالكترونية فأصبحت أكثر تعقيدا، وظهرت أنواع جديدة مثل الاحتيال المالي وسرقة المعلومات البنكية، إذ استخدم المجرمون تقنيات متطورة كالفيروسات والبرمجيات الخبيثة لتعطيل الأنظمة.

شهدت تلك الفترة ازدهارا للبريد الالكتروني ليصبح وسيلة لنشر الفيروسات، وعليه وفقا لتقرير الأمن السيبيراني العالمي تحولت الجرائم الالكترونية إلى أنشطة منظمة ومخطط لها بشكل جيد، من هنا بدأ المجرمون الالكترونيين في استخدام استراتيجيات أكثر تعقيدا، مثل إنشاء مواقع الكترونية مزيفة لجذب الضحايا[3].

5- الجرائم المنظمة والدولية خلال الألفينيات.

أصبحت الجرائم الالكترونية جزء من الجرائم المنظمة وذلك في العقد الأول من القرن الحادي والعشرين 21م، فتشكلت شبكات إجرامية دولية تعرف بالعصابات الرقمية، تستهدف الحكومات والشركات

[1] ميرفت محمد حبايبة، مرجع سابق، ص27.

[2] صادق حطابي، " الجريمة الرقمية: تحليل معاصر لتطور الجرائم الالكترونية وتاثيراتها الاجتماعية"، **مجلة الحكمة للدراسات الفلسفية**، م14، ع01، جانفي2026، ص468.

[3] المرجع نفسه، ص468.

الكبرى، حتى أفراد المجتمع بإتباعها أساليب أكثر تطورا، فاستحدثت جرائم منظمة عبر الفضاء الالكتروني كالهجمات السيبيرانية التي تستهدف البنية التحتية الوطنية.

وفقا للمنتدى الاقتصادي العالمي فان "الهجمات السيبيرانية أصبحت واحدة من اكبر التهديدات العالمية بعد الأوبئة والحروب"، مما يشير لضرورة التدخل القانوني والأمني استجابة لمتطلبات الأمن القومي وحمايته من تهديدات الجرائم الالكترونية[1].

وعليه فان العصابات الالكترونية قد شهدت نقلات نوعية بين مختلف الأزمنة، وانه في لاحق المواعيد والأوقات ستشهد توسعات ضخمة وتنتقل من كونها تمارس إجرامها ومختلف أنشطتها غير القانونية واختراقاتها عبر البريد الالكتروني، فإنها ستستهدف مواقع الكترونية اصطلح عليها اسم " تهديد المواقع".

ثانيا: جرائم العصابات الرقمية.

يمكننا أن نستأنس بعدة عمليات مشهورة توضح كيف تمارس المنظمات الإجرامية الرقمية سلوكياتها غير المشروعة.

1- قضية موريس: يعنى بها تمكن طالب بالغ 23 سنة المدعو ب Rober Morris، من إطلاق فيروس اصطلح عليه لقب "دودة مورس" يكون عبر الانترنت، وذلك بتاريخ فيفري 1988م، فاحدث نتيجة خيالية بإصابته 6000 جهاز مرتبط به ما يقارب 60.000 نظام الكتروني، منها أجهزة المؤسسات والدوائر الحكومية. أما الخسائر التي بلغت فقد تم تقدير مبلغ حوالي 100 مليون دولار لإعادة إصلاح الأنظمة وتشغيل المواقع المصابة، والخسائر غير المباشرة فقد عدت لها مبالغ إضافية اكبر لتصليح الأعطاب الفيروسية[2]، حكم بالسجن لمدة 3 سنوات وغرامة تقدر ب 10.000 دولار على صانع هذا الفيروس المدعو "مورس".

2- قضية نادي الفوضى: خلال عام 1997م قامت جماعة منظمة الكترونيا بإنشاء برنامج مصمم للعمل عبر الانترنت يتم التحكم فيها بلغة مشفرة « Actif-X »، يقوم هذا الأخير باختراق برنامج " كويكن

[1] صادق حطابي، مرجع سابق، ص468.

[2] أحسن رابحي، "الجريمة الالكترونية: النقطة "المظلمة" بالنسبة للتكنولوجية المعلوماتية"، **المجلة الجزائرية للعلوم القانونية والسياسية**، م48، ع01، مارس2011، ص232.

Quiken " المحاسبي، وبذلك تمكنت تلك الجماعات من سرقة أموال ضخمة من أرصدة مستخدمي ذلك البرنامج عبر كافة أنحاء العالم[1].

3- قضية ميليسا: قام شاب أمريكي ينحدر من ولاية "نيوجرسي" بإطلاق اخطر فيروس خلال فترة التسعينيات من القرن الماضي عبر الانترنت، وأطلق عليه اسم فيروس « MELISSA » لاستغلال الخدمات المتصلة ببرامج الاتصالات العامة واختراقها[2].

قامت الشرطة الدولية بفتح تحقيقات استغرقت وقتا طويلا للكشف عن الجاني، وفي مارس1999م اعتقلوه وحكمت عليه السلطات القضائية المختصة بالسجن لمدة 40 عاما إضافة لغرامة مالية قدرت على نحو 500.000 دولار.

4- قضية الجحيم العالمي: قامت جماعة منظمة الكترونيا أو ما يعرف بالعصابات الرقمية تعرف باسم "مجموعة الجحيم العالمي Global Hell"، بإعداد برنامج معلوماتي يتميز بالدقة مما يسمح باختراق المواقع الالكترونية السرية بالنسبة للبيت الأبيض والشرطة الفيدرالية الأمريكية والبنتاقون الأمريكي ووزارة الداخلية الأمريكية، هذه الواقعة صنفت بأنها تهديد خطير و مباشر يمس سلامة وامن البلاد، اتخذت ضدهم الإجراءات القانونية بشن حملة تحقيقات واسعة النطاق والمجال مما كشف عن أفراد تلك العصابات الرقمية الحاملون للجنسية الأمريكية، إما المحاكمة الخاصة بهم فقد ظلت حيثياتها ووقائعها مبهمة تتسم بالغموض و اكتست حيز "الظلام" لليوم الحالي، كون أن تلك الجريمة ترتبط امن واستقرار الدولة وتؤثر على سمعتها الدولية مع باقي العالم، خاصة فيما يخص اقتصادها[3].

بالانتقال للقرن الحادي والعشرين 21م نجد أن أحداثه أكثر إثارة للقلق، في عام 2013م تعرضت شركة "تارجت" العملاقة في قطاع التجزئة لاختراق بيانات هائلة، مما أدى لتسريب المعلومات الشخصية لأكثر من 40 مليون عميل، أما الهجوم فقد نفذ باستخدام بيانات اعتماد مسروقة من جهة خارجية، أثر هجوم برامج الفدية عام 2017م على مئات الآلاف من أجهزة الكمبيوتر عبر 150 دولة، وأيضا البنى التحتية الحيوية كخدمات الصحة الوطنية في المملكة المتحدة. و كان الهجوم من خلا استغلال ثغرة أمنية في نظام التشغيل مايكروسوفت ويندوز.

[1] أحسن رابحي، مرجع سابق، ص ص233، 232 .

[2] المرجع نفسه، ص232.

[3] المرجع نفسه، ص233.

المطلب الثاني: التنظيم الشبكي للعصابات الرقمية.

تعد العصابات الرقمية من أبرز التحولات الجوهرية التي فرضتها الثورة الرقمية، حيث انتقلت من مجرد أفراد منعزلين لكيانات إجرامية شديدة التعقيد، فتطورت هياكلها الهرمية التقليدية لتعتمد تنظيما شبكيا لا مركزيا يمنحها مرونة وخفاء غير مسبوقين، يتميز هذا التنظيم بخصائص فريدة كالجغرافيا العابرة للحدود، والأدوار المتخصصة ديناميكيا والتوظيف الاحترافي لأدوات التشفير والانترنت المظلم، يتوزع أعضاؤها في خلايا مترابطة غير مرئية تجمعها منصات رقمية مشفرة بدلا من أماكن مادية، يستعرض هذا المطلب الخصائص المميزة للعصابات الرقمية، ويحلل هيكلها الشبكي وبنيتها التنظيمية التي تعتبر تحدي أمني.

الفرع الأول: الخصائص المميزة للعصابات الرقمية.

هناك خصائص تتميز بها العصابات الرقمية عن غيرها من الجماعات الإجرامية العادية، ولعل أبرزها:

أولا: التنظيم والتخطيط:

في فضاء الشبكة العالمية للانترنت تقوم العصابات الرقمية بأعمال إجرامية، وفق إستراتيجية التخطي والتنظيم المسبق للعمليات، ودراسة الاحتمالات الممكن وقوعها خلال أي عملية إجرامية يقومون بارتكابها، إذ أن التخطيط يتطلب من الذكاء قدرا عاليا والخبرة لضمان الاستمرارية طويلة الأمد لأنشطتها، ذلك بالابتعاد قدر الإمكان عن رقابة ومتابعة السلطات الأمنية المختصة بقمع الجرائم والأفعال غير المشروعة في الدول، حيث تحتاج العصابات الرقمية إلى طاقم من محترفي الإجرام المتخصصين ذو كفاءات وخبرات عالية المستترة لجرائمهم من الاكتشاف للعيان[1].

ثانيا: التكيف الاجتماعي:

إن هذه الخاصية امتداد لخاصية التخطيط والتطوير، إذ التكييف الاجتماعي بين العصابات الرقمية يخلق لهم منظمة بصفات مشتركة بين أفرادها، فيتكاثفون فيما بينهم بروابط تجمعهم وتساعدهم في ارتكاب جرائمهم، وقد تكون روابط دولية أو تكون محلية، من الروابط الدولية نجد المؤتمرات الدولية الجامعة لمختلف الأصناف الأفراد منهم وحتى الجماعات.

[1] ميرفت محمد حبايبة، مرجع سابق، ص ص65، 64.

تسمح للعصابات المنظمة الرقمية من تحويل أنشطتها ومختلف ممارساتها عبر الدول من دولة لدولة، بحيث أن الدول المحول لها الفعل الإجرامي أو النشاط قوانينها تتسم بالمرونة. كما تجعل هذه الخاصية عمليات الإفلات من إجراءات مكافحة الجرائم الالكترونية سهلة وتيسرها على العصابات الرقمية[1].

ثالثا: التطور في السلوك الإجرامي:

ارتباط العصابات الرقمية بالجرائم الالكترونية ساعدها على تطوير أساليبها الإجرامية، من خلال تبادل الأفكار والخبرات مع ذوي الاختصاص من الجرمين عبر عالم شبكات الانترنت، مما طور من تقنياتها المستخدمة، أما مجرمو العصابات الرقمية فقد اكتسبوا المهارات التقنية ذات الكفاءات العالية في التنفيذ[2].

الفرع الثاني: الهيكل والبنية المنظمة للعصابات الرقمية.

يشكل تحليل الهيكل والبنية المنظمة للعصابات الرقمية مدخلا أساسيا لفهم طبيعتها المعقدة، وتطوير آليات المكافحة القانونية والأمنية الملائمة، لذا يبنى هذا الفرع على مقاربة تحليلية تفكك البينة الداخلية لهذه الكيانات الإجرامية، فيكشف عن هياكلها التنظيمية اللامركزية وتوزع الأدوار وطبيعة الروابط الشبكية التي تجمع بين أعضائها.

أولا: القادة:

يكونون في قمة السلم الهرمي التنظيمي، فيتولى القادة مهمة التخطيط والتنسيق لأنشطة الجرائم الالكترونية، يرسمون المسارات ويحددون الأهداف، يسيرون الشؤون المالية للجماعات الرقمية. أما الكلمة الفاصلة في التنفيذ للعمليات فيكون من نصيبهم، لهم أدوارهم بالغة الأهمية فهم الركيزة للتوجيه وتثبيت الخطى، لضمان الفعالية والنجاح لجميع الأنشطة مع الأهداف الشاملة[3].

ثانيا: المخترقون والخبراء التقنيون:

يمثلون العمود الفقري للعصابات الرقمية، بارعون في الاختراقات للأنظمة وتطوير البرمجيات الخبيثة، إضافة لاستغلال الثغرات الأمنية، يعتبرون القوة التقنية الدافعة لارتكاب الجرائم بالنسبة للعصابات

[1] ميرفت محمد حبايبه، مرجع سابق، ص65.

[2] المرجع نفسه، ص66.

[3] SEARHINFORM, **Decoding The Anatomy of Organized Cybercrime ,** available froum : https://searchinform.com/articles/cybersecurity/cyber-threats/cybercrime/organized-cybercrime Accessed on :17/04/2026.

الرقمية. بفضل خبراتهم في التسلل للأنظمة المتميزة بالسرية والآمنة ونشر مختلف البرمجيات الخبيثة يمكنون العصابات من سرقة البيانات وتحقيق أهدافهم[1].

ثالثا: وسطاء تحويل الأموال:

يلعبون أدوارا حيوية في العمليات المالية للعصابات الرقمية، فهم مسؤولون عن تحويل وغسل الأموال المتحصل عليها بطرق غير مشروعة من خلال مختلف تنفيذ جرائمهم، مما يجعل مهمة أجهزة إنفاذ القانون في التتبع صعبة، يكون دورهم نقل الأموال عبر مختلف الحسابات وولايات قضائية فيصعب جهود السلطات المختصة في استرداد الأموال المسروقة[2].

رابعا: مهندسو التلاعب الاجتماعي:

خبراء في التلاعب بالأفراد للحصول على معلومات سرية أو الولوج للأنظمة الآمنة، يتبعون أساليب نفسية مخادعة للتلاعب بالناس للتمكن من اقتناص وكشف معلومات جد حساسة، مثل كلمات المرور والتفاصيل المالية، حاسمون في تجاوز الدفاعات التقنية واستغلال نقاط الضعف البشرية[3].

خامسا: الموزعون والوسطاء:

لهذه الأعضاء مهمات تتجلى في توليهم تجارة البيانات المسروقة والبرامج الضارة والسلع الرقمية غير المشروعة، أما الموزعون والوسطاء فيعملون في أسواق الانترنت المظلم، يبيعون المعلومات والأدوات المتحصل عليها بمختلف الأنشطة الإجرامية للعصابات الرقمية، دورهم يضمن الاستمرارية للتدفقات والإيرادات من خلال تحويل البيانات المسروقة، والبرامج الضارة لأموال نقدية[4].

وعليه، فالعصابات الرقمية تتخذ هياكل شبكية تنظيمية حيث تتوزع المهام بيم مجموعات صغيرة مستقلة نسبيا، ويتحقق التنسيق عبر بروتوكولات تشغيلية وأطر رقمية وشبكات ثقة، مما يقلل من فرص الرصد والتتبع القانوني لها.

[1] SEARHINFORM, **Decoding The Anatomy of Organized Cybercrime ,** Ibid**.**
[2] Ibid.
[3] Ibid.
[4] Ibid.

المطلب الثالث: الأسلحة الالكترونية للعصابات الرقمية.

في العصر الرقمي الحديث تزايدت التهديدات الالكترونية بشكل كبير، مواكبة لتطور أساليب الإجرام الالكتروني المستمر، ومع تبني الشركات والأفراد للتقنيات الجديدة كيفت العصابات الرقمية أساليبهم لاستغلال الثغرات في تلك الابتكارات، وشن مختلف الهجمات عليهم، سواء كانت الكترونية كرفض أداء الخدمة و قرصنة مواقع الويب، أو تكون أساليب تقنية كشبكات الروبوتات و تهديدات الحوسبة الكمومية، وغيرهم من الأسلحة الالكترونية التي تعتمد عليها بشكل كبير مختلف العصابات الرقمية لتحقيق أهدافهم المرجوة، وهذا ما سنتطرق له خلال هذه الجزئية.

الفرع الأول: الأساليب التقنية في جرائم العصابات الرقمية.

أولا: شبكات الروبوتات واستغلال انترنت الأشياء:

لا تزال شبكات الروبوتات أداة بالغة الأهمية لمجرمي العصابات الرقمية، فهي عبارة عن شبكات من الأجهزة المخترقة، إن انتشار أجهزة انترنت الأشياء التي تعاني من ضعف الحماية يساعد في توسع شبكات الروبوتات. تستعمل هذه الشبكات في لأغراض عدة، منها هجمات الحرمان من الخدمة الموزعة (DDoS) وسرقة بيانات الاعتماد وإرسال البريد العشوائي، على غرار أن الأعداد الهائلة لأجهزة انترنت الأشياء توفر مساحات واسعة للهجمات الالكترونية[1].

ثانيا: استغلال ثغرات التعلم الآلي:

تزايد اعتماد المؤسسات على التعلم الآلي بتطبيقات متنوعة، فالعصابات الرقمية تجد طرقا لاستغلال تلك النماذج التعليمية. وتتضمن هجمات الخصومة إدخال بيانات مضللة لنماذج التعلم الآلي وذلك للتلاعب بمخرجاتها، ولهذا الأمر عواقب وخيمة خاصة في مجالات التمويل والرعاية الصحية والمركبات ذاتية القيادة، إذ أن نماذج التعلم الآلي تستخدم لاتخاذ القرارات الحاسمة[2].

[1]SEARHINFORM, **Decoding The Anatomy of Organized Cybercrime ,** Ibid.
[2] Ibid.

ثالثا: ثغرات الحوسبة الكمومية:

يؤدي لانتشار الواسع لخدمات الحوسبة السحابية لظهور ثغرات أمنية جديدة، وتعد إعدادات الحوسبة السحابية غير المهيأة على النحو الصحيح، إضافة لضوابط الوصول غير الكافية والثغرات الأمنية في البنية التحتية للحوسبة السحابية، كلها تعتبر أهدافا شائعة للعصابات الرقمية والمجرمين الالكترونيين.

ينتج أيضا عن الهجمات على الحوسبة السحابية اختراقات هائلة للبيانات واضطرابات تشغيلية، ذلك لدورها المهم الذي تلعبه في بيئات الأعمال الحديثة[1].

رابعا: إساءة استخدام تقنية البلوك تشين:

بالرغم من الترويج لهذه التقنية لما تتمتع به من مميزات أمنية، فإنها تستغل بشكل ضخم من قبل مجرمي الانترنت والعصابات الرقمية، وهذا راجع لطبيعة البلوك تشين غير القابلة للتغيير واللامركزية في الأنشطة غير القانونية، كإدارة أسواق غير مشروعة يصعب تتبعها

وغسل الأموال. وتستغل أيضا في العقود الذكية حال عدم تأمينها على النحو صحيح لتنفيذ معاملات احتيالية أو التسبب في إجراءات غير مصرح بها.[2]

خامسا: تهديدات الحوسبة الكمومية:

بالرغم من حداثتها إلا أنها تشكل تهديدات مستقبلية لمعايير التشفير الحالية، فالمرجح استغلال العصابات الرقمية لقدرات الحوسبة الكمومية لاختراق أنظمة التشفير، وهذا ما سيؤثر على العديد من إجراءات الأمان الحالية فتصبح غير فعالة، والاستعداد لتلك الاحتمالات يستدعي تطوير خوارزميات تشفير مقاومة للحوسبة الكمومية[3].

[1] Ibid, SEARHINFORM**, Decoding The Anatomy of Organized Cybercrime .**
[2] Ibid.
[3] Ibid.

الفرع الثاني: الهجمات الالكترونية للعصابات الرقمية.

أولا: البرمجيات الخبيثة:

هي برامج صممت خصيصا لإحداث أضرارا بفعل عمدي على المستخدم أو النظام العامل عليه، تختلف لاختلاف أهدافها وتعدد وسائلها والهدف مشترك في السلوكيات العدائية التي توجهها ضد الأنظمة والبيانات والشبكات، تطورت بشكل سريع مواكبة للتطور الحاصل في التكنولوجيا لتصبح أكثر تعقيدا، فمن بين خواصها نجد أنها سريعة الانتشار والتخفي استغلال الثغرات التقنية والاجتماعية سعيا للوصول لأهدافها[1]. من بين البرمجيات الضارة نجد:

- **الفيروسات:** برمجيات تصيب الملفات الشرعية وتنشر بنسخ بنفسها داخل الأنظمة وفي شبكات المعلومات، أو تكرار نفسها لتقوية العدوى، وقد تتكاثر وتنتشر من خلال ملفات أخرى، فتتعمد العصابات الرقمية على زجها لإحداث خلل مؤقت أو دائم داخل الملفات ونظم التشغيل المستهدفة[2].

- **الديدان:** تنتشر ذاتيا وبسرعة فائقة وخيالية دون الحاجة لتدخل بشري أو ملفات مرفقة، فعند الإصابات تنسخ وتكرر نفسها بنفسها، فتستهلك موارد بشرية خلال انتشارها، لذلك تعتبر تهديد وخطر حقيقي على مختلف الشبكات[3].

- **أحصنة طروادة:** خادعة للمستخدمين فتبدو كبرنامج أو ملف عند النظرة الأولى، وحال فتحه يثبت الخادم على الجهاز الخاص بالضحية فيسيطر عليه بلا علمه، وتحدث أضرارا في ثغرات خلفية، كالسرقة للملفات وحذفها، غير أنهم بإمكانهم تثبيت برامج خبيثة أخرى على الجهاز تمكنهم من التصرف بأريحية داخله[4].

- **برامج الفدية:** تشفر بيانات المستخدم وتطالب بالفدية لفك التشفير[5].

---

[1] جميل حسين طويله، **البرمجيات الخبيثة**، د.ط، سوريا، 2015، ص10، في: https://www.scribd.com/document/551801151/، اطلع عليه بتاريخ 2026/04/25، الساعة23:52.

[2] جميل حسين طويلة، مرجع سابق، ص74.

[3] المرجع نفسه، ص11.

[4] المرجع نفسه، ص ص11، 10.

[5] إسماعيل أمحمد، عبد الحليم زوبير، **دور التكنولوجيا الحديثة في ارتكاب الجرائم الالكترونية وسبل مكافحتها**، مذكرة لنيل شهادة الماستر في القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة غرداية، 2025، ص40.

– **برامج التجسس:** تراقب نشاطات المستخدمين دون علمهم، يتم استخدامها لجمع البيانات والمعلومات وكلمات المرور والملفات الحساسة[1].

– **برامج التعدين غير الشرعي:** تستغل موارد الضحية في أجهزته وذلك حتى تعدن العملات الرقمية بطرق غير مشروعة وبلا موافقة منه.[2]

ثانيا: سرقة كلمات مرور المستخدمين للتسلل في الأنظمة:

يتم الحصول على معلومات اتصال المستخدمين الشرعيين بطرق النفاذ فير المشروعة للأنظمة وتكون كالتالي:

– **التخمين:** فيقوم مجرمي العصابات الرقمية بالتفكير في كلمة المرور التي قد تكون اسم المستعمل او اسم زوجته وأطفاله، أو تواريخ مواليدهم، إذ أن الحساب يكون غير محمي أصلا فيسهل عملية السرقة للبيانات.

– **الخداع (الهندسة الاجتماعية):** يكون المسؤول عن عمليات السرقة ذا مظهر لائق ورسمي يتبادر لذهن الضحية انه مسؤول مهم، مما يجعله تحت الدهشة النفسية فينصاع له ويعطيه كلمة المرور الخاصة به تحت أي ذريعة أو سبب تقني كان.

– **الاستماع إلى حركة المرور:** يقوم المهاجم باعتراض بيانات المستخدم التي تكون غير مشفرة والمرسلة للشبكات المختلفة عبر بروتوكولات الاتصال، فيستمع لتلك الحركات عبر التلصص والترصد له.

– **النفاذ للملفات:** يتجسس المجرم الالكتروني على ملفات تخزين المستخدمين لكلمات مرورهم المرسلة والمفسرة، فيسطو عليها، وينشط وسائل التسجيل على معلمات اتصالهم.[3]

يصبح من السهل التسلل للأنظمة والقراءة للمعلومات والكتابات بإضافة مختلف البيانات، ذلك بعد الحصول على المعلومات المركبة لاسم المستعمل فيتم الولوج والنفاذ لمختلف التطبيقات، أما لتفادي انكشاف أمر العصابات الرقمية المتسللة فيقومون بتتبع أثارهم لعدم ترك دلائل تكشف وتفضح عملياتهم التطفلية.

[1] إسماعيل أمحمد، عبد الحليم زوبير، مرجع سابق، ص40.

[2] المرجع نفسه، ص40.

[3] عبد الحميد علي، **مكافحة الجرائم الالكترونية: بين نظم المعلومات والإعلام البديل**، الإسكندرية: مكتبة الوفاء القانونية، ط02، 2024، ص ص158، 157.

ثالثا: الهجمات الطمسية:

يتم شن هجوم الطمس باستبدال صفحات الويب الخاصة بالضحية بصفحات أخرى، فتكون تلك الصفحات معتمدة على محتويات جديدة ببواعث المتسلل قد تكون سياسية مثلا. منوعات هذا الهجوم تكون بإعادة توجيه المستعملين إلى "موقع شبكي شرك" يطابق المواقع التي يستخدمها المستخدمين قبلا، بعد أن يطلب منهم إفشاء معلوماتهم المتعلقة ببطاقات ائتمانهم الخاصة، عن طرق شن هجمات إستراتيجية لاصطيادهم[1].

يمكن طمس محتوى المواقع الشبكية بهدف التضليل عن طريق التأثير في الوقائع وبث الغموض بتشتيت اليقين والتلاعب بالرأي العام، هذه الهجمات تقع في فئة الحرب المعلوماتية لما لها من دلالات سيمانطيقية تعمل على قلب موازين والمحتوى المعلوماتي في معناه.

رابعا: الهجمات على البنية التحتية:

تجدر تكنولوجيات الانترنت يعرض البنى التحتية الرئيسية للمجتمعات سواء كانت إمدادات كهربائية، أو للمياه، النقل والاتصالات، الصرف الصحي... فتصبح نفاذة عن طريق "شبكة الشبكات".

إن تعقد واتساع نطاق العلاقات مع البنى التحتية المختلفة والحرجة يمثل نقطة قوة من جهة، كما يمكن تعرضها للخطر عن طريقها، لذلك من الضروري تأمين بوابات التشغيل بين شبكات الانترنت وشبكات تشغيل البنى التحتية، بإنشاء هيئات إقليمية ووطنية تسهر على حمايتها وتشرف على تنسيق وتصميم وصيانة الخطط الدفاعية للحماية. في الطوارئ يكون التخطيط واتحاد الحلول الاستباقية المنظمة والمتماسكة والمنسقة يكون ضروري لتجنب الكوارث التي قد تقع وتضر بالبنى الأساسية[2].

[1] عبد الحميد علي، مرجع سابق، ص159.

[2] المرجع نفسه، ص163.

خامسا: هجمات الحرمان من الخدمة:

تتم هذه الهجمات من خلال إغراق المواقع بسيل من البيانات غير اللازمة، ترسل عبر برامج متخصصة لنشر تلك الهجمات، مما يحدث بطء في الخدمات وازدحاما على تلك المواقع، مما يصعب الوصول لها من طرف المستخدمين[1].

المطلب الرابع: دوافع العصابات الرقمية.

تقدم تكنولوجيا المعلومات والاتصالات أصبح يشكل تهديدا متزايدا على الأفراد والدول على حد سواء، حيث أن العصابات الرقمية قد تجاوزت حدود الجرائم التقليدية، فاتسمت بدوافع وأسباب خاصة مما يجعلهم يميلون لممارسة شتى الجرائم المعلوماتية عبر استغلال المنصات الرقمية والثغرات النظامية. يهدف هذا المطلب لتحليل هذه الدوافع في ضوء التغيرات التكنولوجية، وتأثيرها في تشكيل السلوك الإجرامي الرقمي واستراتيجيات المكافحة القانونية والأمنية.

الفرع الأول: الدوافع الشخصية.

تختلف الدوافع الشخصية في العصابات الرقمية عن نظيرتها التقليدية و ذلك بسبب الوساطة التكنولوجية التي توفر مسافة نفسية و انفصالا عاطفيا عن الضحية، و يمكن تصنيف هذه الدوافع كالتالي:

أولا: دوافع سيكولوجية ومعرفية.

1- تراكم أحقاد دفينة وضغائن، والرغبة العارمة لتدمير ممتلكات الغير أو تخريبها، ذلك تحقيقا للنوازع غير المتزنة لدى المؤسسات أو النظم الحاكمة أو الأفراد[2].

2- وجود تحدي تقنى بين أفراد العصابات الرقمية، أو ادعاء إدارة نظام معلوماتي امتلاكها لنظام امني محكم لا يخترق، فيتهافت الكثيرون لإثبات العكس بتجاوز جدارها الأمني، وان نظامها يحتوي على ثغرات رقمية تمكن من الولوج واختراقه[3].

---

[1] خالد وليد محمود، "الهجمات عبر الانترنت: ساحة الصراع الالكتروني الجديدة"، **المركز العربي للأبحاث ودراسة السياسات**، الدوحة قطر، سبتمبر 2013، ص09.

[2] حسن مظفر الرزو، **الفضاء المعلوماتي**، لبنان: مركز الدراسات الوحدة العربية، د.ط، 2007، ص31.

[3] المرجع نفسه، ص31.

3- جلب الأضواء لأشخاصهم باللجوء لحماقات يرتكبونها من خلال إظهارهم لقدراتهم في اختراق الأنظمة للغير، حتى يلفتون أنظارهم لهم وإقناعهم بعلو مكانتهم وما يمتلكونه من مواهب.

4-اكتشاف الغموض والفضول للوصول لما هو محظور، هي مزايا في ذات الإنسان البشرية التي تكبر معه فتجعله يسعى أكثر وراءها[1].

ثانيا: الإطراء الغير مشروع.

الإغراءات المادية التي تعرضها الحكومات والمؤسسات والشركات وحتى الإفراد، للتشجيع على الحصول على بيانات ومعلومات سرية من نظام معلوماتي، في الخفاء تكون غايات سياسية أو تقنية أو اقتصادية صرفة.

الفرع الثاني: الدوافع خارجية.

إدا كانت الدوافع الشخصية تمثل البواعث النفسية والذاتية الكامنة في شخصية الجاني، فإن الدوافع الخارجية تُشير إلى مجموعة العوامل البيئية والسياقية والبنيوية التي تُهيِّئ الظروف الموضوعية لنشوء العصابات الرقمية واستمرارها وتوسُّع نشاطها، وهي:

أولا: الفجوات الاقتصادية والتهميش

تُشكِل الاختلالات الاقتصادية الهيكلية أرضية خصبة لاستقطاب الأفراد نحو العصابات الرقمية، وتتجلى في صور متعددة:

ثانيا: البطالة التقنية المُقنَّعة

يُعاني كثير من الكفاءات التقنية في الدول النامية من محدودية الفرص الوظيفية المشروعة التي تتناسب مع مؤهلاتهم، مما يدفع بعضهم إلى توظيف قدراتهم في الاقتصاد الإجرامي، ويُفرز هذا الواقع ما يُصطلح عليه بـ"هجرة المواهب نحو الإجرام.(Criminal Brain Drain) "

ثالثا: الأزمات الاقتصادية الدورية

تُثبت الدراسات الإحصائية وجود علاقة ارتباطية بين الأزمات الاقتصادية وارتفاع معدلات الجريمة السيبرانية المنظمة[4]. فالأزمة المالية العالمية (2008) والجائحة الصحية (2020) شهدتا تصاعداً ملحوظاً في نشاط العصابات الرقمية.

[1] حسن مظفر الرزو، مرجع سابق، ص32.

إضافة إلى أغراض سياسية تستهدف الأنشطة الاستخباراتية بشكل مباشر إما ضد مؤسسات في بلاد عدة أو ضد أنظمة أخرى، فتقوم عصابات رقمية بعمليات الاختراق لكسب لقمة العيش من عمليات القرصنة والاختراقات المعلوماتية[1].

المبحث الثاني: الأنشطة الإجرامية التي تمارسها العصابات الرقمية.

تمتاز الأنشطة الإجرامية بأنها مجموعة أفعال ومحاولات غير مشروعة تكون ضارة بهدف اختراق أو تعطيل أو سرقة بيانات من الأنظمة المعلوماتية والشبكات والأجهزة الرقمية، تعتمد العصابات الرقمية على تقنيات وبرمجيات ترتكز على الحيلة للوصول لمعلومات مختلف الأجهزة، وتنوعت هذه الأنشطة في العصر الرقمي الحديث لتتوسع في شمولها للأفراد والمؤسسات والشركات، فتتعد أنواعها وتختلف أساليبها حسب الأهداف التي تسعى لها العصابات الرقمية، فمنها الهجمات الواقعة على الأموال، والواقعة على الأشخاص، والواقعة على الشبكات الالكترونية، أو الواقعة على امن الدولة، فيما يلي سنبرز أهم تلك الأنشطة.

المطلب الأول: الهجمات الواقعة على الأموال.

تحولت الهجمات على الأموال من الجرائم التقليدية إلى أشكال الكترونية متطورة تهدد الأمن المالي العالمي، وغالبا ما تقوم بها عصابات رقمية منظمة تسيطر على الشبكات العالمية، إذ استثمرت الفضاء السيبيراني لإعادة إنتاج أنماط في قوالب تقنية بالغة التعقيد، فهي تستهدف أموالا مصرفية أو الكترونية التي يسهل التطبيق عليها إما بالتصيد الاحتيالي أو الاحتيال عبر الانترنت، أو الاحتيال باستخدام بطاقات الائتمان عبر الانترنت أو السرقة، تقوم على أساس خرق ثقة الضحية بآليات يصعب كشفها وتتبعها، وفيما يلي سنتطرق لأبرز تلك الهجمات.

الفرع الأول: الاحتيال باستخدام بطاقات الائتمان عبر الانترنت.

يهدف احتيال الانترنت في الغالب وبصورة اعتيادية للاحتيال على المستخدمين بسلب أموالهم أو سرقة أرقام بطاقات ائتمانهم أو بجعلهم يقومون بإرسال حوالات مالية أو شيكات، وتختلف الأغراض لبعتها فقد تكون بدافع شخصي من الضحية للشراء عبر الانترنت، أو من خلال دفعهم للكشف عن معلومات شخصية لأغراض التجسس، وإلا للحصول على معلومات تتعلق بحساباتهم في مراكز حساسة.

[1] حسن مظفر الرزو، مرجع سابق، ص32.

يمكن تعريف احتيال بطاقات الائتمان على انه قيام العصابات الرقمية بخداع شخص أو مجموعة أشخاص لسرقة معلوماتهم عبر الاستخدام غير المشرع وغير المصرح ببيانات ومعلومات البطاقات الائتمانية[1].

يمكن أن يقوم بالاحتيالي الالكتروني صاحب البطاقة الشرعي من خلال إساءته لاستخدام البطاقة الائتمانية في الأوقات المصرح بها، إما بدفعه لأسعار السلع ومختلف الخدمات عبر الشبكات الالكترونية ويقوم بملء الاستمارة وهو يعلم يقينا أن رصيده ناقص ولا يكفي لتغطية معاملاته، أو يحول الرصيد الخاص به لبنك أخر وهو يعلم بتجاوز المبلغ لرصيده الأصلي[2].

كما يمكن أن يتم الغش عبر البطاقات الائتمانية باستخدامها بعد انتهائها أو إلغائها، فقد يلغيها البنك لسوء استغلالها أثناء مدة صلاحيتها من قبل العميل فيعيدها للبنك، الذي بدوره قد يستمر بالعمل بها وعقد صفقات ائتمانية وهمية بعد سحب خدماتها.

يتم التزوير ببطاقات الائتمان بعد خلق بيانات وأرقام بطاقات ائتمان تخص بنك معين باستخدام برامج التشغيل الخاصة وتزويدها بالرقم الخاص بالبنك[3].

الفرع الثاني: التصيد الاحتيالي الالكتروني.

يعتبر التصيد الاحتيالي أكثر الهجمات التي تقوم بها العصابات الرقمية، فهو يعتمد على استخدام رسائل أو مواقع الكترونية مزيفة لتبدو شرعية لحد بعيد، وتكون مصممة بعناية فائقة.

يعتمد التصيد الاحتيالي على خداع الأشخاص للحصول على معلومات سرية وشخصية خاصة بهم، مثل كلمات المرور وأرقام الحسابات المصرفية وبطاقات الائتمان، فيتم التوصل للضحايا والتواصل معهم من خلال البريد الالكتروني والرسائل النصية والوسائط الاجتماعية، فتنتحل العصابات الرقمية ادوار ومكانة الجهات الرسمية فتتعامل معهم على أساس أنها جهة مصرفية أو شركة هاتف أو أي هيئة أخرى، فيطلبون من الأشخاص تزويدهم بمختلف المعلومات الشخصية بتعبئتهم لاستمارات يرسلونها لهم

[1] جاسم محمد جندل، **الجرائم الالكترونية**، الأردن: دار المعتز للنشر والتوزيع، ط01، 2022، ص ص116، 115.

[2] صفيان بخدة، ناصر وقاص، " الطبيعة القانونية لجرائم المستحدثة ووسائل ارتكابها جريمة الانترنت كنموذج "، **مجلة البحوث القانونية والسياسية**، م03، ع16، أفريل2021، ص132.

[3] المرجع نفسه، ص133.

على أساس الربح بجوائز، أو ادعائهم انه تم السطو على حساباتهم الخاصة بأعمال غير قانونية وأنهم سيوفرون كامل طرق المساعدة بذلك ينجزون مهمتهم ويحصلون على البيانات وتتم السرقة عبر التصيد[1].

الفرع الثالث: الاحتيال عبر الانترنت.

تقوم العصابات الرقمية بوهم الجنات بوجود مشروع كاذب وإحداث الأمل لهم بالأرباح بتسليمهم المال بالطريق المعلوماتي أو بتصرفهم فيه، مع علم العصابات الرقمية انه ليس لها سلطة وصفة التصرف في الأموال باتخاذها اسم وصفة كاذبة، حيث تمكنهم من الاستيلاء على الأموال وتحويلها الكترونيا بالاتصال بالجنات عبر الشبكة أو بالتعامل مباشرة ببيانات الحاسب أي بالانترنت[2].

يتم الاحتيال عبر الانترنت عبر الوسائط المختلفة مثل المواقع الالكترونية والبريد الالكتروني ذلك لتحقيق أرباح مالية عبر الاحتيال، وتتعدد أشكاله فمن أهمها بيع سلع وهمية أو سرقة معلومات البطاقات الائتمانية واستخدامها، أو بتوجيه المستخدم بغرض التحايل عليه لموقع خاطئ، أو بالاصطياد الاحتيالي عن طريق خداعهم للحصول على معلوماتهم واستخدامه بغرض كسب مالي[3].

المطلب الثاني: الهجمات الواقعة على الأشخاص.

ظهور العالم الافتراضي شكل خطرا على الحياة الخاصة للأشخاص مما أصبح يهدد سلامتهم عبر الشبكات الالكترونية، مما دفع بالعصابات الرقمية لاستغلال هذه الأزمات من خلال قيامهم بالعديد من الأنشطة الإجرامية كالتهديد والمضايقات الشخصية، وحتى الابتزاز الالكتروني حول المعلومات، وسرقة الهوية وانتحال شخصيات الغير، فيما يلي سنفصل في مختلف الهجمات التي تقع على الأشخاص.

الفرع الأول: الابتزاز الالكتروني.

يكون الابتزاز من خلال تعرض موقع الكتروني أو خادم بريد الكتروني أو نظام حاسوب لمجموعة هجمات متكررة يقوم بها العصابات الرقمية الذين يطالبون بمبالغ مالية ضخمة مقابل توقيت تلك الهجمات[4].

[1] جاسم محمد جندل، مرجع سابق، ص ص122، 121.

[2] صفيان بخدة، ناصر وقاص، مرجع سابق، ص131.

[3] جاسم محمد جندل، مرجع سابق، ص155.

[4] المرجع نفسه، ص42.

تغرق هجمات الحرمان من الخدمة المواقع الالكترونية بالكثير من الطلبات لتصبح غير قادرة على الرد لتلبية المتطلبات الخاصة بالزبائن، إضافة لهجمات رانسوموير التي تقوم العصابات الرقمية فيها بعمليات التشفير لمختلف المواقع الالكترونية والملفات ولا يتم فك التشفير إلا بعد دفع مبالغ مالية مقابل تلك الخدمة[1].
تتعد إشكال الابتزاز الالكتروني حسب الأهداف المسطر تحقيقها فنجد:

أولا: ابتزاز الكتروني عاطفي:

تقوم به العصابات الرقمية بعد جمعها للمعلومات الكافية عن الأشخاص المراد ابتزازهم عاطفيا لتحقيق أهداف معينة قد تم تحديدها من الأول، إضافة لتحديد الطرق حتى يتم تنفيذ الإيقاع في الشرك، وذلك مع أخذ الحيطة والحذر التام من كشف أمورهم، ويتم هذا النوع من الابتزاز من خلال الإساءة للضحايا لجعلهم يرضخون لأمورهم المفروضة عليهم عبر مختلف المواقع الشهيرة كشبكات التواصل الاجتماعي "فيسبوك" و"تويتر" و"انستقرام" وغيرها من الشبكات. المعلومات التي تستخدم للابتزاز تكون العصابات الرقمية قد جمعتها بالتواصل الدائم والبحث الجيد في شخصية الضحية والتقصي للمعلومات الخاصة والبيانات المهمة التي تكون مصدر الثقة لديهم لشن هجوم الابتزاز على الضحايا[2].

ثانيا: ابتزاز الكتروني مهني:

يكون حال الضحية تابع للعصابات الرقمية أي عضو فيها، فيمتلكون كافة المعلومات الخاصة به لجعله يدخل في حالة هلع وتوتر مما هو قادم، قد تكون الأهداف المراد تحقيقها هي ساعات عمل إضافية له أو للتخلي عن تحفيزات مالية، وإلا كان جزاءه هو فضح وكشف أسراره الخاصة إما متعلقة بالعمل الإجرامي أو بالحياة الخاصة[3].

ثالثا: ابتزاز الكتروني سياسي:

الأهداف التي تسعى لتحقيقها العصابات الرقمية هنا هي مكاسب سياسة، بالبحث في الهفوات والأخطاء السياسية الواقع فيها الضحية لاستعمالها ضده وعند رفض الاستجابة يتم تهديده بكشف أموره إما

[1] صادق حطابي، مرجع سابق، ص469.

[2] سعيد زيوش، "ظاهر الابتزاز الالكتروني وأساليب الوقاية منها–قراءة سوسيولوجية وأراء نظرية– "، **مجلة العلوم الاجتماعية**، د.م، ع22، جانفي2017، ص72.

[3] المرجع نفسه، ص ص73، 72.

في مواقع انترنت عامة أو خاصة، وحتى اللجوء لإنشاء مواقع بأسماء مستعارة ونشر وثائقه المزورة وأخطائه التي تهدم مسيرته السياسية وتؤثر على حياته ونفسيته الاجتماعية[1].

رابعا: ابتزاز الكتروني مادي:

تحقيق المنفعة المادية هي الغاية المرجوة منه بالربح المادي وكسب مبالغ ضخمة لصالح العصابات الرقمية بإيهام الضحايا بفضح حقائقهم الشخصية، باستخدام برامج لتحسين وتعديل الصور الشخصية للضحية بصور إباحية أو مخلة بالحياء ذلك لتهديده للرضوخ والانصياع لطلباتهم، والرفض لها يؤدي لنشرها عبر شبكات التواصل والمواقع[2].

الفرع الثاني: سرقة الهوية.

تتم سرقة الهوية من طرف العصابات الرقمية بالاستيلاء على المعلومات الشخصية ذات الطابع الحساس للأشخاص ثم بشكل غير مشروع تنتحل شخصياتهم، الهدف من تلك السرقات هي الوصول للاسم الكامل للضحايا، أرقام الهوية والأرقام الوطنية، بيانات تخص الحسابات المصرفية، أرقام بطاقات الائتمان، كلمات المرور والمعلومات الصحية والوظيفية عند الحاجة[3].

عند إصابة جهاز الحاسب الآلي بإحدى البرامج الضارة والخبيثة يتم تقنيا البحث عن البيانات الشخصية للضحية كالاسم والعنوان ورقم الهاتف ومكان الميلاد ورقم بطاقة الهوية وأرقام بطاقات الائتمان...، ذلك لاستخدامها في انتحال الهوية بتزوير شهادات الميلاد وكشوف حسابات البنوك المصرفية وبطاقات الهوية، كل هذا لتحقيق مكاسب والقيام بأعمال غير قانونية تتصف بالأفعال الإجرامية باسم الضحية[4].

يتم التصرف بمعلومات الضحية باستخدام بيانات البطاقات الائتمانية لسحب أموال وطلب مشتريات، وكلمات السر التي قد تكون تاريخ الميلاد للقيام باختراق حسابات الضحايا من مواقع التواصل الاجتماعي والبريد الالكتروني، فتح حسابات بقروض بنكية جديدة مستغلين أسماء الضحايا بلا إذن ولا علمه[5].

---

[1] سعيد زيوش، مرجع سابق، ص73.

[2] المرجع نفسه، ص73.

[3] فهد قطينة، **الأمن السيبيراني: تعلم الأمن السيبيراني من الصفر حتى الاحتراف**، أكاديمية الأمن السيبيراني، ط01، 2025، ص92، https://www.ktobati.com/book/، اطلع عليه بتاريخ 2026/04/22، الساعة21:50.

[4] جاسم محمد جندل، مرجع سابق، ص 154.

[5] فهد قطينة، مرجع سابق، ص91.

وعليه فخطورة سرقة الهوية ترتب أضرارا طويلة الأثر ومعقدة وتكون أليمة للأفراد، فالضحايا لا يكتشفون العواقب إلا حين وصول فواتير أو إشعارات بالعمليات الاحتيالية الانتحالية التي لم يقوموا بها أصلا، وتعرض سمعتهم للتشويه.

الفرع الثالث: الملاحقة والتشهير الالكترونية.

تمارس العصابات الرقمية المضايقة والملاحقة الالكترونية على ضحاياها باستخدام البريد الالكتروني ووسائل الحوارات الآنية على الشبكات الالكترونية، تكون الملاحقة ببعث رسائل تخويف ومضايقات للضحايا، إذ أن أهدافهم مسطرة ومرسومة من بداية التخطيط للعمليات للرغبة بالتحكم في الضحايا، فتمتاز الملاحقة بإخفاء هوية المرتكبين وتعدد وسائلها كونها لا تتطلب اتصال مادي مع الضحية، لان القصد من المضايقات هي خلق التذمر والسلبية في نفس الضحية فيطبق طلبات العصابات الرقمية[1].

أما التشهير فتقوم العصابات الرقمية بنشر معلومات تمتاز بالسرية وتكون مغلوطة ومضللة على الضحايا، ويختلفون بين الأفراد والمجتمعات والمؤسسات التجارية كانت أم سياسية، وتتعدد الوسائل المستخدمة فيه كإنشاء مواقع على الشبكات تتضمن المعلومات المراد نشرها، أو إرسال المعلومات عبر القوائم البريدية لمستخدمين كثر، يمكن أن تضاف للتشهير عمليات تشويه السمعة ونشر الشائعات والأخبار الكاذبة عن الضحايا[2].

المطلب الثالث: الهجمات الواقعة على الشبكات الالكترونية.

تشكل الشبكات الالكترونية العمود الفقري للبنية التحتية الرقمية المعاصرة، مما جعلها هدفا استراتيجيا للعصابات الرقمية التي تستهدف سريتها وسلامتها وتوافرها، يتمحور هذا المطلب حول أبرز أنماط الهجمات الواقعة على الشبكات، والمتمثلة في هجمات الاختراق التي تستهدف تجاوز نظم الحماية للوصول غير المشروع للبيانات، وهجمات التجسس الالكتروني الرامية لاعتراض الاتصالات واستنزاف المعلومات الحساسة بصورة خفية، فضلا عن الهجمات الماسة بالتوقيع الالكتروني باعتباره الركيزة في إضفاء الحجية القانونية على المعاملات الرقمية، تكتسي هذه الهجمات خطورة بالغة إذ تتجاوز آثارها المساس الفردي إلى تهديد الأمن القومي والاقتصادي للدول.

[1] صفيان بخدة، ناصر وقاص، مرجع سابق، ص ص136، 135.

[2] المرجع نفسه، ص ص137، 136.

الفرع الأول: هجمات الاختراق.

تتم تلك الهجمات بالدخول غير المصرح به وغير المشروع للأنظمة الآلية بتجاوز أنظمة التامين الخاصة[1] بها، قد يكون هدف الاختراق هو الاطلاع على المعلومات الالكترونية فقط بصورة غير مشروعة، إما حذف البيانات والمعلومات إما نسخها أو الإضافة لها أو نشرها أو تعديل أي بيانات أو معلومات على النظام الالكتروني[2].

يكون الاختراق كامل إذا تمكنت العصابات الرقمية من السيطرة بشكل كامل على الحاسب الآلي وتقوم بإحداث تغييرات في البيانات، أو تبديلها أو الزرع فيها برامج خبيثة داخل الأجهزة الالكترونية، أما في بعض الحالات يستخدمون الحاسب الآلي المخترق من قبل كأداة لشن هجمات الكترونية أخرى على باقي الأجهزة، وحال ارتباط الشبكات هنا تكون المهمة في التخطيط بالبحث عن معلومات على النظام والشبكة التي تم وضعهم كهدف للاختراق والتعرف على كل ما هو متعلق بهم من أنظمة التامين والتشغيل الخاصة بهم لفك شفراتهم واستغلال ثغراتهم حتى يتوصلوا لاختراقها[3].

تتعد وسائل الاختراق فهناك الاختراق الالكتروني بواسطة الحاسوب والشبكة الالكترونية، أو بواسطة الهاتف أو بواسطة الأقمار الصناعية، أو عبر البريد الالكتروني، سنندرج فيهم فيما يلي:

أولا: الاختراق الالكتروني بواسطة الحاسوب والشبكة الالكترونية:

يعد ابسط الأنواع وهو أكثرهم انتشارا ومعرفة في الوسط الرقمي، تستخدم فيه العصابات الرقمية برامج مختلفة إما على أساس العميل أو الخادم، على أن يشترط في برنامج الخادم عمله في نظام الهدف لتقوم العصابات الرقمية بعد ذلك بالاتصال بواسطة برنامج العميل لتباشر عمليات الاختراق، وهذا النوع يكون في الحواسيب الشخصية[4].

[1] جاسم محمد جندل، مرجع سابق، ص154.

[2] عبد الله ذيب محمود، أسامة إسماعيل دراج، **الوجيز في الجرائم الالكترونية القواعد الموضوعية والإجرائية**، الأردن: دار الثقافة للنشر والتوزيع، ط01، 2022، ص155.

[3] جاسم محمد جندل، مرجع سابق، ص155.

[4] عبد الله ذيب جندل، أسامة إسماعيل دراج، مرجع سابق، ص107.

ثانيا: الاختراق الالكتروني بواسطة الهاتف:

امتدت هذه الأنشطة الهجومية لتشمل أجهزة الهاتف الحديثة والاتصالات، مخترقة نظام الحاسوب كما ذكرنا سابقة لتمتد للهواتف الذكية، فاعتمدت العصابات الرقمية على استغلال الهواتف النقالة الحديثة لما تحتويه على خصائص وبرمجيات متطورة في الوقت الراهن مواكبة للتطور الرقمي، فيمكن لهم التصنت على المحادثات بواسطة الهاتف المرتبط بالشبكة الالكترونية والذي يكون موضوع في غرفة مثلا، وحتى فتح الكاميرات الخاصة بالهواتف والتجسس على حامله وذلك كله بلا علم صاحبها[1].

ثالثا: الاختراق الالكتروني بواسطة الأقمار الصناعية وطائرات التصنت والمراقبة:

يكون هذا الاختراق دولي باستخدام أجهزة نادرة التوفر للمواطن العادي كونها تقتصر على السلطات الحاكمة فقط، والاختراق عبر الأقمار الصناعية تقوم به العصابات الرقمية بالتصرف مع جماعات لها كيان في السلطة حال وجود جاسوس بها، بغرض السيطرة على كافة البيانات في العالم وهو اخطر الاختراقات على الإطلاق[2].

رابعا: الاختراق الالكتروني بواسطة البريد الالكتروني وبرامج المحادثات الفورية:

أصبحت وسائل التواصل الاجتماعي (الفيس بوك، ماسينجر، الواتس آب، انستقرام، ...) والبريد الالكتروني من الضروريات العملية للقيام بالاتصالات الفورية، تنتشر عند اغلب المستخدمين والاختراقات تحدث في الغالب عبرها، مثل البريد الالكتروني بإرسال ملفات مرفقة ضمن رسائل عادية من الخارج أما مضمونها مشفر للاختراق بمجرد فتحها والدخول لها يتم الولوج لكافة ملفات ذلك الجهاز وتتبع حركاته عبر حساباته المتنوعة ومختلف أنشطته[3].

الفرع الثاني: التجسس الالكتروني.

تكون هجمات التجسس الالكتروني عبر التصنت والتجسس على مختلف أجهزة الحواسيب باعتراض المراسلات الالكترونية، ويتم ذلك بعد تثبيت برامج التجسس التي تكون معرفة بأنها برامج مصممة لجمع البيانات من الحواسيب، وهي تقوم بإعادة توجيهها لأطراف أخرى دون موافقة وعلم المستخدم، وعمليات

[1] عبد الله ذيب جندل، أسامة إسماعيل دراج، مرجع سابق، ص108.

[2] المرجع نفسه، ص109.

[3] المرجع نفسه، ص109.

جمع المعلومات تشمل جمع البيانات السرية وكلمات المرور وأرقام بطاقات الائتمان كذلك مراقبة ضغطات لوحة المفاتيح، تعقب الاستعراضات وجمع عناوين البريد الالكتروني، ومن إضرار التجسس نجد بطئ في الشبكة وأدائها وتعريض العمليات التجارية للعرقلة.

برامج التجسس تنقسم لأربعة أصناف على أساس الأهمية وهي: أحصنة طروادة، ثم برامج الإعلانات المتسللة، ثم ملفات تعريف الارتباط للتعقب، ثم برامج مراقبة النظام في الأخير[1].

غيرت التطورات التكنولوجية من عمليات التجسس بتوفر الآليات التكنولوجية والانترنت عمليات التجسس، فنجد الولايات المتحدة الأمريكية في قمة قائمة الدول التي تعرضت لهجمات التجسس في النصف الأول من عام 2005 م حيث بلغت 12 مليون هجوم الكتروني لأغراض التجسس، ثم تليها نيوزيلندا ثانيا في نفس العام ب 1,2 مليون هجوم، ثم الصين بمليون هجوم خلال نفس السنة. أما عام 2009م فقد تم الكشف عن وجود شبكة تجسس تستهدف اختراق المؤسسات والوزارات الحكومية والشركات والأهداف الإستراتيجية للعديد من الدول كالهند وإيران وجنوب إفريقيا وألمانيا وباكستان، وليست تلك الدول فقط محل الهجمات بل تمتد هجماتهم إلى الشركات التجارية والإعلانية ومختلف المنظمات الأخرى[2].

الفرع الثالث: التوقيع الالكتروني.

يعرف التوقيع الالكتروني بأنه بيانات الكترونية مضافة أو ملحقة أو مرتبطة بمعاملة الكترونية، يكون لها طابع يسمح بتحديد هوية الشخص الموقع عليها ويجعل له ميزة تحقق الموافقة على مضمون المعاملات[3].

كما عرفته منظمة الآونسيترال[4] بأنه:" مجموعة بيانات تكون في شكل الكتروني تدرج في رسالة بيانات او تضاف إليها أو مرتبطة بها منطقيا، ويجوز استخدامها لتعيين هوية الموقع لرسالة بيانات لتبيان الموافقة على المعلومات الواردة فيها".

---

[1] لمياء زواوي، فهيم رملي، "التهديدات السيبيرانية وأمن المجتمع الرقمي: دراسة حالة الجزائر"، **المجلة الجزائرية للأمن والتنمية**، م12، ع02، أفريل2023، ص151.

[2] جاسم محمد جندل، مرجع سابق، ص ص116، 115.

[3] عبد الله ذيب محمود، أسامة إسماعيل دراج، مرجع سابق، ص130.

[4] منظمة الآونسيترال: هي الهيئة القانونية التابعة لمنظومة الأمم المتحدة في مجال القانون التجاري الدولي. وهي هيئة قانونية ذات عضوية عالمية متخصصة في إصلاح القانون التجاري على النطاق العالمي منذ ما يزيد على 50سنة، مهمتها عصرنة ومواكبة القواعد المتعلقة بالأعمال التجارية الدولية.

وعليه فان التوقيع الالكتروني هو مجموعة حروف، أرقام، رموز، إشارات لها طابع مميز ومنفرد، أو تعبير شخصي عن الإرادة المنفردة بالالتزام بتصرفات معينة تسمح بتمييزه على أنه الشخص الموقع ويتم اعتماد توقيعه من الجهات المختصة.

كون أن التوقيع الالكتروني يكون في فضاء رقمي فهو متعدد الصور منها:

أولا: تحويل التوقيع العادي لتوقيع الكتروني عبر جهاز الماسح الضوئي:

يتم تحويل التوقيع التقليدي لتوقيع الكتروني عند نقل صاحبه لتوقيعه اليدوي عبر جهاز الماسح الضوئي الذي يقوم بتصويره ونقله لأجهزة الحاسوب، وبذلك يصبح قابل للاستعمال الالكتروني واعتماده في الوثائق الالكترونية، غير أنه طريقة لكثرة سهولتها فهي تستعمل من قبل أي شخص فتكون غير قانونية، وهذا ما تلجأ له العصابات الرقمية عادة لتزوير وتزييف التوقيعات الخاصة بالأفراد أو حتى المؤسسات والشركات[1].

ثانيا: التوقيع الكودي:

يكون عن طريق استخدام بطاقات ممغنطة صادرة عن البنوك وأرقام سرية، ينتشر في التعاملات البنكية عبر الصراف الآلي، وهنا يأتي دور العصابات الرقمية فتدخل هي البطاقة في جهاز الصراف ثم وضع الأرقام السرية لإتمام عمليات السرقة والنهب للأموال عن طريق التوقيع الكودي[2].

ثالثا: التوقيع البيومتري:

يعتمد هذا التوقيع على جملة الخواص الكيميائية والطبيعية للأفراد، يشمل عدسة العين حركة اليد وبصمة الإصبع، التعرف على ملامح وانحناءات الوجه، نبرات ودرجات الصوت، وتقوم العصابات الرقمية بتزييف هذه العلامات والخواص لتتمكن من الولوج لمختلف الأنظمة، وهي نظام جد امن يتطلب اختراقات وعمليات بحث دقيقة[3].

رابعا: التوقيع الرقمي:

[1] عبد الله ذيب محمود، أسامة إسماعيل دراج، مرجع سابق، ص131.

[2] المرجع نفسه، ص131.

[3] المرجع نفسه، ص131.

يعتمد هذا التوقيع على وسائل التشفير الرقمي من خلال معادلات حسابية لضمان سرية المعلومات بطرق أمنة بتحويله لمعادلة لا يمكن قراءتها إلا من طرف صاحب مفتاح الشفرة، ويقوم هذا الأخير بإرسالها فيفك الطرف المستقبل لها التشفير بمفتاح ثاني للتمكن من الحصول على المعلومات المرسلة لتظهر ما تحتويه الرسالة، حيث يجود مفتاحين الأول يكون مفتاح خاص يستعمل من طرف صاحب التوقيع الالكتروني والثاني يكون مفتاح عام يستعمله الجميع ممن وجلت لهم تلك الرسالة للتأكد من صحة التوقيع وهوية صاحبه ليثبت لهم صحة السند الالكتروني، أما العصابات الرقمية فتستغل كلا المفتاحين[1].

المطلب الرابع: الهجمات الواقعة على أمن الدولة.

في عصر العولمة الرقمية أصبحت الدول تواجه تهديدات معقدة تتجاوز الحدود الجغرافية التقليدية، حيث تحولت الشبكات الالكترونية لساحة رئيسية على أمن الدولة، هذه الهجمات تشمل الإرهاب الالكتروني والجرائم المنظمة عبر الانترنت التي تقوم بها مختلف العصابات الرقمية، فتهدد الاستقرار السياسي والاقتصادي وحتى الاجتماعي للدول، مما يستدعي استراتيجيات دفاعية تكون متطورة للتصدي لها، فهي تستهدف نقاط الضعف في البنية التحتية الرقمية والمجتمعات البشرية، في هذا المطلب سنتطرق لأبرز تلك الهجمات كالإرهاب الالكتروني و الاتجار بالبشر عبر الانترنت، الهجمات عبر تطبيقات الويب والمخدرات عبر الشبكات الالكترونية.

الفرع الأول: الاتجار بالبشر عبر الانترنت.

يعرف الاتجار بالبشر عبر الانترنت على انه: " استغلال وسائل الاتصال الالكتروني في تبادل المعلومات بخصوص الصفقات غير المشروعة والتي محلها هو بيع الإنسان حي أو استغلاله، وحتى بيع جزء من جسده أو أجزاء من مشتقاته[2]".

إذا الاتجار الالكتروني بالبشر هو إبرام صفقات تجارية عبر الوسائط الالكترونية إما بإنشاء مواقع خاصة الكترونية أو الاتصال بالضحايا باستغلال الوسائل الالكترونية، ذلك لعقد اتفاق لبيع أو شراء إنسان لاستغلاله بموافقته أو بغيرها، حتى تحقق تلك الصفقة أرباح للعصابات الرقمية، وعليه فالاتجار بالبشر عبر الانترنت يحتاج لتوفر عناصر أساسية هي:

[1] عبد الله ذيب محمود، أسامة إسماعيل دراج، مرجع سابق، ص132.

[2] نبيلة كردي، "الاتجار بالبشر عبر الانترنت "، **مجلة أبحاث**، م08، ع02، جوان2022، ص525.

السلعة: تتشكل من الإنسان سواء باستغلاله كاملا أو انتزاع جزء أو إحدى أعضائه أو مشتقاته أو منتجاته، يتوصل إليه العصابات الرقمية عن طريق جذبهم للأشخاص إما بإيهامهم بالحصول على فرص عمل أو عقد وإبرام زيجات أو تتبع أولئك الأفراد الذين ليس لهم إيواء بسبب فرارهم من الحروب في دولهم فيحتجزونهم ويتصرفون بهم حسب الحاجة[1]

الوسيط: وهي العصابات الرقمية الإجرامية تباشر عملياتها من البداية للنهاية باستخدام الوسائل التكنولوجية المتوفرة، فتمارس أعمالها عبر تخطيط منظم حيث يكون لها مقرات رئيسية وحتى الفروع موزعة وموظفين مجهزين للعمل، وفق استراتيجيات تكون طويلة الأمد بتتبع السلم الهرمي التنظيمي. تقوم العصابات الرقمية بعقد تحالفات مع المنظمات الإجرامية لتوسيع أعمالها وتوفير السلع من جهة وتحقيق أرباح اكبر[2].

السوق: هو مكان عرض السلعة(الإنسان) ويتم في الفضاء الالكتروني بالترويج للأشخاص وعرض ميزاتهم لجذب العملاء بأعلى الأسعار في مزادات تقام لمن يزيد الطلب عليهم، فالطلب هو الفاصل في ارتفاع الأسعار وانخفاضها بالنسبة للأرباح التي تحققها العصابات الرقمية[3].

شكلت الانترنت فضاء مظلما تستغله العصابات الرقمية بكل ما يحتويه من تكنولوجيا لتسيير أعمالهم وعملياتهم الإجرامية الالكترونية وتنظيمها بما يضمن سريتها من خلال اعتماد الطرق منها:

أولا: الاستخدام للمواقع الالكترونية:

يتم استخدام المواقع الالكترونية عبر الانترنت لهدفين رئيسيين، الأول لجذب الأشخاص محل الجريمة عن طريق استقدامهم من دولهم للدول التي تقع فيها العملية، أو تكون في نفس الدولة، وهذه الفئة تكون بحاجة لأمر معين فتستغل العصابات الرقمية نقطة ضعفهم التي تكون الحاجة للعمل أو الزواج أو الهروب من ظروف قاسية للبحث عن مستوى معيشي أفضل، هذا الأمر الذي يدفعهم للبحث عبر الانترنت عن غاياتهم التي توقعهم ضحية الإعلانات الكاذبة للعصابات الرقمية الإجرامية، بتوفير ظروف السفر والاستقبال المناسبة ثم يحجزونهم فور وصولهم للاستغلال لاحقا في مختلف العمليات[4].

[1] نبيلة كردي، مرجع سابق، ص525.

[2] المرجع نفسه، ص525.

[3] المرجع نفسه، ص ص526، 525.

[4] المرجع نفسه، ص ص528، 527.

أما الهدف الثاني هو فتح مواقع الكترونية تختص بالترويج للأشخاص حتى يتم استغلالهم جنسيا، فتقوم العصابات الرقمية بفتحها وتشغيلها بنفسها، كما قد تحليلها لإداريين مختصين في التشغيل مقابل عمولات نظير أعمالهم، ذلك بعرض مميزاتهم وصفاتهم من سن وجنس، أيضا المواصفات الجسدية وغيرها من الأمور الخاصة بالضحية، وعلى الراغبين فيهم المشاركة في المزاد حتى يتمكنوا من الحصول على الخدمات المطلوبة، ويكون هذا المزاد في ساعات محددة والانضمام له يكون وفق شروط تحدد مسبقا من طرف العصابات الرقمية حتى تتم العمليات بانتظام[1].

ثانيا: استخدام البريد الالكتروني:

يستعمل البريد الالكتروني لتسهيل عمليات الاتصال بين أفراد وأعضاء العصابات الرقمية وكذلك اتصالاتها مع المستخدم الضحية أو الشخص الطالب للسلعة والخدمة، يوفر البريد الالكتروني للعصابات الرقمية الأمان والخصوصية كونه يحمي الاتصالات بين العملاء ويعتمد على تقنيات مشفرة وكلمات سرية، فهم يعتمدون على الاتصالات الصامتة من خلاله إذ لا يمكن سماع محادثتهم لأنها تتم عبر الكلمات المشفرة يفهمها أعضاء العصابات فقط، لذلك لا يفهم معناها إذا كانت تتحدث عن الاتجار بالبشر لأنهم يلجئون لمختصين محنكين في مجال التشفير وتغيير عناوين البريد الالكتروني الخاصة بالعصابات الرقمية وثم تحويلها عبر الدول مما يصعب الكشف عنها وتتبعا والعثور على منفذيها[2].

ثالثا: الاستخدام للتجارة الالكترونية:

تمثل التجارة الالكترونية فضاء حيوي لعمليات الاتجار بالبشر لأن مراحلها تكون في العالم الافتراضي فتمتاز بالنعومة بغياب العنصر المادي فيسهل العمل على العصابات الرقمية للتعاقد مع العملاء، والدفع يكون باستخدام عملات مشفرة كالبيتكوين[3].

فالعصابات الرقمية باتت تمارسها أعمالها الإجرامية بسلاسة عبر الدول بلا حاجة للانتقال لموقع العملية بتوفير الوقت والجهد، فيصعب إثبات جرائمهم والتهرب منها، لأنها تكون عمليات سرية فيعيق هذا

[1] نبيلة كردي، مرجع سابق، ص128.

[2] المرجع نفسه، ص128.

[3] المرجع نفسه، ص129.

سير التحقيقات على المصالح الأمنية المختصة بمكافحة الاتجار بالبشر والأعضاء البشرية عبر الانترنت وأيضا كشف المتواطئين في تلك الجرائم[1].

تجدر الإشارة لأخطر العصابات الرقمية العالمية التي تمارس الاتجار بالبشر عبر الانترنت نجد: العصابات(المافيا)الفيتنامية، العصابات(المافيا)الروسية، العصابات(المافيا)المغربية، العصابات(المافيا)اللبنانية.

الفرع الثاني: الاتجار بالمخدرات عبر الشبكات الالكترونية.

تعتبر المخدرات الرقمية نوعا جديدا من المخدرات، إذ تعرف بأنها: "ملفات صوتية تحتوي على نغمات أحادية أو ثنائية عند الاستماع من طرف المستخدم، تجعل الدماغ يتخدر بشكل مماثل للمخدرات الحقيقة، وتلك الملفات الصوتية تصمم لتحاكي الهلوسة وحالات الانتشاء التي تصاحب المتعاطي للمخدرات، لها تأثيرات على العقل تجعله في اللاوعي بواسطة موجات صوتية غير سمعية للأذن وهي الضوضاء البيضاء[2]".

تم تعريفها أيضا بأنها: "ملفات صوتية تحمل من مواقع الانترنت تكون عالمية ومعروفة، أو برسالات بينية، تكون بها نغمات حين سماع الإنسان لها تكون بصدى يتردد على الإذن بشكل مختلف بين الاثنين، لها اثر معادل لتدخين سجائر من الحشيش وتناول جرعات من الكوكايين، كما لها نفس تأثيرات المخدرات والجنس والرعب..."[3].

وعليه يمكن تعريف المخدرات الرقمية بأنها عبارة عن سلسلة ملفات صوتية يستمع لها بأساليب مختلفة عن طريق سماعات الأذن، يؤدي السماع لها للشعور بآثار هلوسة فهي تعدل مزاج حسب الحالات العاطفية والبيولوجية للمتلقي والمستمع، أيضا تعدل التركيز والتأمل والانتباه للمستخدم كونها تعتمد على موجات صوتية متزامنة مع موجات الدماغ، لتحقق في الأخير للفرد المستمع حالة تعاطي للمخدرات تحاكي الواقعية فيصبح العقل غير متزن وغير مستقر كهرومغناطيسيا، فيصبح الجسم في حالة إفراط للإفرازات الهرمونية مثل"الدوبامين" ليعدل المزاج ويعرف باسم هرمون السعادة.

---

[1] نبيلة كردي، مرجع سابق، ص129.

[2] لامية طالة، " المخدرات الرقمية...جريمة الإدمان الجديد في الفضاء السيبيراني قراءة في التأثيرات وأساليب المواجهة "، **مجلة للدراسات الإعلامية**، م06، ع01، مارس2022، ص121.

[3] المرجع نفسه، ص122.

يعود أصل "المخدرات الرقمية" لتقنية اكتشفها العالم الألماني الفيزيائي "هاينريش ويلهيلم دوف Heinrich Wilhelm Dove" عام 1935م وأطلق عليها اسم "النقر بالأذنين"، وتم استخدامها لأول مرة عام 1970م لعلاج حالات نفسية لبعض المصابين بالاكتئاب الخفيف للمرضى الرافضين للعلاج السلوكي، حيث توصل بأنه حال تسليط ترددات وذبذبات على الأذن بأشكال مختلفة بين كلا الجهتين يؤدي ذلك لإفراز مواد منشطة كالدوبامين وبيتا أندروفين الذي يعطيان مفعول مخدر يعدل المزاج.

استخدمت الموسيقى على مستوى المستشفيات للأمراض النفسية لنقص المواد المنشطة للمزاج عند بعض المرضى النفسانيين، ذلك تحت إشراف طبي حتى لا تتجاوز ثواني أو أجزاء من الثانية ولا تستخدم لأكثر من الحالات المسموح بها وهي مرتين يوميا، وتوقف العلاج بها لغلاء تكاليفها[1].

نحن أمام جيل جديد من الإدمان يتطلب تعاطيها توفر أجواء مناسبة لها تتمثل في الانزواء في الغرف وغلق الستائر والنوافذ وإسدال الستائر وبقاء الفرد بمفرده، أيضا غلق كل الأجهزة وقطع الاتصال بالأنترنت، ووضع عصبة فوق العينين، كما تكون من خلال التمدد على السرير ومحاولة البقاء في حالة استرخاء تام، استعمال سماعات الأذن والانطلاق في رحلة تعاطي المخدر الرقمي حسب الاختيارات المناسبة لكل ظرف للفرد[2].

تتخذ العصابات الرقمية من التجارة بالمخدرات الرقمية عبر الانترنت سوقا ومقرا فعالا لبيعها والترويج لها، فتبيع الملفات الصوتية والموسيقية من خلال وسائل الاتصال كالحاسوب، الهاتف النقال، اللوحات الالكترونية، كما تروج لها بأسعار زهيدة أحيانا مع إمكانية تحميلها لأول مرة مجانا لجذب العملاء والدعاية لها، هكذا حتى يتعود عليها الأفراد ويتعاطونها كونها يتم الحصول عليها بطرق سهلة تحقق رغباتهم في المتعة، ومتاحة في أي وقت وكل مكان بعيدا عن المختصين في مكافحة هذه الظواهر، كما أن العصابات الرقمية تنتهج أسلوب تقديم خدمة العرض على المتعاملين الترويج للمخدرات الرقمية وإقناع مستهلكين جدد بها مقابل أن تدفع لهم مبالغ مالية لقاء ترويجهم أو حتى تدفع لهم عن طريق الملفات الصوتية أي بالمخدرات الرقمية نفسها[3].

[1] لامية طالة، مرجع سابق، ص122.

[2] المرجع نفسه، ص123.

[3] المرجع نفسه، ص123.

يكمن التفرق بين المخدرات الرقمية والمخدرات التقليدية من حيث الناحية العضوية المخدرات التقليدية أخطر كونها مثبتة علميا، أما من الناحية الاجتماعية فالمخدرات الرقمية اشد خطورة نظرا لعدة أسباب هي:

- سهولة الحصول على المخدر الرقمي عبر الشبكات الالكترونية.

_ تكاليفها المنخفضة في أسواق الانترنت.

- تتطلب جهاز الكتروني كالحاسوب وسماعات ذات جودة جيدة ولا يهم العمر فيها.

- انعدام الجهات والمصالح المختصة لمطاردة العصابات الرقمية ومكافحة ترويج تلك السموم السمعية[1].

الفرع الثالث: هجمات الإرهاب الالكتروني.

يهدد الإرهاب حياة الناس اليومية لما له من أضرار على الأفراد والمجتمعات البشرية، ومع التطور التقني الحديث ظهر الإرهاب الالكتروني الذي يقوم به إرهابيين الكترونيين يعرفون باسم العصابات الرقمية يستغلون الثغرات الأمنية لتلبية أهدافهم السياسية والاجتماعية بمختلف الهجمات على أجهزة الحواسيب والشبكات الالكترونية[2].

يعرف الإرهاب الالكتروني على انه ذلك العدوان أو التخويف أو التهديد المادي وحتى المعنوي الصادر عن الدول أو الجماعات أو الأفراد، مستهدين الإنسان في دينه أو عرضه أو ماله بغير وجه حق مستخدمين وسائل الكترونية وموارد معلوماتية في ذلك[3].

تعتمد العصابات الرقمية خلال أنشطتها الهجومية التي تمس بسلامة وأمن الدول على دعم مالي ونشاط اقتصادي تحصل عليهما من خلال:

أولا: الحوالات الالكترونية:

اعتمدتها البنوك الالكترونية خلال تطويراتها لخدماتها المالية، عبرها يتم نقل الأموال بين الحسابات أو للمستفيدين عبر الوسائط الالكترونية دون الحاجة لمعاملات ورقية، وتمتاز هذه الآلية بالسرعة في التنفيذ وانخفاض أسعارها، مع إمكانية القيام بها في أي وقت ومكان، وذلك مواكبة للمتطلبات الحديثة القائمة على

[1] لامية طالة، مرجع سابق، ص125.

[2] جاسم محمد جندل، مرجع سابق، ص156.

[3] يوسف مرين، "إرهاب الانترنت، عندما تتحول التقنية إلى وسيلة للإجرام"، **مجلة الدراسات القانونية والسياسية**، جامعة عبد الحميد بن باديس مستغانم، م04، ع02، جوان2018، ص208.

الفعالية والمرونة في المعاملات المصرفية، غير أنها تساهم في تعزيز دقة العمليات وتقليل الأخطاء البشرية، وتدعم الشفافية في تتبع ومراقبة العمليات داخل النظام المصرفي[1].

ثانيا: وسائل الدفع الخاصة بالبنوك الالكترونية:

تمول هذه الوسائل العصابات الرقمية في الهجمات الإرهابية الالكترونية إما بالنقود الالكترونية التي تحول القيمة النقدية لمخزون الكتروني على نحو الصور الشائعة لها على وسيلة تقنية، لتكون أداة محمولة للدفع مقدما، أشكالها وأوزانها تختلف بحسب الوسيلة التي تم تخزين القيمة النقدية فيها. أو عن طريق الشيكات الالكترونية بإرسال الشيك الالكتروني عبر الانترنت من المشتري للبنك، فيقبله ثم يظهره ثم يرده للبنك البائع الكترونيا حتى يتمكن العامل من التحصيل من البنك المشتري الكترونيا. أو بالبطاقات ولها أشكال وأنواع مختلفة منها بطاقات الائتمان، بطاقات الخصم الشهري، بطاقات الدفع والطاقات الذكية[2]

[1] يوسف مرين، مرجع سابق، ص211.

[2] المرجع نفسه، ص211.

ملخص الفصل الأول

يتجلى من خلال هذا الفصل أن العصابات الرقمية أصبحت ظاهرة إجرامية ذات امتداد دولي، تستدعي تأطيرا قانونيا محكما لمواجهتها. فهي تقوم على جماعات إجرامية منظمة تضم أفرادا ذوي كفاءات تقنية عالية، يعتمدون على أساليب حديثة ومتطورة لارتكاب جرائم متعددة، كجرائم القرصنة والاحتيال الالكتروني، بدوافع تتراوح بين تحقيق المكاسب المالية والسعي الى النفوذ والمكانة داخل المنظمات بإبراز المهارات.

كما أظهر هذا الفصل أن هذه العصابات قد تجاوزت النمط التقليدي للجريمة، لتصبح أكثر تنظيما ومرونة، قائمة على هياكل هرمية محكمة، تستغل مختلف الثغرات الأمنية في الشبكات والأنظمة المعلوماتية. وتعتمد في ذلك على تقنيات متقدمة وهجمات الكترونية متنوعة، تشمل البرمجيات الخبيثة، وهجمات الحرمان من الخدمة، وسرقة المعطيات، وغيرها من الأساليب التي تستهدف الأموال والأفراد والمؤسسات.

ولم يقتصر نشاطها على الجرائم المالية، بل امتد ليشمل تهديد الأفراد من خلال الابتزاز الالكتروني وانتحال الهوية، والتشهير، فضلا عن استهداف أمن الدول عبر أنشطة التجسس والهجمات السيبيرانية، ما يبرز خطورة هذه الظاهرة وتعقيدها.

وهو ما يستدعي التطرق في الفصل الموالي إلى دراسة مخاطر هذه الهجمات الالكترونية التي تقوم بها العصابات الرقمية، وكذا الإطار القانوني الكفيل بمكافحتها والحد من أثارها بما يسمح بتحقيق السلم والأمن.

.

الفصل الثاني:

الإطار القانوني الدولي للعصابات الرقمية

تمهيد:

يشهد الفضاء السيبيراني تحولا نوعيا في أنماط الإجرام المنظم، إذ لم تعد العصابات الرقمية مجرد أفراد متناثرين يمارسون اختراقات عرضية، بل أضحت شبكات إجرامية عابرة للحدود تتبنى بنى تنظيمية مرنة وتستثمر أدوات تقنية متقدمة، يستغلون الثغرات التشريعية والتقنية والتباين الكبير بين الأنظمة القانونية للدول لتحقيق مكاسب مالية وسياسية، ويترتب على ذلك أن مكافحتها لم تعد ممكنة بالاعتماد على المقاربات الجنائية التقليدية وحدها، مما يستدعي استجابة إستراتيجية وقانونية متكاملة تتجاوز الحدود الوطنية الضيقة.

رغم وجود ترسانة قانونية دولية وإقليمية إلا أن الفجوة بين النص والتطبيق لا تزال واسعة، ذلك لتعدد جهات الاختصاص القضائي وتعدد مساطر الإنابة القضائية والمساعدة القانونية المتبادلة، وهذا ما يؤدي عمليا لخلق مناطق ملاذ تستغلها العصابات لتفادي الملاحقة أو لقطع أوصال الأدلة بين دول متعددة، مما يستدعي إعادة النظر في الآليات الحالية واقتراح مسارات جديدة لتعزيز التعاون على المستويات التقنية والردع الأمني والوعي المجتمعي، مع تسليط الضوء على البعد الوقائي والاستباقي ليكون السبيل الأوفر حظا لبناء دفاع دولي متكامل قادر على الصمود في وجه التهديدات المستمرة والمتطورة للعصابات الرقمية.

وعليه، سيتم دراسة الفصل من خلال مبحثين رئيسين، حيث نخصص المبحث الأول لاستراتيجيات الأمن السيبيراني لمكافحة العصابات الرقمية بالتطرق للجهود الإقليمية لمواجهتها، دور اتفاقية الأمم المتحدة 2024 في التصدي لها، المحاكمة الإجرائية في الاتفاقيات الدولية، آليات التعاون القضائي الدولي. أما المبحث الثاني فسيكون لسبل تعزيز الجهود الدولية في مواجهة العصابات الرقمية من حيث التحديات القانونية، الإجراءات الجنائية والتحقيقية، الأجهزة الدولية للتصدي للعصابات الرقمية واليات الوقاية والمواجهة المستقبلية لأنشطتها.

المبحث الأول: استراتيجيات الأمن السيبيراني لمكافحة العصابات الرقمية.

المبحث الثاني: سبل تعزيز الجهود الدولية في مواجهة العصابات الرقمية.

المبحث الأول: استراتيجيات الأمن السيبيراني لمكافحة العصابات الرقمية.

تشهد البيئة الرقمية تحولا جذريا في أنماط الجريمة المنظمة، فدفعت تلك التهديدات المتزايدة على أمن الفضاء السيبيراني بالعديد من الدول للعمل على بذل جهود مضنية في استحداث قوانين لمكافحة هجمات العصابات الرقمية، فتداخلت الجهود الدولية والإقليمية لتشكيل مظلة قانونية تهدف لحماية الفضاء السيبيراني ومواكبة التطور السريع لهذه العصابات، لذلك اعتمدوا على استراتيجيات من شأنها توحيد الأطر القانونية والتنظيمية والإجرائية لمواجهة الهجمات السيبيرانية التي تقوم بها المنظمات الإجرامية في العالم الافتراضي المتمثلة في العصابات الرقمية، وعملت الدول على تعزيز أشكال التعاون الدولي في سبيل مكافحتها حيث تبرز اتفاقية الأمم المتحدة لمكافحة الجرائم الالكترونية(2025) كأحدث مسعى لتوحيد الرؤى الدولية وتوفير منصة شاملة للتعاون القضائي الدولي.

وعليه، سيتم في سياق هذا المبحث التطرق إلى تبيان الجهود الإقليمية في مواجهة العصابات الرقمية، إضافة للدور الفعال لاتفاقية الأمم المتحدة لمكافحة الجريمة الالكترونية 2025، وإجراءات المحاكمة في ظل الاتفاقيات الدولية، ومختلف سبل وآليات التعاون القضائي الدولي لمكافحة العصابات الرقمية وكبح شتى أنشطتها الإجرامية.

المطلب الأول: الجهود الإقليمية في مواجهة العصابات الرقمية.

تشكل الجهود الإقليمية حجر الزاوية في بناء استراتيجيات الردع السيبيراني، حيث أدركت المنظمات الإقليمية منذ وقت مبكر أن الطبيعة العابرة للحدود بالنسبة للعصابات الرقمية تستوجب تنسيقا قانونيا وتقنيا دقيقا، وقد تبلورت هذه الجهود من خلال صكوك دولية وإقليمية تهدف إلى توحيد المفاهيم وتسهيل التعاون القضائي العابر للحدود، أما ركائزه تتمحور حول اتفاقية بودابست(2001) إضافة للبروتوكولات المكملة لها، والاتفاقية العربية لمكافحة الجرائم المعلوماتية، ولا ننسى التوصيات والتوجيهات الحيوية للمجلس الأوروبي.

الفرع الأول: اتفاقية بودابست 2001 لمكافحة الجرائم السيبيرانية.

أولا: لمحة عن ميلاد اتفاقية بودابست.

تأسست معاهدة بودابست بمبادرة من مجلس أوروبا في 23 نوفمبر 2001م استجابة للتحولات التكنولوجية المتسارعة والعولمة الرقمية التي أدت إلى تنامي التهديدات السيبيرانية، دخلت حيز النفاذ في

01 جويلية 2004، تميزت عملية صياغة المعاهدة بصبغة دولية واسعة، حيث شارك في إعدادها خبراء قانونيين وأجهزة إنفاذ قانون من خارج النطاق الأوروبي، بما في ذلك الولايات المتحدة، اليابان، كندا، وجنوب إفريقيا، مما منحها طابعا عالميا يعكس توافقا دوليا حول ضرورة مواجهة الإجرام العابر للحدود.

استهدفت معاهدة بودابست 2001 إرساء سياسة عقابية موحدة وتطوير تشريعات وطنية متوائمة، تهدف في جوهرها إلى حماية المجتمعات من الأنشطة الإجرامية في البيئة الرقمية. وتأسيسا على هذا الإطار قام الاتحاد الأوروبي بتعزيز بنته المؤسساتية عبر أنشاء أجهزة متخصصة، أبرزها نجد " اليوروبول" و"المركز الأوروبي لمكافحة الجريمة الالكترونية" الذي باشر نشاطه عام2013م، يمثل هذا التوجه السياسي تأكيدا على أولوية التعاون القضائي والأمني كأداة لا غنى عنها في تعقب الجرائم الالكترونية والحد من مخاطرها، خاصة الأنشطة الإجرامية المنظمة التي تقوم بها العصابات الرقمية في الفضاء السيبيراني[1].

ثانيا: مضمون الاتفاقية.

تتكون اتفاقية بودابست من 48 مادة إذ تهدف أساسا إلى وضع إطار قانوني يلزم الدول باتخاذ تدابير تشريعية فعالة للتصدي لجرائم الحاسوب والحد من مخاطرها، كما تعد مرجعا مهما في مجال محاربة ومكافحة الإرهاب السيبيراني، سواء على المستوى الدولي أو في التشريعات الوطنية، نظرا لما تتضمنه من توجيهات وتوصيات للدول الأعضاء، وقد ركزت هذه الاتفاقية على ثلاثة عناصر أساسية، فنجد العنصر الأول يتمثل في أهمية التدابير التشريعية الموضوعية (نصوص التجريم الموضوعية)، أما العنصر الثاني يتمثل في أهمية التدابير التشريعية الإجرائية المتلائمة مع طبيعة الجرائم الالكترونية.، ليبرز العنصر الثالث أهمية تدابير التعاون الدولي والإقليمي في مجال مكافحة الجرائم، انطلاقا من جهود دولية وإقليمية في هذا المجال[2].

أما مواد الاتفاقية فهي موزعة على أربعة فصول، إذ الفصل الأول تضمنت مواده تعريفا للمصطلحات الأساسية (نظام الكمبيوتر ، الشبكة، مقدمو الخدمة، بيانات الحركة)؛ أما الفصل الثاني مواده معنية بالخطوات الواجب اتخاذها على الصعيد الوطني، وهو بدوره مؤلف من ثلاثة أقسام نجد الأول يضم المواد من 02 إلى 13 تعالج فيها النصوص الموضوعية لجرائم الحاسوب، أما الثاني فيضم المواد من 14 إلى 21 تتعلق

[1] ميرفت محمد حبايبة، مرجع سابق، ص ص266، 265.

[2] سليمان قطاف، عبد الحليم بوقرين، "الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري"، **المجلة الأكاديمية للبحوث القانونية والسياسية**، م06، ع01، مارس2022، ص239.

بالقواعد الإجرائية، والقسم الثالث يضم المادة 22 ويتعلق بالاختصاص؛ والفصل الثالث تم تسميته بالتعاون الدولي يضم المواد من 23 إلى 35؛ ليشمل بذلك الفصل الرابع الأحكام الختامية من المادة 36 إلى 148[1].

كما حددت اتفاقية بودابست الجرائم المعلوماتية وقامت بتصنيفها لخمسة عناوين في القسم الأول، فالعنوان الأول: جوهر جرائم الحاسب أو الجرائم المعلوماتية التي تعرف بالجرائم ضد سرية، سلامة، إتاحة البيانات والنظم؛ أما العنوان الثاني للانتهاكات الممارسة بواسطة الحاسب الآلي التي تمس بعض المصالح القانونية وجرائم الغش المعلوماتي والتزوير المعلوماتي؛ والعنوان الثالث للانتهاكات والجرائم المرتبطة بالمحتوى وتخص الإنتاج والنشر غير المشروع للمواد الإباحية الطفولية عبر النظم المعلوماتية (المادة09 منها)؛ ليأتي العنوان الرابع بالجرائم المتعلقة بالاعتداء على الملكية الفكرية والحقوق المرتبطة بها (المادة10 منها)؛ أما العنوان الخامس فهو عبارة عن أحكام إضافية تخص الشروع والاشتراك طبقا للمعايير الحديثة لمسؤولية الأشخاص والجزاءات والتدابير المعنوية[2].

ثالثا: الإجراءات الجنائية الجديدة لمكافحة العصابات الرقمية على ضوء اتفاقية بودابست.

تمثل اتفاقية بودابست لمكافحة الجريمة المعلوماتية (2001) منعطفا جوهريا في القانون الدولي، حيث أوجدت إطارا متكاملا للإجراءات الجنائية الحديثة الرامية لمواجهة العصابات الرقمية. تقوم هذه الاتفاقية على مبدأ إلزام الدول الأعضاء بدمج هذه التدابير في تشريعاتها الوطنية، وهو ما يعكس التوجه الدولي نحو توحيد الجهود التشريعية والإجرائية، نظرا للطبيعة العابرة للحدود التي تتسم بها الأنشطة الإجرامية التي تمارسها العصابات الرقمية، والتي يستحيل كبحها دون تنسيق قضائي وقانوني دولي مشترك.

وفي سياق التدابير الإجرائية منحت الاتفاقية أولوية قصوى لآلية "الحفظ السريع للمعطيات المخزنة" حسب المواد16 و17 بهدف حماية المعلومات الرقمية من التلف أو المحو العمدي، ونظرا للطبيعة المؤقتة للأدلة الرقمية وسرعة تأثيرها، حولت المادة16 للسلطات الوطنية إصدار أوامر قضائية أو إدارية للحفظ الفوري للبيانات مع الحرص على إيجاد توازن دقيق بين متطلبات فاعلية التحقيق، وبين حماية حقوق الأفراد وضمان خصوصيتهم الرقمية[3].

[1] سليمان قطاف، عبد الحليم بوقرين، مرجع سابق، ص239.

[2] المرجع نفسه، ص ص240، 239.

[3] سعيد مسعود الكثيري، "الجريمة الالكترونية في ضوء اتفاقية بودابست: الإطار المفاهيمي والتصنيفي"، مجلة البحوث القانونية والاقتصادية سلطنة عمان، م09، ع01، ديسمبر 2025، ص958.

كما توسعت الاتفاقية في الجوانب التقنية للتحقيق حيث تناولت آليات تجميع المعلومات الخاصة بالمشتركين، مثل أرقام الهواتف وعناوين البريد الالكتروني باعتبارها أدوات حاسمة لتحديد هوية الجناة، وقد أقرت الاتفاقية إجراءات "التفتيش المعلوماتي" و"التصنت" كأدوات مستحدثة تتيح اعتراض المراسلات أو تسجيل المكالمات، شريطة أن يتم ذلك وفق إجراءات رسمية وإذن قضائي مسبق، لضمان توافق القوانين مع التطور التكنولوجي المتسارع دون المساس بالحقوق والحريات.

في ختامها شددت الاتفاقية (المادة 23 وما بعدها) على أن التعاون الدولي هو الركيزة الأساسية لتفعيل كافة الإجراءات السابقة، من خلال تبادل المعلومات والأدلة وتسليم المجرمين بمرونة وسرعة[1].

ساهمت الاتفاقية من خلال صياغة مصطلحات قانونية مستحدثة وتوحيد الإجراءات القضائية بين الدول، وذلك بمعالجة القصور الذي يعتري القوانين التقليدية مما عزز من فاعلية مكافحة العصابات الرقمية في الجرائم الالكترونية وأرسى دعائم الأمن المعلوماتي على المستوى العالمي[2].

مما سبق، نستخلص أن اتفاقية بودابست2001 ساهمت في مكافحة العصابات الرقمية بإلزام الدول الأطراف بتجريم أفعال العصابات الرقمية مثل سرقة البيانات، تعطيل الأنظمة، والتورط في شبكات القرصنة المنظمة. وتجهيز سلطات التحقيق بالأدوات الإجرائية لجمع الأدلة الرقمية مثل مصادرة البيانات وحجز الأجهزة. كما تسهل تبادل المعلومات والمساعدة القضائية الدولية قي الوقت الفعلي، مما يساعد في تتبع العصابات العابرة للحدود، وطلب تسليم المجرمين وتنسيق التحقيقات بين أكثر من دولة في وقت واحد. غير أن الاتفاقية قامت بإنشاء قواعد إجرائية مشتركة لتعاون الشرطة والنيابة والجهات القضائية، وذلك بما يسمح بتبادل بيانات الاتصال وحفظ السجلات الرقمية لفترة تتيح تتبع أنشطة العصابات.

الفرع الثاني: اتفاقية الجامعة العربية لمكافحة الجريمة السيبيرانية.

صدور قانون استرشادي لمكافحة جرائم تقنية الفضاء السيبيراني عن جامعة الدول العربية، إذ سعت الدول العربية من خلاله لتقنين وتجريم الأعمال غير مشروعة التي ارتكبت عبر الفضاء السيبيراني بالتوقيع على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010/12/21، وذلك بغرض تعزيز التعاون بين الدول العربية لمكافحة الجرائم السيبيرانية، والحفاظ على أمنها وسلامة مجتمعاتها.

[1] سعيد مسعود الكثيري، مرجع سابق، ص959.

[2] المرجع نفسه، ص960.

أولا: التعريف بالاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010:

تعتبر الاتفاقية العربية لمكافحة جرائم تقنية المعلومات من الاتفاقيات العربية الحديثة في مجال مكافحة جرائم تقنية المعلومات على مستوى الدول العربية، تمتاز بالطابع الإقليمي الدولي، عبارة عن اتفاق معقود بين دول جامعة الدول العربية، وقد حررت في مدينة القاهرة بجمهورية مصر العربية في 21 ديسمبر 2010 (الموافق ل 15 محرم 1432هـ). تم إيداعها على مستوى الأمانة العامة لجامعة الدول العربية بنسخة واحدة باللغة العربية، ووقع عليها وزراء الداخلية والعدل العرب نيابة عن دولهم، وشملت دولا عربية متعددة منها الأردن، الإمارات، البحرين، تونس، الجزائر، السعودية، السودان، العراق، سوريا، عمان، فلسطين، قطر، الكويت، ليبيا، مصر، المغرب، موريتانيا، اليمن[1].

ثانيا: الهيكل العام للاتفاقية.

تتكون الاتفاقية من ديباجة وثلاثة وأربعين (43) مادة موزعة على خمسة فصول رئيسة، حيث أن الفصل الأول (أحكام عامة) يكون من المادة 01 إلى المادة 4 يتناول صيانة السيادة ونطاق التطبيق والمصطلحات، أما الفصل الثاني (التجريم) يكون من المادة 05 إلى المادة 21 ويضم نصوص التجريم والعقوبات لجرائم تقنية المعلومات، والفصل الثالث (الأحكام الإجرائية) يكون من المادة 22 إلى المادة 29، ويتعلق بالتحفظ العاجل، الكشف الجزئي، التفتيش، الضبط، والجمع الفوري للمعلومات، والفصل الرابع (التعاون القضائي) من المادة 30 إلى المادة 43، والفصل الخامس (أحكام ختامية)[2].

كما خصصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات حيزا لتعريف المصطلحات التقنية لضمان فهم موحد، وهذه المصطلحات هي تقنية المعلومات (النظام المعلوماتي)، مزود الخدمة، البيانات، البرنامج المعلوماتي، الشبكة المعلوماتية، معلومات المشترك، الالتقاط.

ثالثا: أهداف الاتفاقية.

تظهر ديباجة الاتفاقية وأهدافها الغاية الأساسية من وضعها، وتتمثل في تعزيز التعاون العربي لمكافحة جرائم تقنية المعلومات ومواجهة التهديدات الأمنية الناتجة عنها للحفاظ على امن المجتمعات و أفرادها؛ وإلزام الدول الأطراف اتخاذ الإجراءات التشريعية والتنظيمية لوضع أحكام الاتفاقية موضع التنفيذ

[1] عمار حمبلي، دليلة عثماني، **جرائم تقنية المعلومات في ظل الاتفاقية العربية 2010 وفي التشريع الجزائري**، مذكرة ماستر في القانون الجنائي والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2022، ص19.

[2] المرجع نفسه، ص ص21، 20.

من خلال تبني سياسة جنائية مشتركة مع مراعاة أحكام الشريعة الإسلامية والتراث الإنساني العربي؛ كما تسعى لتجريم الأفعال الواردة في فصل التجريم (المواد 6 الى18) التي تشكل جرائم تقنية المعلومات التي تشمل الدخول غير المشروع والاعتراض غير المشروع، الاعتداء على سلامة البيانات والأنظمة، إساءة استخدام وسائل تقنية المعلومات، التزوير والاحتيال المعلوماتي، الاعتداء على حرمة الحياة الخاصة والجرائم المتعلقة بالإباحية والإرهاب والجريمة المنظمة، والجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة[1].

وعليه، تعد اتفاقية الجامعة العربية لمكافحة جرائم تقنية المعلومات من أهم الأدوات الإقليمية التي تسخرها الدول العربية لمواجهة العصابات الرقمية وتنظيم الجريمة السيبيرانية عبر الحدود، إذ تهدف إلى مواءمة التشريعات الجنائية العربية في مجال الجرائم الالكترونية، بما يمكن من تجريم الأنشطة التي تمارسها العصابات الرقمية من اختراق وتصيد احتيالي والبرمجيات الخبيثة وتزوير الكتروني...، فتعرف تلك الأفعال مما يسهل في توحيد إطار المساءلة ضد العصابات الرقمية المنظمة العاملة في أكثر من دولة عربية. فهي تعزز التعاون القضائي والأمني بين الدول العربية عبر أحكام واضحة حول المساعدة المتبادلة وتبادل المعلومات والتحفظ على البيانات الالكترونية، وهو ما يفكك روابط العصابات الرقمية العابرة للحدود، كما تشجع الدول على إنشاء وحدات متخصصة في الجرائم السيبيرانية وبناء قدرات فنية من تحليل البيانات وتتبع الأثر الرقمي وتحليل الشبكات لرصد وتحييد العصابات الرقمية.

المطلب الثاني: دور اتفاقية الأمم المتحدة لمكافحة الجرائم الالكترونية 2024.

تعد اتفاقية الأمم المتحدة لمكافحة الجريمة الالكترونية المعتمدة سنة2024، نقلة نوعية في التعاون الدولي لمجابهة التحديات الرقمية، وتحولا جذريا في منظومة العدالة الجنائية الدولية، باعتبارها أول معاهدة عالمية متكاملة تنظم المكافحة الشاملة للجرائم السيبيرانية من منظور الأمم المتحدة، بما يشمل كل الدول الأعضاء بصرف النظر عن انتمائها القانوني أو الجغرافي، تم التفاوض حولها بين أكثر من 150 دولة على مدار سنوات، تهدف لوضع إطار شامل وموحد يعزز الأمن الرقمي الدولي ويمكن الدول من حماية فضائها السيبيراني ومواجهة التهديدات الرقمية المتصاعدة، فيما يلي سنوضحها أكثر.

[1] عمار حمبلي، مرجع سابق، ص ص23، 22.

الفرع الأول: اعتماد الاتفاقية.

اعتمدت الجمعية العامة للأمم المتحدة في 24 ديسمبر 2024 اتفاقية منع الجريمة السيبيرانية، وذلك بموجب القرار رقم 79/243 بعد خمسة سنوات من المفاوضات بين الدول الأعضاء، بهدف تعزيز التعاون الدولي في مكافحة الجرائم الالكترونية وحماية المجتمعات من التهديدات الرقمية.

وقد أنشأت الجمعية العامة لجنة خاصة لإعداد اتفاقية دولية شاملة لمكافحة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية، وأقرت اللجنة مشروع الاتفاقية في أوت 2024م. كما كلفت اللجنة بعقد جلسات لإعداد مشروع قواعد الإجراءات الخاصة بمؤتمر الدول الأطراف، والتفاوض على مشروع بروتوكول تكميلي للاتفاقية يضم الجرائم الإضافية حسب الاقتضاء.

وفي 25 أكتوبر 2025 فتح في العاصمة الفيتنامية هانوي باب التوقيع على الاتفاقية العالمية لمنع الجريمة السيبيرانية، فتم التوقيع عليها حينها من طرف 65 دولة ويتعين عليهم الصادقة على الاتفاقية وفقا لإجراءاتها الوطنية الخاصة، على أن تدخل الاتفاقية حيز النفاذ بعد مرور 90 يوما من مصادقة الدولة الأربعين عليها[1].

الفرع الثاني: مبررات الأهمية الإستراتيجية للاتفاقية.

تبرز أهمية اتفاقية الأمم المتحدة لمكافحة الجريمة الالكترونية 2024 في كونها تجسد إرادة جماعية دولية لسد الفجوات القانونية التي تستغلها الجماعات الإجرامية العابرة للحدود وهي العصابات الرقمية، مما يمهد الطريق لنظام تعاوني أكثر فاعلية واستدامة في الفضاء السيبيراني، إذ تستمد أهميتها من عدة أبعاد جوهرية تمس الأمن القومي والتعاون القضائي الدولي، فهي أداة لمواجهة التهديد المتنامي بتوفير الاتفاقية لأدوات وحلولا لمواجهة الجرائم الالكترونية المتزايدة حول العالم، بما يشمل القرصنة والبرمجيات الخبيثة وبرامج الفدية، وتحمي الأفراد والاقتصاد والبنى التحتية الحيوية وتعزز الثقة في الأنظمة الرقمية، كما تعزز التعاون الدولي بين الدول الأطراف عبر تبادل الأدلة الالكترونية ودعم التحقيقات، والملاحقات القضائية والمساعدة القانونية المتبادلة، إضافة لإجراءات تسليم المطلوبين واسترداد عائدات الجريمة، بما يضمن استجابة أسرع وأكثر تنسيقا للجرائم العابرة للحدود، وتحمي الأطفال وفق المنظمة الدولية فنجد اتفاقية منع الجريمة هي الأولى عالميا عبر الانترنت، مما يتيح للحكومات أدوات قانونية لحماية الأطفال من الاستغلال

[1] **أبرز بنود اتفاقية الأمم المتحدة لمنع الجريمة السيبرانية**، 2025/10/26، https://www.aljazeera.net/encyclopedia/، اطلع عليه بتاريخ 2026/05/06، الساعة 16:46.

والإيذاء وملاحقة المعتدين قضائيا، وتدعم الضحايا فتشجع الاتفاقية الدول على تقديم خدمات دعم للضحايا، وتشمل التعويض واسترداد الحقوق وإزالة المحتوى غير القانوني، بما يضمن حماية الضحايا وتلبية احتياجاتهم القانونية والاجتماعية، وأخير تعمل على الوقاية من الجرائم الالكترونية فتركز الاتفاقية على الوقاية قبل وقوع الجرائم الالكترونية عبر تطوير استراتيجيات شاملة وتدريب العاملين في القطاعين العام والخاص، وإنشاء برامج إعادة تأهيل وإدماج للجناة، بهدف تقليل المخاطر وخلق بيئة رقمية أكثر أمانا للجميع[1].

الفرع الثالث: الإطار القانوني الدولي لمكافحة الجريمة السيبيرانية عبر الاتفاقية.

تأتي اتفاقية الأمم المتحدة لمكافحة الجريمة الالكترونية 2024 كجهد دولي يهدف إلى سد الفجوات التي تركتها الاتفاقيات الإقليمية السابقة مثل اتفاقية بودابست 2001 والاتفاقية العربية 2010، تهدف الاتفاقية لوضع إطار عالمي شامل لمكافحة استخدام تكنولوجيات المعلومات والاتصالات لأغراض إجرامية، مع التركيز على التوازن بين إنفاذ القانون وحماية حقوق الإنسان، نظمت الاتفاقية أحكامها في ستة محاور رئيسية تبدأ بوضع تعريفات دقيقة للمصطلحات ذات الصلة في المادة 02 ثم تنتقل لتنظيم باقي الجوانب الأخرى كالأتي:

أولا: الأحكام الموضوعية (التجريم).

تحدد الاتفاقية الإطار الموضوعي للمسؤولية الجنائية عبر تجريم أحد عشر نمطا من السلوكيات السيبيرانية المستحدثة، تبدأ من الوصول غير المشروع وتصل إلى غسل عائدات الجرائم، مع توسيع نطاق التجريم ليشمل الأشخاص الاعتبارية وإقرار مبدأ العقاب على المشاركة والشروع لضمان شمولية الملاحقة القانونية[2]، حيث نظمت تلك السلوكيات من المادة (07) إلى المادة (19) من الاتفاقية.

ثانيا: الأحكام الإجرائية (التدابير الإجرائية وإنفاذ القانون).

تنظم هذه الأحكام صلاحيات سلطات إنفاذ القانون في جمع الأدلة الرقمية، والحفظ الاحتياطي للبيانات، والاعتراض الآني لحركة المرور والمحتوى، مع إخضاع هذه السلطات الاستثنائية لمنظومة من

[1] أبرز بنود اتفاقية الأمم المتحدة لمنع الجريمة السيبرانية، مرجع سابق.

[2] المرجع نفسه.

الضمانات القانونية والحقوقية التي تكفل حماية حقوق الإنسان والحريات الأساسية أثناء التحقيقات[1]، وأهم هذه التدابير نجدها من المادة (23) إلى المادة (34) من الاتفاقية.

ثالثا: الأحكام القضائية (الولاية القضائية والسيادة).

تضع الاتفاقية معايير دقيقة لتحديد الاختصاص القضائي الوطني وآليات فض تنازعه عند تعدد التحقيقات الدولية، مع التأكيد الصارم على مبادئ السيادة الوطنية والمساواة بين الدول، وعدم التدخل في الشؤون الداخلية للدول، وحظر ممارسة أي دولة لصلاحياتها داخل إقليم دولة أخرى دون سند قانوني[2].

رابعا: التعاون الدولي.

تقنن الاتفاقيات آليات التعاون العابر للحدود لمواجهة الطبيعة اللامادية للجريمة السيبرانية، وذلك من خلال تنظيم تبادل الأدلة الرقمية، والمساعدة القضائية المتبادلة، وتسليم المجرمين في الجرائم الجسيمة، مع استحداث منظومة نقاط اتصال فورية تعمل على مدار الساعة (24/7) لضمان سرعة الاستجابة الدولية[3].

خامسا: التدابير الوقائية.

تعتمد الاتفاقية منهجا استباقيًا لمكافحة الإجرام السيبيراني عبر إلزام الدول بسن تشريعات وطنية وسياسات وقائية شاملة، ترتكز على تفعيل الشراكة المجتمعية بين أجهزة إنفاذ القانون والقطاع الخاص والمؤسسات الأكاديمية والمجتمع المدني، ترسيخا لمبدأ المسؤولية المشتركة في تأمين الفضاء الرقمي[4].

سادسا: بناء القدرات والمساعدة التقنية.

تكرس الاتفاقية محور بناء القدرات كركيزة جوهرية لدعم الدول لاسيما النامية من خلال نقل التكنولوجيا، وتوفير برامج التدريب المتخصصة، وتبادل الخبرات الفنية، بهدف تمكين هذه الدول من تطوير بنيتها التشريعية والمؤسسية القادرة على مواجهة التهديدات السيبرانية بفاعلية[5].

---

[1] أبرز بنود اتفاقية الأمم المتحدة لمنع الجريمة السيبرانية، مرجع سابق.

[2] المرجع نفسه.

[3] المرجع نفسه.

[4] المرجع نفسه.

[5] المرجع نفسه.

نستخلص مما سبق، أن اتفاقية الأمم المتحدة لمكافحة الجريمة الالكترونية 2024 أداة إستراتيجية لتقويض هيكلة "العصابات الرقمية" المنظمة، حيث توفر إطارا قانونيا موحدا يمنع المجرمين من استغلال الفجوات القانونية وتحول الفضاء السيبيرانية من بيئة خصبة للإفلات من العقاب إلى بيئة خاضعة للمساءلة القانونية المشتركة. فتعمل على سد ثغرات الملاذات الآمنة بإجبار الدول على التعاون في ملاحقة مجرمي العصابات الرقمية، مما يحرم عليهم استغلال الدول التي كانت تفتقر سابقا لقوانين تجرم أفعالهم أو تمنع تسليمهم. كذلك تجمد الأصول المالية بفرضها أطر للتعاون في تعقب وتجميد ومصادرة العائدات المالية غير المشروعة، مما يزعزع القدرة التمويلية للعصابات التي تعتمد على الاحتيال وغسيل الأموال. كما توفر آلية إجرائية موحدة لجمع وتبادل الأدلة الرقمية الحساسة، مما يسرع من وتيرة التحقيقات الجنائية العابرة للحدود التي كانت تتوقف سابقا بسبب التعقيدات السياسية. وأيضا تقوم بتعزيز القدرات الوطنية ببرامج بناء القدرات، فتساعد الاتفاقية الدول التي لا تملك خبرات تقنية متقدمة على رصد وتفكيك عمليات العصابات الرقمية داخل حدودها أو عبرها.

المطلب الثالث: المحاكمة الإجرائية في الاتفاقيات الدولية.

تعد المحاكمة الإجرائية في الاتفاقيات الدولية من المبادئ التي تسهم في ضمان العدالة وحماية الحقوق في النظام القانوني الدولي، خاصة في ظل تزايد الاعتماد على الاتفاقيات والمعاهدات الدولية كآلية لتنظيم العلاقات بين الدول والأفراد، إذ تشمل الآليات القضائية والتحكيمية بالإضافة إلى الإجراءات الإدارية كآليات الإبلاغ والتفتيش التي تتسم بخصوصيتها الدولية. كما أن معاينة مسرح الجريمة من الإجراءات الأساسية في التحقيقات الجنائية فهي حجر الأساس في جمع الأدلة وتحديد ملابسات الجريمة سواء على الصعيد الوطني أو الدولي، ومع تزايد الاعتماد على نظم المعلومات في ارتكاب الجرائم الالكترونية من طرف العصابات الرقمية، فبرزت الحاجة إلى إجراءات قانونية دقيقة لتنظيم تفتيش نظم المعلومات وضبطها في إطار الاتفاقيات الدولية، لضمان عدم انتهاك الحقوق الأساسي للأفراد مع الحفاظ على فعالية التحقيقات في الفضاء السيبيراني.

إذ أفردت تلك الاتفاقيات الدولية نصوصا تفصيلية تحدد الشروط والضوابط القانونية لمعاينة الأنظمة المعلوماتية، تفتيشها، حجز المعلومات والحفاظ على سلامتها كأدلة جنائية رقمية، فيما يلي سنتطرق لمعاينة مسرح الجريمة وإجراءات تفتيش نظم المعلومات وضبطها.

الفرع الأول: معاينة مسرح الجريمة.

تتسم الجرائم الالكترونية بالسرية التامة لصعوبة اكتشافها وإثباتها وحتى الاستدلال على مرتكبيها، فالعصابات الرقمية لا تترك أثر مادي على أنشطتها مما يصعب الانتقال لمسرح الجريمة وضبط جهاز الحاسوب الذي يتطلب دراية كبيرة بتقنية المعلومات لمعاينته، فمعاينة مسرح الجريمة الالكترونية يمكننا من إثبات أو نفي وقوع الفعل الإجرامي المنظم، وكيفية البحث عن الدليل للإثبات.

أولا: تعريف مسرح الجريمة.

يعرف مسرح الجريمة بأنه مكان قام الجاني باقتراف جرمه فيه، ومنه تبدأ عمليات التحقيق والبحث عن الفاعل في النشاط الإجرامي بتتبع أثار ما خلفه في المكان[1].

كما تم تعريفه أيضا بكونه مكان أو مجموعة أماكن شاهدة على تنفيذ الجريمة، فيرسم للمحققين طريق للبحث عن الجاني باعتبار مسرح الجريمة يحتوي على أثار ومخلفات تعتبر أدلة للاتهام، كما يمكن تمثيل أحداث الجريمة التي وقعت فيه ذلك لغرض إعطاء مساحة أوسع لتقفي الحقيقة[2].

ثانيا: معاينة مسرح الجريمة الالكترونية.

يتم معاينة مسرح جريمة الكترونية في مسرح افتراضي يترك فيه مستخدم الشبكة المعلوماتية أو الانترنت أثاره فيه من رسائل وكافة اتصالاته التي تمت عبر الشبكة العالمية. وفكرت المسرح الافتراضي تتضاءل مع مرور الوقت لسببين هما أن الجريمة الالكترونية في الغالب لا تترك أثار مادية، إضافة لإمكانية أن تكون جرائم مستمرة فيتردد مرتكبيها من العصابات الرقمية على ذلك المسرح مما يؤدي لتغير أثاره[3].

ثالثا: حماية المسرح الافتراضي للجرائم الالكترونية.

القيام بالتنقل للمسرح الافتراضي مباشرة بعد ارتكاب الجرائم واحتجاز جميع الأجهزة الالكترونية من حواسيب وما يتصل بها، ذلك بما يحفظ الدليل الرقمي من الإتلاف أو المحو، والبحث بشكل منتظم ورتيب لسلامة الأدلة والأشخاص، من خلال تشكيل فريق فني متخصص وجمع المعلومات المسبقة عن طبيعة الواقعة ومكوناتها التقنية، وتأمين مصادر الطاقة والأجهزة والشبكات والملحقات المتصلة بها، وتوثيقها

[1] ميرفت محمد حبابية، مرجع سابق، ص281.

[2] المرجع نفسه، ص281.

[3] المرجع نفسه، ص282.

تصويرا ووصفا[1]، ومنع غير المصرح لم من العبث بها، والإبقاء على الأجهزة في حالتها الأصلية، وضبط الأدلة الرقمية والمادية المرتبطة بها، وإجراء المقابلات الأولية مع الضحايا والشهود[2]، وعدم نقل أي وسيط معلوماتي قبل التحقق من سلامة البيئة المحيطة، بما يكفل قانونيا صون الدليل الرقمي من التلف أو المحو أو التغيير وضمان سلامة إجراءات التفتيش والتحقيق[3].

نستنتج مما سبق، أن المحقق في مسرح الجريمة الالكترونية يقوم بمعاينة مكونات الحاسوب والتي تعتبر مصدر غني بالأدلة الالكترونية، وتقوم المعاينة بطريقتين الأولى معاينة ذاتية يقوم بها الكمبيوتر بنفسه ويقدم التقرير للمحقق، أما الثانية هي المعاينة بكمبيوتر آخر، وذلك بفحص كلي للقرص الصلب وجزئي للبيانات الرقمية، كونها تساعد المحقق على جمع البيانات والمعطيات المخزنة إضافة لتتبع فحص البرمجيات الداخلية والخارجية، ومعاينة النظام المعلوماتي للكمبيوتر المخزن في ذاكرة تخزين الحاسب، وأيضا معاينة أنظمة الاتصال بشبكة الانترنت عبر تتبع الحركة الترسانية للنشاط الممارس عبر استخدام نظام فحص الكتروني يسمى بعلم البصمات يتم بمقتضاه التعرف على الحاسب الآلي الموصول بشبكة الانترنت، واستقبال العناوين العددية وتخزينها على هيئة رقمية.

الفرع الثاني: إجراءات تفتيش نظام المعلومات وضبطها.

يقوم القاضي بعملية التفتيش الالكتروني بناء على إذن مسبق من السلطة المختصة وذلك بغية الحصول على الأدلة المتعلقة بالجريمة الالكترونية وضبطها ونسبتها لشخص معين، والهدف من التفتيش الالكتروني هو ضبط المكونات المادية للكمبيوتر التي تمثل أداة الجريمة، أو ضبط الدعامات المعلوماتية التي تمثل محل الجريمة.

أولا: تعريف التفتيش الالكتروني.

إن التفتيش العادي إجراء من إجراءات التحقيق يهدف للبحث عن أدلة مادية لجناية أو جنحة تقع في محل جريمة يكون يتمتع بحرمة المسكن أو الشخص، بغرض إثبات ارتكاب أو نسبة الجريمة للمتهم عن طريق إتباع إجراءات محددة قانونا[4].

[1] ميرفت محمد حبايبة، مرجع سابق، ص283.

[2] المرجع نفسه، ص284.

[3] المرجع نفسه، ص284.

[4] المرجع نفسه، ص287.

أما التفتيش الالكتروني فهو تفتيش قضائي يكون بإذن مسبق من القاضي، وهو إجراء من إجراءات التحقيق للبحث داخل نظام حاسوبي سواء كان مكونا من حاسوب واحد أو عدة حواسيب تكون مرتبطة بشبكة لها حرمة حسب القانون، بغرض البحث عن الحقيقة عن طريق استخراج أدلة معلوماتية كالمعلومات والبيانات التي تكشف نوع الجريمة الالكترونية سواء جنحة أو جناية يحقق فيها[1].

ثانيا: شروط التفتيش الالكتروني.

يعد إجراء التفتيش من أخطر الإجراءات لأنه يمس بالحرية الشخصية للأفراد وأغلب الدول تعمل به للكشف عن ملابسات الجريمة، وذلك بوضع شروط موضوعية وأخرى شكلية الواجب توفرها عند التفتيش، وهي:

1- الشروط الموضوعية.

يخول لسلطة التحقيق الحق في مباشرة بعض الإجراءات الموضوعية التي تمس بالحياة الخاصة بضم أداة الجريمة الالكترونية.

أ- سبب التفتيش.

يشترط لإجراء التفتيش في جرائم العصابات الرقمية أن تشكل الواقعة المرتكبة وصف جنحة أو جناية فعلية الوقوع مع استبعاد المخالفات، وأن تتوافر فيها الأركان المادية والمعنوية اللازمة لقيام الجريمة، إذ لا يصدر قرار التفتيش إلا بوجود أدلة قاطعة تدعو للاشتباه في شخص أو مجموعة أشخاص ساهموا في ارتكابها سواء بوصفهم فاعلين أصليين أو مشاركين، أن الأجهزة التقنية المستعملة في الجريمة موجودة بمسكن المتهم أو مكان تواجده[2].

وعليه، فان محل التفتيش في الجريمة الالكترونية هو الجهاز التقني سواء كان هاتف نقال أو حاسوب تابع للمتهم.

[1] ميرفت محمد حبايبة، مرجع سابق، ص288.

[2] المرجع نفسه، ص ص291، 290.

ب- محل التفتيش.

يقصد بمحل التفتيش في جرائم العصابات الرقمية المكان الذي تحفظ فيه الأدوات والوسائل المادية الفاعلة في ارتكاب الأنشطة الإجرامية، ويشمل ذلك المكونات المادية للحاسوب كوحدات الإدخال والإخراج والذاكرة الرئيسية ووحدات التخزين الثانوي، إضافة إلى المكونات المعنوية المتمثلة في برامج النظام وبرامج التطبيقات بأنواعها، وشبكات الاتصال المرتبطة بالخادم والمضيف والملحقات التقنية والوسائط الالكترونية المختلفة، كما يمتد نطاق التفتيش ليشمل الأشخاص المستخدمين للحاسوب. ويشترط في محل التفتيش أن يكون محددا بدقة من حيث المكان والشخص، وألا يوجه إلا بوجود اتهام محدد لمرتكب الجريمة مع توافر دلائل كافية لإدانته كحيازته لأشياء ذات صلة بالأنشطة الإجرامية الالكترونية[1].

ج- السلطة المختصة بالتفتيش.

أسندت مهمة التفتيش للسلطات القضائية لأنها تعمل على حماية الحقوق والحريات، فحددت لقاضي التحقيق أن يختص بالتفتيش بمساعدة النيابة العامة فتتبع الجرائم الالكترونية وتتخذ ما يلزم لها من إجراءات. ويكون التفتيش عن طريق التنقل لمسكن المتهم أو لمكان تواجد الأجهزة المتعلقة بالجريمة أو يكون عن بعد.

ولأن العالم يشهد انتشار متزايد للجرائم الالكترونية فتم تكليف رجال الضبطية القضائية بالتحقيق من خلال نذبهم للتفتيش، فيصدر قرار ينيب أحد مأموري الضبط القضائي لإجراء التفتيش ضمن اختصاصه المكاني، ولقاضي التحقيق الحق في إنابة قاضي تحقيق أخر ذلك حالة امتدت الجريمة الالكترونية لمكان ليس من ضمن صلاحياته بتحديد مكان الإنابة ضمن القرار الخاص بها[2].

2- الشروط الشكلية.

يتعلق الأمر في الشروط الشكلية حول الإذن بالتفتيش ويتطلب له أن يكون مسبب وينفذ بحضور أشخاص معينون.

[1] ميرفت محمد حبايبة، مرجع سابق، ص291.

[2] المرجع نفسه، ص ص293، 292.

أ-تسبيب الإذن.

يجب أن يكون الإذن بالتفتيش مسببا بإظهار الغاية من إصداره، وتكمن الغاية من إجراء التفتيش في ضبط الأدلة التي تثبت وقوع الجريمة الالكترونية من طرف متهم تقني أو العصابات الرقمية بتعبير أخر[1].

ب- وقت إجراء التفتيش.

تختلف التشريعات الدولية بخصوص تحديد وقت إجراء التفتيش، غير أنه وحسب ما يعمل به فإن التفتيش في الجرائم الالكترونية يكون في أي وقت باعتبار أن عنصر الوقت مهم فيها، والدليل الرقمي قد يختفي مع مرور الوقت[2].

ج- الحضور الضروري لبعض الأشخاص.

يتطلب إجراء التفتيش حضور أشخاص معينين له حتى يكون إجراء سليما ويتمثلون في المتهم والشهود وصاحب المكان، غير أنه يعتبر شرط في طريق الزوال لما يتميز به الدليل الالكتروني من سرية وخصوصية وقدرة العصابات الرقمية من التلاعب به في أوقات قصيرة. والدول التي تعتمد التفتيش عن بعد لا تعمل به وفي حالة إغفاله يتعرض للبطلان النسبي[3].

د- محضر التفتيش.

لابد من تحرير محضر يثبت الأدلة التي أسفر عنها التفتيش، ولا يوجد للمحضر شكل قانوني محدد، وعليه فإن محضر تفتيش نظم الحاسوب تتطلب نفس القواعد العامة في المحاضر كلها، على أن يكون المحضر محرر ومكتوب باللغة الرسمية ويؤرخ تاريخه ويوقع عليه، ويجب أن يتضمن كل الإجراءات الخاصة المتبعة من قبل الخبير في الحواسيب والانترنت الذي استعين به للضرورة الحالية[4].

ثالثا: ضبط الدليل الالكتروني.

[1] ميرفت محمد حبايبة، مرجع سابق، ص293.

[2] المرجع نفسه، ص293.

[3] المرجع نفسه، ص ص294، 293.

[4] المرجع نفسه، ص294.

في الجرائم الالكترونية يكون ضبط الأدلة عن طريق الحصول على معلومات ودلائل تفيد التحقيق، سواء كانت مكونات مادية أو معنوية ويشمل البيانات المعالجة الكترونيا كذلك. فالضبط عملية تتبع التفتيش وإحراز المضبوطات الالكترونية، يلزم فيه اللجوء للطرق والوسائل التقنية التي تكون متفقة مع البيانات الالكترونية وأيضا مع البعد الجغرافي في أيادي أجهزة الضبط، وطرق الضبط نجد منها:

– **النسخ:** يكون من خلال برامج معدة خصيصا لهذا الغرض، ويتم النسخ في وسائل النقل.

– **التجميد:** يتم تجميد التعامل بالكمبيوتر الذي يحتوي على المضبوطات الالكترونية أو تجميد القسم الصلب الذي يحمله، عن طريق برامج تكون مخصصة لهذا الغرض فتقوم بضغط الملفات في ملف واحد أو في ملفات صغيرة[1].

وعليه، فإن المحاكمة الإجرائية في الاتفاقيات الدولية تشكل أساسا مهما لتنظيم إجراءات الكشف عن الجرائم وجمع الأدلة، لاسيما في الجرائم المعلوماتية التي تقوم بها العصابات الرقمية التي تتسم بالسرعة في محو أثارها وتجاوزها للحدود الوطنية.

المطلب الرابع: آليات التعاون القضائي الدولي.

لم يعد الإجرام المعاصر ظاهرة محصورة ضمن الحدود الإقليمية للدول بل تحول بفعل العولمة والتطور التكنولوجي المتسارع وتشابك العلاقات الدولية إلى ظاهرة عابرة للحدود الوطنية، تتسم بالتعقيد والتنظيم والتشعب في أساليبها ووسائلها وأثارها. وقد أفرز هذا التحول النوعي في طبيعة الجريمة تحديات جسيمة أمام الأنظمة القضائية الوطنية، التي وجدت نفسها عاجزة في كثير من الأحيان عن مواجهة هذه الأنماط الإجرامية المستحدثة بمعزل عن غيرها من الأنظمة القانونية خاصة الأنشطة الإجرامية التي تمارسها العصابات الرقمية.

وانطلاقا من هذا الواقع، برزت الحاجة الملحة إلى إرساء منظومة متكاملة من آليات التعاون القضائي الدولي، باعتبارها الإطار المؤسسي والقانوني الذي يمكن الدول من تجاوز الحواجز التي تفرضها مبادئ السيادة الوطنية والاختصاص الإقليمي، دون المساس بجوهر تلك المبادئ.

الفرع الأول: تعزيز التعاون القضائي الدولي.

[1] ميرفت محمد حبايبة، مرجع سابق، ص ص295، 294.

يعد ضعف التنسيق الدولي أحد أبرز العوائق البنيوية التي تحد من فاعلية مكافحة العصابات الرقمية، إذ يستغل أفرادها التباين القائم بين الأنظمة القانونية الوطنية وما ينشأ عن من فجوات تشريعية واختلافات إجرائية، بما يسمح بتعقيد التتبع الرقمي وتفادي المساءلة الجنائية ضدهم، بل واتخاذ بعض البيئات القانونية "ملاذات أمنة" بفعل قصور التجريم أو بطء التعاون القضائي.

وتزداد حدة هذه الإشكالية عند غياب نموذج موحد لتعريف النشاط الإجرامي السيبيرانية وضبط عناصره (الركن المادي والمعنوي) وتحديد نطاق الاختصاص القضائي، الأمر الذي يفضي عمليا إلى صعوبات في إنفاذ القانون وتنازع الاختصاص، وتعذر تنفيذ طلبات المساعدة القانونية المتبادلة أو تسليم المجرمين، فضلا عن إشكاليات الاعتراف المتبادل بالأدلة الرقمية.

وانطلاقا من ذلك، فإن تجاوز هذه العراقيل يستلزم تبني مقاربة متعددة المحاور قوامها ما يلي:

أولا: تبني رؤية موحدة للنشاط الإجرامي السيبيراني.

إن وضع تصور دولي موحد أو على الأقل متقارب لمفهوم العصابات الرقمية وأنشطتها وامتداداتها العابرة للحدود يعد خطوة أولى لتدعيم التعاون القضائي، ذلك أن توحيد المفاهيم والمصطلحات القانونية والتقنية مثل بيانات الحاسوب، بيانات المرور، مزود الخدمة، الحفظ العاجل للبيانات، يمكن من تجنب التضارب في التكييف القانوني، ويحد من فرص الإفلات من العقاب[1].

ولا يكفي في هذا السياق مجرد الاتفاق النظري على المبادئ العامة بل يتعين تفعيل الاتفاقيات الدولية المصادق عليها تفعيلا عمليا، وإدماج مقتضياتها في التشريعات الوطنية عبر تحديث القوانين الجنائية والإجرائية بما يستوعب صور الإجرام المستحدثة، كالتحرش الالكتروني، الاحتيال المعلوماتي، غسل الأموال عبر الأنترنت، الاعتداء على ن نظم المعالجة الآلية للمعطيات. ذلك بما يحقق التوازن بين فعالية المتابعة الجنائية وحماية الحقوق والحريات الرقمية[2].

ويتجلى التوحيد للرؤى في اتفاقية بودابست لمكافحة الجريمة السيبيرانية2001 الأكثر نجاحا في هذا الصدد، حيث نجحت بتوحيد التشريعات الجنائية للدول الأطراف وتيسير التعاون القضائي. إضافة

[1] سندس بن أوذينة، **الجهود الدولية في مواجهة الجرائم السيبرانية**، مذكرة ماستر في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة غرداية، 2025، ص42.

[2] المرجع نفسه، ص42.

لاعتماد حد أدنى تشريعي دولي يضمن تجريم الأفعال الأساسية وتحديد المسؤوليات، مع ترك مساحة للدول لتكييف التفاصيل وفق خصوصيتها الدستورية.

ثانيا: تسريع إجراءات التعاون وتبني الإنابة القضائية الفعالة.

تظهر الممارسة العملية أن آليات التعاون التقليدية وخاصة طلبات التسليم والمساعدة القضائية المتبادلة بصيغها الورقية لا تواكب طبيعة الجرائم السيبيرانية التي تمارسها العصابات الرقمية وتتسم بالسرعة وقابلية الأدلة الرقمية للتلف أو المحو أو النقل الفوري عبر خوادم متعددة، وعليه يصبح إصلاح البينة الإجرائية للتعاون القضائي ضرورة لا مجرد خيار، وهنا تبرز أهمية الإنابة القضائية بوصفها آلية لتجاوز بطء المساطر الدبلوماسية التقليدية، وذلك عبر إرساء قنوات اتصال مباشرة بين النيابة العامة والسلطات المركزية المختصة، وإقرار آليات الحفظ العاجل للبيانات وطلب تجميدها مؤقتا لمنع طمس الدليل الرقمي، واعتماد نماذج موحدة للطلبات وتحديد آجال قصوى للرد والتسليم بما يضمن السرعة، والتحول نحو رقمنة التعاون القضائي والأثر التتبعي للطلبات.

إذ يستحسن إقرار قواعد واضحة بشأن قبول الأدلة الرقمية عبر الحدود وفق معايير السلامة التقنية ووضع بروتوكولات مشتركة للخبرة الرقمية بما يدعم حجية الدليل الرقمي أمام القضاء[1].

ثالثا: محاكاة النماذج الناجحة والاستفادة منها.

يعد الاستئناس بالنماذج الدولية الرائدة أحد المسالك العملية لتعزيز التعاون القضائي وفي مقدمتها اتفاقية أوروبا بشأن الجريمة الالكترونية (بودابست2001)، ذلك لما حققته من تقارب في المصطلحات القانونية والتقنية وتيسير التعاون العابر للحدود، وتكتسب هذه التجربة أهميتها من كونها تؤسس لفكرة "المعايير المرجعية" التي يمكن للدول البناء عليها عند صياغة أو مراجعة تشريعاتها الداخلية، ولا تقتصر الاستفادة على تبني النصوص[2]، بل تمتد إلى تطوير آليات الاستجابة وفرق الاتصال الوطنية(24/7)، وتوحيد إجراءات جمع الأدلة وحفظها ونقلها، وتأهيل الكفاءات القضائية والضبطية وفق منهجية مشتركة[3].

---

[1] نوارة طابي، صليحة بوجادي، "الانابة القضائية كالية للتعاون الدولي من أجل استرداد عائدات الفساد"، **مجلة الأستاذ الباحث للدراسات القانونية والسياسية**، م10، ع01، جوان 2025، ص861.

[2] اتفاقية المجلس الأوروبي المتعلقة بمواجهة الجرائم الالكترونية 2001، الموقعة في بودابست، بتاريخ 23 نوفمبر 2001، دخلت حيز التنفيذ 01 جويلية 2004.

[3] سندس بن أوذينة، مرجع سابق، ص43.

كما يمكن تعزيز ذلك بإبرام اتفاقيات إقليمية مكملة تراعي الخصوصيات المحلية، وتحقق الملائمة بين الالتزامات الدولية والمبادئ الدستورية الوطنية.

رابعا: نشر ثقافة الإبلاغ عن الجرائم السيبيرانية.

تعد محدودية الإبلاغ عن مختلف الأنشطة الإجرامية المنظمة التي تقوم بها العصابات الرقمية من الأسباب المباشرة لضعف كشفها وتفكيك شبكاتها، إذ يحول الخوف من المساس بالسمعة أو نقص الوعي أو عدم الثقة في فاعلية التتبع دون تقديم الشكاوي، مما يسمح باستمرار السلوك الإجرامي واتساع نطاقه.

وتأسيسا على ذلك، ينبغي تكريس سياسة عمومية تشجع الإبلاغ عبر إرساء منصات وطنية مؤمنة للإبلاغ وتبسيط الإجراءات، وحماية المبلغين وضمان سرية بياناتهم حيث يلزم، وإقرار التزامات قانونية بالإبلاغ في القطاعات الحيوية كالبنوك والطاقة والاتصالات والصحة على غرار بعض التوجهات الأوروبية، وتعزيز الوعي الرقمي لدى الأفراد والمؤسسات بشأن مخاطر التصيد والابتزاز والاختراقات[1].

ولتشجيع فكرة الإبلاغ عليهم بربطه بآليات الإخطار المبكر وتبادل التنبيهات، بما يسمح بتقليص الأضرار والحد من إعادة استهداف الضحايا.

الفرع الثاني: تعزيز تبادل المعلومات والإنذار المبكر.

لم يعد التعاون الدولي في هذا المجال ترفا تكتيكيا بل تحول إلى التزام استراتيجي وقانوني تفرضه مبادئ حسن الجوار، وبذل العناية الواجبة في الفضاء السيبيراني، فالخطر لم يعد يقتصر على الإخلال بأمن المعلومات إنما بات يمس صلب استقرار الدول السياسي والاقتصادي، وتشهد على ذلك السوابق الدولية كالهجوم الذي استهدف منشآت نووية وغيرهم من الهجمات التي تثبت قصور المقاربات الأحادية وضرورة الانتقال إلى استجابة جماعية منسقة.

[1] سندس بن أوذينة، مرجع سابق، ص44.

أولا: الإنذار المبكر السيبيراني كآلية وقائية استباقية.

يعرف الإنذار المبكر السيبيراني في الفقه التقني القانوني بأنه منظومة مؤسسية وإجرائية متكاملة ذات طابع استباقي، تقوم على الرصد المنهجي للمؤشرات الأولية للتهديد وتحليلها، ثم تعميمها على الشركاء والدوليين في الزمن شبه الحقيقي[1].

وتدار هذه المنظومة في غالبية التشريعات المقارنة عبر "مراكز الاستجابة لطوارئ الحاسب الآلي" سواء الوطنية أو القطاعية، والتي تعتبر بمثابة سلطات فنية تتمتع بالاختصاص الوظيفي في تحليل التهديدات واحتواء الحوادث، وتستند هذه المراكز في عملها إلى مصادر استخبارات التهديدات (Cyber Threat Intelligence–CTI)، فنجد قواعد بيانات الهجمات السابقة وتحليل البرمجيات الخبيثة، ورصد أنماط حركة الشبكة غير الاعتيادية، ومؤشرات الاختراق (Indicators of Compromise–IoCs)، إضافة لأساليب وتكتيكات وإجراءات المهاجمين (TTPs).

وظيفيا، لا يقتصر دور الإنذار المبكر على التنبيه بل يمتد ليشمل تفعيل خطط الطوارئ الوطنية، وتقييم نقاط الضعف وعزل الأنظمة المصابة، ومنع الانتشار الأفقي للهجوم، وهو ما يجعله تجسيدا عمليا لمبدأ الوقاية خير من العلاج في القانون الجنائي الرقمي.

ثانيا: الأطر القانونية والمؤسسية للتعاون الدولي.

تتخذ آليات التعاون الدولي في تبادل المعلومات صيغا متعددة يمكن تصنيفها إلى مستويين:

1- المستوى الإتفاقي: يتمثل في الاتفاقيات الثنائية والمتعددة الأطراف التي تهدف إلى تجاوز مبدأ الإقليمية الجنائية الضيق، وتتضمن هذه الصكوك عادة أحكاما نموذجية تتعلق بتوحيد التجريم الإجرامي للجرائم السيبيرانية، وإرساء آلية التبليغ الفوري المشترك، ووضع ضمانات لحفظ سرية البيانات المتبادلة وحماية المعطيات ذات الطابع الشخصي، وتنظيم التعاون القضائي الدولي والمساعدة القانونية المتبادلة في التحقيقات العابرة للحدود[2].

[1] إبراهيم الصافي، **أنظمة الإنذار المبكر ودورها في التصدي للإرهاب**، 2023/01/08، https://trendsresearch.org/ar/insight/، اطلع عليه بتاريخ 2026/04/30، الساعة21:42.

[2] إسماعيل أمحمد، عبد الحليم زوبير، مرجع سابق، ص78.

وتعتبر اتفاقية بودابست لمجلس أوروبا بشأن الجريمة السيبيرانية 2001 النموذج المرجعي الأكثر نضجا، بانضمام أكثر من 65 دولة لكونها أرست معايير المواءمة التشريعية وأنشأت شبكات تعاون شرطي–قضائي دائمة (24/7Network).

2- المستوى المؤسسي التقني: تقوم بتكملته شبكات تنسيق غير تعاهدية تضطلع بدور محوري في بناء الثقة وتبادل المعلومات العملية، ومن أبرزها منتدى فرق الاستجابة FIRST الذي يضم أكثر من 600 فريق معتمد ويشكل منصة موثوقة لتبادل المؤشرات الفنية، والاتحاد الأوروبي عبر وكالة " Cyber Europe " ENISA التي تدير تمرين الدوري لمحاكاة الأزمات السيبيرانية الكبرى واختبار جاهزية الدول الأعضاء، أيضا حلف شمال الأطلس (الناتو) الذي أنشأ بعد هجمات 2007 على استونيا مركز التميز للدفاع السيبيراني CCDCOE، ليصح مختبرا قانونيا وتقنيا لتبادل الإنذارات، أما على المستوى العربي فقط أنشأ الاتحاد الدولي للاتصالات المركز الإقليمي للأمن السيبيراني CSIRT بمسقط، والذي طور منظومة موحدة للفرق العربية، كما وقعت دول مجلس التعاون الخليجي اتفاقية مشتركة لتبادل الإنذارات، ونجد APCERT على المستوى الأسيوي فهذا المشروع يربط فرق أسيا والمحيط الهادئ بآلية تقنية موحدة[1].

ويعد تبادل معلومات استخبارات التهديدات أكثر صور التعاون تطورا، إذ يتيح الاطلاع على IoCs وTTPs، ويتم عبر بروتوكولات معيارية مؤتمتة بما يضمن التشغيل البيني الأمن.

ثالثا: التحديات القانونية والسيادية.

يواجه التعاون السيبراني العربي تحديات قانونية والسيادية التقنية التي تعترض تفعيل التعاون العربي في المجال السيبراني، إذ تبرز معضلة الثقة والسيادة الرقمية بوصفها عائقًا رئيسيًا، خاصة في ظل التخوف من توظيف المعلومات المتبادلة لأغراض استخباراتية أو سياسية بما يمس مبدأ عدم التدخل، كما تشير إلى تضارب الأطر التشريعية الوطنية المتعلقة بحماية البيانات وحرية التعبير، وغياب قاموس موحد للمصطلحات وبروتوكولات تشغيلية مشتركة، فضلًا عن ثقافة عدم الإفصاح عن الهجمات السيبرانية خشية المساس بالهيبة الوطنية أو كشف هشاشة البنى التحتية الحيوية، وهو ما يضعف متطلبات الشفافية في إدارة الأزمات[2]، وبذلك لابد من اعتماد مقاربة عربية إقليمية متكاملة تقوم على إنشاء منصة موحدة للإنذار المبكر تربط المراكز الوطنية ضمن نظام حوكمة يضمن السرية والتناسب، وتطوير تصنيف عربي موحد للحوادث

[1] إسماعيل أمحمد، عبد الحليم زوبير، مرجع سابق، ص79.

[2] المرجع نفسه، ص80.

السيبرانية يحدد درجات الخطورة وآليات الإبلاغ، وتعزيز بناء القدرات عبر التدريب والمحاكاة المشتركة مع إشراك القطاع الخاص، وإرساء بروتوكول تشغيلي عربي قائم على قواعد قانونية شفافة تراعي مبادئ المشروعية، وتحديد الغرض، وحضر الاستخدام المزدوج للمعلومات على غرار ما اعتمده مركز الناتو[1].

يمكن القول، أن الانتقال من منطق السيادة المنفردة إلى منطق السيادة التعاونية في الفضاء السيبيراني هو الضمانة القانونية الوحيدة لمواجهة تهديدات وعصابات رقمية لا تعترف بالحدود.

الفرع الثالث: تعزيز التعاون التقني والفني.

لا يقل التعاون التقني والفني أهمية عن التعاون القضائي إنما قد يشكل شرطا سابقا له، لأن تتبع الأنشطة الإجرامية للعصابات الرقمية يتوقف على إمكانات الرصد والتحليل والاستجابة، وهي إمكانات تتطلب تنسيقا دوليا وتبادلا للخبرات والأدوات والبيانات وفق ضوابط قانونية دقيقة.

أولا: تقاسم الخبرات وتكوين الأطر.

تؤكد الاتفاقيات الدولية ذات الصلة بمكافحة الجريمة المنظمة عبر الوطنية ضرورة دعم الدول لبعضها البعض في مجال تبادل الخبرات وبناء القدرات، وذلك عبر إعداد برامج تدريبية مشتركة، وتنظيم مؤتمرات وورش عمل، وإنشاء مراكز تدريب إقليمية متخصصة. ويكتسي هذا الأمر أهمية بالغة أمام تطور أساليب الهجمات السيبيرانية التي تقوم بها العصابات الرقمية وتعقدها، لاسيما الجرائم ذات الطابع المالي مثل الاحتيال الالكتروني وتبييض الأموال.

كما يقتضي الأمر تحديث المؤسسات القضائية والأمنية وتأهيل الموارد البشرية في مجالات التحقيق الرقمي، وتحليل البرمجيات الخبيثة وتتبع التدفقات المالية الرقمية، بما يضمن فعالية الاستجابة ونجاعة التدخل[2].

[1] إسماعيل أمحمد، عبد الحليم زوبير، مرجع سابق، ص90.

[2] ماجد أحمد الزاملي، **الإستراتيجية الوطنية للتعاون الدولي في مجال مكافحة الجريمة**، 2021/08/03، https://www.ahewar.org/debat/show.art.asp?aid=727111، اطلع عليه بتاريخ 2026/04/30، الساعة 22:18.

ثانيا: استعمال برامج الذكاء الاصطناعي:

يمكن توظيف الذكاء الاصطناعي في التحقيق والرصد الاستباقي للهجمات الإجرامية السيبيرانية، ودعم اتخاذ القرار الأمني، وتحليل الأنماط الإجرامية وكشف عمليات الاختراق والتجسس. غير أن توسع استخدام هذه التقنيات يثير تحديات قانونية وحقوقية، خاصة ما يتصل بحماية الخصوصية الرقمية ومنع التمييز الخوارزمي وضمان الشفافية والمساءلة[1].

وعليه، يقتضي الأمر وضع إطار قانوني يوازن بين متطلبات الأمن السيبيراني وحماية الحقوق الأساسية، مع التنصيص على مبدأ التناسب والضرورة في المعالجة الآلية للبيانات، وقيود استخدام تقنيات التعرف على الوجوه عند الاقتضاء، وآليات رقابة مستقلة على نظم الذكاء الاصطناعي الأمنية.

ثالثا: إبرام تعاقدات مع القطاع الخاص.

يمثل التعاون بين الحكومات والشركات التكنولوجية الكبرى رافعة مهمة لتعزيز القدرة على رصد التهديدات وتبادل المعلومات والاستجابة للحوادث، شريطة احترام قواعد حماية المعطيات والسرية المهنية وحقوق المستخدمين. وتبرز أهمية التعاون في بناء فرق استجابة مشتركة وتبادل مؤشرات الاختراق وتطوير أدوات محاكاة الهجمات ورفع الجاهزية.

غير أن هذا المسار يواجه تحديات كتضارب المصارح وتردد بعض الشركات في مشاركة البيانات خشية التأثير على السمعة أو المصالح التجارية، وقضايا الخصوصية واحتمال إساءة استخدام البيانات خارج الإطار المتفق عليه، إضافة لتأخر الإبلاغ عن الاختراقات لأسباب مالية أو اعتبارية[2].

ورغم ذلك، يظل هذا التعاون ضرورة حتمية لبناء فضاء سيبيراني آمن، لاسيما مع تزايد تهديدات البنية التحتية الحيوية وارتباطها بالأمن القومي.

[1] يحي إبراهيم دهشان، " قواعد المسؤولية الجنائية عن تطبيقات الذكاء الاصطناعي"، **مجلة الشريعة والقانون**، الإمارات العربية المتحدة، م34، ع82، أفريل 2020، ص04.

[2] سندس بن أوذينة، مرجع سابق، ص47.

المبحث الثاني: سبل تعزيز الجهود الدولية في مواجهة العصابات الرقمية.

أفضت الرقمنة المتسارعة إلى توسع الجرائم العابرة للحدود في الفضاء السيبيراني، بحيث لم تعد "العصابات الرقمية" مجرد اعتداءات فردية متفرقة، بل غدت – في كثير من الوقائع – شبكات إجرامية منظمة تتقاطع فيها أدوار التخطيط والتنفيذ وتوزيع العائد الاقتصادي، مستندة إلى أدوات تقنية متقدمة كالاختراق عن بعد، وبرمجيات التجنيد والابتزاز، وسلاسل الإجرام القائم على الخدمات والتشفير وتخفي الأثر. وتتجلى خصوصية هذه الظاهرة في أن آثارها لا تقف عند حدود إقليم دولة بعينها، إذ قد تنفذ الجريمة من دولة، بينما يقع الضحايا في دولة أخرى، وتستخدم البنية التحتية في مكان ثالث وتستضاف الأدلة الرقمية في مواقع متعددة.

انطلاقا من هذه الطبيعة العابرة للحدود تبرز الحاجة إلى تعزيز الجهود الدولية بوصفه مدخلا عمليا وقانونيا لمواجهة العصابات الرقمية، على نحو يوازن بين متطلبات الفعالية الإجرامية من جهة وضمانات حقوق الإنسان وسيادة القانون من جهة أخرى، وهذا ما تفضي له دراستنا اللاحقة من إبراز سبل الجهود الدولية في مواجهة العصابات الرقمية.

المطلب الأول: التحديات القانونية لمكافحة العصابات الرقمية.

في ظل التحولات الجوهرية التي أحدثتها التقنيات الرقمية على بنية الجريمة المنظمة، باتت العصابات الرقمية تشكل تهديدا متصاعدا للأمن الوطني والمصلحة العامة، ولا تقتصر خطورتها على كونها تتخفى خلف طبقات التشفير وهويات مجهولة، بل تتسم أيضا بقدرة عالية للتحايل على أجهزة العدالة الجنائية التقليدية، وإخراج أنشطتها عن نطاق الرقابة المحلية. وبالتالي فالمواجهة القانونية الفعلية لهذه العصابات تطرح تحديات بنيوية متعددة تتقاطع فيها الصعوبات الإجرائية مع القصور التقني والقانوني معا، وهذا ما سندرس في هذا المطلب.

الفرع الأول: إشكالية الاختصاص القضائي.

تعد العصابات الرقمية من أبرز التحديات القانونية المعاصرة، نظرا لطابعها العابر للحدود وامتدادها عبر الفضاء الإلكتروني، مما يعسر تطبيق قواعد القانوني التقليدية المبنية على مبدأ الإقليمية، لذلك سنتناول هذا الفرع على جزأين هما:

أولا: القانون الواجب التطبيق.

1- إشكالية توحيد التشريعات الوطنية.

تتسم الجريمة الالكترونية التي تفرعت عنها العصابات الرقمية بخاصية استحالة حصر ركنه المادي في إقليم دولة بعينها، إذ قد يقع السلوك الإجرامي في دولة فيما تتحقق نتيجته في دولة أخرى أو عدة دول في آن واحد، وينجم عن ذلك تنازع الاختصاص القانوني والقضائي مما يعقد مسار الملاحقة الجزائية وتطبيق العقوبة، وقد تصدت المجتمعات الدولية لهذه الإشكالية عبر منظومة من الجهود متعددة المستويات، أبرزها مؤتمر الأمم المتحدة السابع (ميلانو 1985) الذي دعا إلى تحديث التشريعات الجنائية في مواجهة جرائم الحاسوب، ومؤتمر الأمم المتحدة الثامن (هافانا 1990) الذي أقر جملة من الإجراءات الإلزامية للدول الأعضاء شملت تحديث القوانين الوطنية المتعلقة بإجراءات المتابعة والتحقيق، مصادرة لأصول غير المشروعة، حماية مصالح الدولة وحقوق ضحايا جرائم الانترنت، وأيضا اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية (فيينا 2010) التي جاءت استجابة لتصاعد وتيرة الجرائم المعلوماتية وتنوعها[1].

2- تحديد القانون الواجب التطبيق في الجرائم المعلوماتية.

تعترض مسألة التكييف للنشاط الإجرامي المعلوماتي عقبات بنيوية متعددة وتباينا حادا بين المدارس الفقهية والتشريعات الوضعية، فما يعد جريمة خطيرة في دولة ما قد يصنف كمخالفة بسيطة أو ممارسة مشروعة في دولة أخرى، ذلك نظرا لاختلاف مفاهيم الحرية العبير أو حماية البيانات، فالبعد الدولي للأنشطة الإجرامية المعلوماتية يفرض على المجتمع الدولي القيام ببحوث عن مختلف الوسائل التي تحقق ملائمة لكل أنواع الجرائم الالكترونية، والسعي لتضييق الثغرات القانونية المستغلة في الهروب من الجزاء، واستثمارها في نشر أنشطتهم عبر ربوع العالم.

إن الجريمة المعلوماتية لا يطبق عليها المبادئ المكملة لمبدأ الإقليمية المتمثلة في مبدأ الشخصية والعينية، ذلك راجع لكون بعض الدول تعمل وفق قوانينها على تطبيق مبدأ الإقليمية على اعتباره انه أساسي، في حين نجد دول يقوم قانونها على أن تعتد بمبادئ أخرى، وهذا ما ينتج عنه إشكال قانوني حول

[1] محمد خليفي، " إشكالية الاختصاص القضائي الدولي في مكافحة الجريمة المعلوماتية "، **مجلة الميزان**، د.م، ع01، ديسمبر 2016، ص256.

الاختصاص، لذلك يتوجب على الدول أن تتفق على نوع محدد من المبادئ لفض النزاعات التي قد تقع لاحقا بسبب اختلاف التشريعات الوطنية[1].

ثانيا: صعوبة تحديد الاختصاص القضائي.

1- الاختصاص المكاني.

إن قواعد الاختصاص القضائي تكون بموجب المكان الذي تم فيه السلوك الإجرامي، من خلال الأخذ معايير وضوابط أساسية وهي مكان وقوع الجريمة، أو محل إقامة المتهم، أو مكان القبض على المتهم. وهذا ما يبرز عنه تنازع بين السلوك والنتيجة، ويكون تنازع حاد بين محكمة السلوك الإجرامي (مكان إرسال الفيروس) ومحكمة النتيجة (مكان تدمير البيانات)، ورغم أن الفقه التقليدي يميل لمنح الأولوية لمكان ارتكاب السلوك إلا أنه في طريق الزوال في الجرائم الرقمية. كما أنه يحدث تنازع مع المحكمة التي تم إلقاء القبض على المتهم فيها، غير أن الاختصاص يؤول لمكان ارتكاب الجريمة[2].

2- القانون الأكثر ملائمة.

يتم العمل بهذا المعيار من أجل مراعاة حجم الضرر، وذلك بالأخذ بقانون الدولة التي تعرضت لأكثر الأضرار، إذ أخذت به محاكم القضاء الأمريكي عندما أفضت إحدى محاكم ولاية نيويورك بعدم اختصاصها في قضية تزوير ماركات تجارية أقدم عليها موقع ويب بإقليمها، فتنازلت عن اختصاصها لمحكمة بولاية ميسوري كون أن تلك القضية لم تلحق بها ضررا فعليا يجعلها تدخل في اختصاصها[3].

الفرع الثاني: صعوبات الإثبات الرقمي.

يعد إثبات الجرائم الالكترونية من أعقد التحديات التي تواجه الأنظمة القانونية والقضائية المعاصرة، نظرا للطبيعة الخاصة للدليل الالكتروني الذي يختلف جوهريا عن الأدلة التقليدية، فبينما تعتمد الأدلة المادية على وجود ملموس يمكن ملاحظته وجمعه بالطرق التقليدية، يتسم الدليل الالكتروني بالطابع الرقمي غير المرئي والقابل للتعديل أو الإزالة بسرعة فائقة، مما يجعل عملية اكتشافه واستخراجه وحفظه أمرا بالغ التعقيد.

[1] محمد خليفي، مرجع سابق، ص ص257، 256.

[2] المرجع نفسه، ص257.

[3] المرجع نفسه، ص258.

وتتطلب هذه الخصوصية تطوير منهجيات تحقيقية وفنية متخصصة تتناسب مع الطبيعة الرقمية للبيانات، فضلا عن تعزيز الإطار التشريعي لضمان سلامة الدليل ومشروعية الحصول عليه.

أولا: الخصوصية الفنية للدليل الالكتروني كعائق للإثبات.

تم تعريف الدليل الالكتروني سابقا بأنه مجموعة البيانات أو المعلومات الرقمية المستخلصة من وسائط التخزين أو المنقولة عبر الشبكات، والتي يمكن استقراؤها ومعالجتها فنيا للوقوف على حقيقة الواقعة، وتتجلى صعوبة التعامل معه في النقاط التالية:

1- عدم ظهور الدليل الالكتروني.

يعتمد الدليل الالكتروني في استمداده من بيئة الكترونية خالصة من ذات الطبيعة الرقمية، ولا يمكن كشفه بالطرق التقليدية وإنما قد يحتاج إلى استخدام تقنيات علمية متطورة يجب إتباعها للوصول إليه، لكونه دليلا غير ملموس أو مادي وغير مرئي وغير مقروء[1]، حيث تتجلى الخصوصية الفنية للدليل من خلال كونها أدلة غير مرئية إذ كل ما يتم إنتاجه عن نظم المعلومات من أداة عن الجرائم الرقمية الواقعة بها أو بواسطتها تكون بيانات غير مرئية لا يمكنها أن توضح عن شخصية معينة، كما أن تلك البيانات غير المرئية لا يمكن للإنسان قراءتها إلا عن طريق استخدامه لأجهزة الحاسوب أو الأجهزة الالكترونية التي تكون متخصصة في ذلك[2]. إضافة لكون أغلب الآثار المتخلفة عن تلك الجرائم تكون أثار رقمية غير مرئية لا ترى بالعين المجردة، فهي عبارة عن نبضات الكترونية غير مرئية إذ تصل في حجمها وشكلها ومكان تواجدها لدرجة شبه منعدمة، غير أنه لا يمكن رؤيتها إلا بالاستعانة بأجهزة ووسائل تقنية تظهرها للعيان. كما يتعين على الجهات الأمنية توفير الإمكانيات التقنية تكون عالية الدقة للتمكن من التحقيق في الجرائم المعلوماتية واستقطاب وجذب الكفاءات المهنية التي تكون متخصصة في المجال الالكتروني بما يحقق فعالية جذرية في التحقيقات، ولا يسمح بإعطاء أعذار أو التذرع بانخفاض الميزانيات المادية لسبب يجعل من الدولة عاجزة عن تحقيق العدالة الجنائية الرقمية، بل يجب العمل والتكاثف والقيام بكل ما يلزم ومن شأنه أن يكشف الدليل ويحفظه من الزوال ويتم تقديمه للإدانة فيه[3].

---

[1] الطيبي البركة، "إشكالية الإثبات في الجرائم الالكترونية The issus of proof in cybercri "، **مجلة أفاق علمية**، م11، ع01، أكتوبر 2018، ص269.

[2] المرجع نفسه، ص270.

[3] المرجع نفسه، ص270.

وعليه، لابد من تطوير معايير دولية موحدة للكشف عن تلك الأدلة غير المرئية كاستخدام تقنيات التصوير الرقمي تكون عالية الجودة، وبرامج تحليل البيانات الضخمة، إضافة إلى الغاية الحتمية في إدراج مقررات متخصصة في الطب الشرعي الرقمي ضمن برامج كليات الحقوق، وأيضا مراكز الشرطة لتأهيل الكوادر البشرية على التعامل مع تلك الأنشطة الإجرامية التي ينتج عنها أدلة رقمية غير ظاهرة.

2- سهولة محو الدليل الالكتروني أو تدميره.

من المعوقات التي يمكن أن تعترض عمليات الإثبات في الجرائم الالكترونية هي سهولة محو أدلة الإدانة أو تدميرها في فترة زمنية يسيرة، فالعصابات الرقمية يمكنها محو الدليل الذي يكون ضدها أو تخريبها في أوقات قصيرة إذ لا تتيح للسلطات المعنية من الكشف عن الجريمة، أما حالة علمها بالجريمة فالعصابات تستهدف المحو السريع لعدم تمكين تلك السلطات من إقامة الدليل ضدها، وبالتالي لا تتصل بالفاعلين الأصليين وترجع الجريمة لسبب خطأ في نظام الحاسبة الالكترونية أو الشبكة أو الأجهزة[1].

تجدر الإشارة لقيام أحد مهربي الأسلحة في النمسا بإدخال تعديلات على الأوامر العادية لنظام تشغيل جهاز الحاسبة الالكترونية الذي يستخدمه في تخزين عناوين عملائه والمتعاملين معه، بحيث يترتب على إدخال أمر النسخ أو الطباعة إلى تلك الحاسبة من خلال لوحة مفاتيحه وتدمير كافة البيانات كاملة، ومع أن تعديل برمجة نظام تشغيل الحاسب قد أجري خصيصا بواسطة الفاعل للحيلولة دون نجاح أجهزة الملاحقة في إجراءات التوقع للبحث عن الأدلة[2].

ثانيا: التحديات الإجرائية والميدانية في ملاحقة العصابات الرقمية.

تواجه ملاحقة العصابات الرقمية مجموعة معقدة من التحديات الإجرائية والميدانية، تتجلى في الصعوبات التقنية المرتبطة بطبيعة البيانات الإلكترونية المُخزَّنة عبر حدود جغرافية وسياسية متعددة، مما يستدعي تدخل آليات التعاون الدولي والإنابة القضائية التي غالبًا ما تكون بطيئة وغير متوافقة مع السرعة التي يتسم بها الدليل الرقمي القابل للمحو. وتُفاقم هذه الإشكالية عوائق بشرية ومؤسسية، أبرزها نقص التأهيل التقني لدى رجال إنفاذ القانون[3]، وإحجام الضحايا — خاصة المؤسسات المالية والاقتصادية — عن التبليغ خوفًا من تبعات سمعية أو مالية، ما يوسع "الرقم الأسود" للجريمة ويُغذي إفلات المجرمين من

[1] الطيبي البركة، مرجع سابق، ص271.

[2] المرجع نفسه، ص272.

[3] المرجع نفسه، ص273.

العقاب ويشجع على تكرار الأنشطة الإجرامية الرقمية[1]، كما أن الطبيعة العابرة للحدود للجريمة الإلكترونية تصطدم بمبدأ السيادة الوطنية، حيث لا تملك السلطات المحلية صلاحية الوصول إلى الأدلة المخزنة خارج إقليمها دون إجراءات قانونية معقدة، مما يُضعف فعالية الإثبات ويُعطّل مسار العدالة، ويبرز الحاجة إلى إصلاحات تشريعية ومؤسسية تعزز التخصص البشري، وتنسق بين الأطر الوطنية والدولية لضمان استجابة قانونية فعالة وسريعة تحمي النزاهة الرقمية وتحقق الردع المطلوب ويشجع على تكرار الأنشطة الإجرامية الرقمية[2].

الفرع الثالث: دور الذكاء الاصطناعي في استشراف ورصد العصابات الرقمية.

يعتبر الذكاء الاصطناعي المحرك الأساسي للعصابات الرقمية لممارستها لأنشطتها الإجرامية، لذلك تعمل أجهزة أمن الدولة على استغلاله أيضا لتطوير عملها وتحسينه بخلق نوع من التوازن للحاق بالثورة المعلوماتية، فاعتمدت على مجموعة طرق تقنية لمكافحتها وهي:

أولا: الشرطة الاستباقية.

يعنى بها الردع للجرائم من خلال العمل الاستباقي الشرطي المدفوع بتحليلات للبيانات، والعمل الشرطي الذي يقوم على الأدلة المادية، وللمساعدة على القيام بذلك تتخذ الأجهزة الأمنية أنظمة التخزين السحابي كإجراء أساسي للردع ومنع الجرائم المستحدثة، الذي يمكن من حل مشاكل التخزين مع فرصة ربط الشبكات بعضها ببعض لغرض العمل على الجرائم بشكل يكون أكثر سلاسة وسهولة[3].

ثانيا: الشرطة الرقمية.

المقصود بها تطوير أجهزة الشرطة لتعتمد على الأجهزة المتطورة والتقنيات الحديثة لتقوم بأعمال رجال الشرطة حتى توفر الاستفادة من الأدلة الرقمية بشكل كبير، التي يمكن الحصول عليها من خلال لقطات الدوائر التلفزيونية المغلقة ووسائل البريد الالكتروني وسجلات الهاتف، وذلك ما يدعو لضرورة وجود

[1] الطيبي البركة، مرجع سابق، ص274.

[2] المرجع نفسه، ص274.

[3] نورة أمينة الأخنش، محمد العيداني، " الذكاء الاصطناعي لجابهة الجريمة الالكترونية Artificial intelligence as a mechanism to confront cybercrime "، **مجلة القانون والعلوم البينية**، م02، ع02، سبتمبر 2023، ص536.

تعاون قانوني باستحداث روابط بين المؤسسات المختلفة حتى تقدم الأدلة الرقمية بسهولة ودون تباطؤ، فالشرطة الرقمية حقيقة بلا لأقنعة أهدافها تكمن في فرض الرقابة الصارمة على مواقع الشبكة المعلوماتية[1].

ثالثا: التحقيق الرقمي.

يقوم بالاعتماد على شبكة الانترنت في رفع الملفات الرقمية للقضايا التي تكون بها أدلة جنائية، ذلك لاستخدامها من طرف المسؤولين، حيث لابد من تحول الحكومة بكاملها لحكومة رقمية حتى يتم رفع ملفات الجرائم، وقبلها لابد من تفعيل الهوية الرقمية إذ بتوفر هوية مستخدم الأنترنت تبرز لقوات الأمن حلول تمكنها من منع الجريمة الالكترونية والكشف عن العصابات الرقمية، التي قد تكون هذه الخاصية ذات فعالية في التحليل بسهولة وتقليل الوقت لحل القضايا، مثل إثبات عمر الهواتف الذكية عن طريق إعطاء نسخة رقمية من الهوية فتزيد سلامة المستخدمين للأنترنت[2].

يمكن تعريف التحقيق الرقمي على أنه عملية تحقيق في الجرائم التي تكون استخدمت لها أي نوع من أجهزة الحوسبة كالخوادم وأجهزة الكمبيوتر سواء الثابتة أو المحمولة، والهواتف المحمولة والأجهزة اللوحية، الكاميرا الرقمية وأجهزة الشبكات، أجهزة أنترنت الأشياء وكل جهاز من شأنه أن يخزن البيانات.

المطلب الثاني: الإجراءات الجنائية والتحقيقية.

تعد الإجراءات الجنائية والتحقيقية في الفضاء السيبيراني من أهم المجالات القانونية المعاصرة التي تتفاعل فيها متطلبات العدالة الجنائية مع تطورات التكنولوجيا الرقمية، حيث انعكس انتشار الحوسبة وتدفق المعلومات عبر الانترنت على طبيعة الجريمة والدفاع عنها، مما استدعى إعادة صياغة الإطار القانوني والتنظيمي لضمان الحفاظ على حقوق الأفراد وحرياتهم، في الوقت الذي لا يقل عنه من أهمية حماية المجتمع من أنشطة العصابات الرقمية، وتبرزت أهمية هذا المطلب في ضوء التحديات التي تواجه سلطات الإنفاذ القانوني في مواجهة العصابات الرقمية، سواء من حيث انقراض الأدلة الرقمية أو تعقيدها أو عدم وضوح نطاق الاختصاص بين الجهات المعنية، مما يفرض تبني منهجية قانونية متكاملة تجمع بين الإجراءات التحقيقية والإجراءات الجنائية السليمة، مع مراعاة خصوصية البيانات الرقمية وحماية الخصوصية وفقا لأعلى معايير القانون الدولي والقانون المحلي.

[1] نورة أمينة الاخنش، مرجع سابق، ص536.

[2] المرجع نفسه، ص537.

الفرع الأول: إجراءات الجهات المعنية بالمواجهة.

تمثل أجهزة الشرطة إحدى الركائز الجوهرية لاستقرار المجتمعات وصون كيانها، إذ تعد أيا كان النظام الاجتماعي أو السياسي أو الاقتصادي السائد التجسيد الطبيعي للسلطة العامة المنوط بها حماية الجماعة منكل من تسول له نفسه العبث بالنظام القانوني أو المساس بالأمن العام الذي كفله المشرع بنصوصه الموضوعية والإجرائية على حد سواء.

ولما كانت الجريمة ظاهرة اجتماعية متطورة بطبيعتها تساير ركب التقدم العلمي والتكنولوجي وتستثمر معطياته في ابتكار صور إجرامية مستحدثة، فقد بات لزاما على الجهاز الأمني أن يواكب هذا التطور باستحداث إدارات متخصصة لمكافحة الأنماط الحديثة من الإجرام، ولاسيما جرائم العصابات الرقمية التي أفرزتها العولمة، نتيجة الاعتماد على التقنيات الرقمية المتطورة.

أولا: مراحل المكافحة الشرطية للعصابات الرقمية.

إن مواكبة التطور التقني ومجابهة الصور المستحدثة من الإجرام المعلوماتي، تستلزم من الجهات الأمنية المتخصصة تبني سياسية مكافحة قائمة على أسس علمية وتكنولوجية رصينة، تتوزع على مرحلتين متكاملتين هما:

1- المرحلة السابقة على وقوع الجريمة.

تعتمد أجهزة الشرطة المنوط بها مكافحة الجرائم المعلوماتية في هذه المرحلة على جملة من الإجراءات الوقائية والاستباقية الهادفة للحد من وقوع الجريمة قبل تحققه[1]، ويمكن إجمالها فيما يلي:

أ- الإجراءات الوقائية.

تتبنى الاستراتيجية الوقائية لمكافحة الجرائم المعلوماتية مقاربة شاملة تدمج بين الأبعاد التقنية والتشريعية والرقابية، وهذا من خلال إعداد البحوث الفنية المتخصصة ووضع خطة تأمين متكاملة لشبكة المعلومات الخاصة بالجهاز الأمني، والعمل على رسم الخطط الأمنية ودراستها في المجال المعلوماتي والمتابعة المستمرة لأحداث الجرائم المرتكبة دوليا وإقليميا ومحليا، إضافة لمتابعة التراخيص الصادرة للشركات والمكاتب العاملة في مجال نظم المعلومات والانترنت، مع ضرورة الرقابة على مقاهي الانترنت ومتابعة

[1] طاهر محمود أبو قاسم، **الجرائم المعلوماتية صعوبات وسائل التحقيق فيها وكيفية مواجهتها**، مصر: المنظمة العربية للتنمية الإدارية جامعة الدول العربية، ط01، 2019، ص220.

العاملين بهذا المجال[1] والمرور على متاجر بيع المصنفات الفنية، وذلك لإبداء الرأي والمشورة وتقديم المساعدات الفنية للجهات المعنية والبحث في مدى ملائمة التشريعات الجنائية القائمة لمواجهة الجرائم المعلوماتية، وتدعيمها بإنشاء قاعدة بيانات متكاملة بالجرائم المعلوماتية لتعزيز التعاون الدولي مع الأجهزة الأمنية النظيرة وتوعية مستخدمي شبكة الانترنت مع جميع فئات المجتمع[2].

ب- متابعة محتوى الانترنت.

أصبح من الأهمية في إطار العمل الشرطي المعلوماتي متابعة محتوى شبكة الانترنت وما تتضمنه من معلومات وبيانات، وذلك في ضوء اعتماد العناصر الإجرامية ولاسيما العصابات الرقمية على التقنيات الحديثة في تنفيذ مخططاتها، إذ تستخدم العصابات الرقمية الفضاء السيبيراني لتداول المعلومات فيما بينها، وإصدار التكليفات لتنفيذ عملياتهم واستقطاب عناصر جديدة وتمويل أنشطتهم.

وتعد عملية متابعة محتوى الشبكة عملية بالغة الصعوبة نظرا لما تحويه من حجم هائل من المعلومات والمواقع، وافتقار العالم لمنهجية موحدة لتنفيذ هذا الإجراء، إضافة لصعوبة استمرار المتابعة على مدار الساعة، لذلك بات من الضروري تنظيم هذه الأعمال وتحديد أهدافها بدقة بالاستعانة بأحدث الأنظمة المعتمدة في المتابعة والتحليل[3]، وذلك على النحو التالي:

- **نظرية المتابعة على شبكة الانترنت.**

تقوم هذه النظرية على ضرورة التحديد الدقيق للعناصر العملية وتشمل الزمان، والشخص أو الموقع المراد متابعته، والسبب الموجه للمتابعة، يستلزم أيضا تشكيل فريق عمل متخصص يمتلك الخبرة والقدرة على تنفيذ تلك المهام، وتوزيع الأعمال على أعضائه بشكل منظم، وتحديد المعلومات المستهدفة بدقة، وتحليل البيانات التي تحتاجها المؤسسة الأمنية، وتطوير الأدوات المستخدمة من برامج وأجهزة بصورة مستمرة[4].

تستدعي الضرورة أن يضم فريق العمل العناصر أخرى مثل، فنيون تقنيون على دراية كاملة بشبكة الانترنت وآليات عملها، اختصاصيون في تحليل المعلومات وتصنيفها، فنيون لصيانة أجهزة الحاسب الآلي

[1] طاهر محمود أبو قاسم، مرجع سابق، ص221.

[2] المرجع نفسه، ص221.

[3] المرجع نفسه، ص222.

[4] المرجع نفسه، ص222.

المستخدمة في عملية المتابعة، ومترجمون يجيدون عدة لغات لتفسير وترجمة المعلومات المنشورة بلغات أجنبية على شبكة الانترنت[1]. ويمكن إضافة محللين قانونيين يضمنون أن تتم عمليات المتابعة في إطار المشروعية حسب النصوص الدستورية لحماية الحقوق والحريات.

- **أهداف المتابعة والتحليل.**

تتمحور أهداف المتابعة والتحليل في الجرائم الالكترونية في تحديد وتقييم الرأي العام والوصول إلى تصور شامل عن آراء الأشخاص واتجاهاتهم، والبحث السريع عن التهديدات المحتملة وتوقعها قبل وقوعها، وتحديد التهديدات الأمنية المختلفة ومحاولة استباقها قبل تجسدها على أرض الواقع[2].

في كل الأحوال لابد على الشرطة من شراء البرامج اللوجستية وتحديث البرامج المستخدمة بصفة دورية، ذلك لغرض المتابعة لمحتوى الانترنت من رسائل وصور للمستخدمين العاديين ومواكبة تطور أدوات العصابات الرقمية المستحدثة.

2- المرحلة اللاحقة على وقوع الجريمة.

رغم اطلاع الجهاز الأمني بالدور الوقائي في المرحلة السابقة لوقوع الجريمة، إلا أن الواقع العملي يشهد استمرار وقوع الجرائم المعلوماتية المنظمة من طرف العصابات الرقمية، وهو ما يستوجب من إدارات البحث المعنية الاضطلاع بدورها لكشف الفاعلين من العصابات وتقديمهم للعدالة، ويتجلى ذلك من خلال إجراءات التحقيق الجنائي ومراحل المواجهة الفعلية للأنشطة الإجرامية المعلوماتية، فضلا عن الأدوات التقنية التي يستعين بها المحققين الجنائيين في عمليات البحث عن الأدلة عبر شبكات الانترنت، وذلك على النحو الآتي:

- **الدور الأمني في المواجهة.**

تتمحور الاستراتيجية الأمنية في مكافحة الجرائم المعلوماتية عبر مسار إجرائي متكامل، يستهل بمرحلة الاستجابة الإجرائية من خلال قنوات البلاغات، ثم ينتقل إلى الدور العملي والتقني المتمثل في حماية الأنظمة وتفعيل آليات التحري الرقمي لتعقب الأثر التكنولوجي وتحديد هوية الجناة[3]، وتكتمل هذه المنظومة بمرحلة إنفاذ القانون عبر إجراءات الضبط والتقديم للمساءلة الجنائية، مع الالتزام الصارم بمبادئ

[1] طاهر محمود أبو قاسم، مرجع سابق، ص222.

[2] محمد خليفي، مرجع سابق، ص222.

[3] المرجع نفسه، ص224.

الشرعية الإجرائية والموضوعية، وهذا لضمان مواءمة التدابير الأمنية مع الأطر التشريعية والاتفاقيات المنظمة[1].

ثانيا: أهم أدوات البحث في جرائم العصابات الرقمية.

يستعين العاملون في مجال التحقيق الجنائي والبحث في جرائم المعلومات التي تقوم بها العصابات الرقمية بمجموعة من الأدوات والمواقع والبرامج التي تسهم في عمليات البحث والمتابعة والتعقب، بهدف الوصول للحقيقة وضبط الجناة المنظمين الالكترونيين وتقديمهم للعدالة، ومن أبرز هذه الأدوات:

– **موقع Viewdns.info:** يتميز هذا الموقع بأنه يدون أغلب بيانات بروتوكول الانترنت (IP) للمستخدمين على الشبكة، ومن خلاله يمكن معرفة تاريخ بروتوكول انترنت معين، مع تحديد أول شخص استخدمه للاتصال بالشبكة[2].

– **موقع Stolencamerafinder.com:** يتميز هذا الموقع بقدرته على تحديد الجهاز الذي تم استخدامه في عرض صور بعينها على الشبكة، وتحديد ما إذا كانت تلك الصور قد عرضت على مواقع أخرى أم لا، حتى إذا تم تعديلها أو تغييرها باستخدام برامج معالجة الصور ك"لفوتوشوب"، وذلك من خلال تحليل المعطيات الرقمية للصورة (EXIF) سواء التقطت بكاميرا أو بهاتف، ويستخدم هذا الموقع بصفة خاصة في الجرائم المعلوماتية المتعلقة بنشر صور الإباحية، والاستغلال الجنسي للأطفال وجرائم التشهير، وكلهم أنشطة تقوم العصابات الرقمية بممارستهم[3].

– **موقع Trendsmap.com:** يساعد هذا الموقع في تحديد خاصية (الهاشتاج) ومكانه الجغرافي على مواقع التواصل الاجتماعي (Facebook–Tweeter)، مما يسمح بتتبع انتشار الموضوعات وتحديد بؤر النشاط الإجرامي المنظم[4].

الفرع الثاني: استراتيجيات جمع الأدلة الرقمية وتحليلهاDigital Forensics.

يعد جمع الأدلة الرقمية وتحليلها من أبرز الإشكالات التي تواجه أجهزة العدالة الجنائية في البيئة الرقمية المعاصرة، بالنظر للتحول العميق الذي عرفته وسائل ارتكاب الجريمة. فقد أصبحت الحواسيب والهواتف

[1] محمد خليفي، مرجع سابق، ص224.

[2] المرجع نفسه، ص225.

[3] طاهر محمد أبوقاسم، مرجع سابق، ص225.

[4] المرجع نفسه، ص225.

الذكية، والشبكات المعلوماتية، ومنصات التواصل الاجتماعي، والخدمات السحابية، فضاءات افتراضية يمكن أن ترتكب من خلالها جرائم متنوعة، أو تستخدم كوسيلة لإخفاء آثارها أو تسهيل تنفيذها[1].

وتتميز الأدلة الرقمية بطبيعة خاصة تختلف عن الأدلة التقليدية، فهي أدلة غير مادية في أصلها، سريعة الزوال، قابلة للتعديل أو المحو خلال وقت وجيز، وقد تكون موزعة عبر أجهزة أو خوادم تقع في دولة مختلفة، لذلك فإن التعامل معها يتطلب كفاءات دقيقة وقانونية متخصصة، فضلا عن الالتزام بإجراءات دقيقة تضمن سلامتها وحجيتها أمام القضاء، فالأدلة الرقمية أصبحت عنصرا مركزيا في منظومة الإثبات الجنائي المعاصر[2].

وتخضع عملية جمع الأدلة الرقمية وتحليلها إلى قواعد قانونية وتقنية صارمة، غايتها ضمان سلامة الدليل والمحافظة على مصداقيته، ومنع أي عبث أو تغيير قد يؤدي إلى استبعاده أو الطعن فيه. فهو لا يستمد قيمته الإثباتية من محتواه فقط بل أيضا من مشروعية طريقة الحصول عليه وسلامة إجراءات حفظه وتحليله.

أولا: تقنيات جمع وتحليل الأدلة الرقمية.

تبدأ عملية التحري الرقمي منذ اللحظة الأولى للاشتباه في وقوع أنشطة إجرامية من عصابات رقمية أو استخدام الوسائل الرقمية في ارتكابها، هنا في هذه المرحلة يتعين على فريق التحقيق المختص تأمين مسرح الجريمة الرقمي، سواء كان جهازا معلوماتيا، أو شبكة الكترونية، أو حسابا رقميا، أو خادما سحابيا، وذلك دون المساس بالمحتوى أو إفساد الخصائص التقنية للبيانات[3].

ويقتضي تأمين الدليل الرقمي اتخاذ تدابير فنية دقيقة منها عزل الأجهزة محل الاشتباه عن الشبكة عند الضرورة، ومنع أي اتصال خارجي قد يؤدي إلى محو البيانات أو تعديلها، مع مراعاة طبيعة البيانات المتطايرة التي قد تزول بمجرد إطفاء الجهاز أو قطع الاتصال عنه. ولهذا قد لجأ الخبراء إلي تحليل الذاكرة الحية قبل إغلاق الجهاز بغرض استخراج البيانات المؤقتة، مثل كلمات المرور، ومفاتيح التشفير، والعمليات الجارية، والاتصالات الشبكية المفتوحة[4].

---

[1] إسماعيل أمحمد، عبد الحليم زوبير، مرجع سابق، ص81.

[2] المرجع نفسه، ص82.

[3] محمد خليفي، مرجع سابق، ص82.

[4] المرجع نفسه، ص82.

ومن أهم التقنيات المعتمدة في هذا المجال تقنية التصوير الجنائي للأقراص الصلبة Disk (Imaging)، أو النسخ الجنائي (Forensic Imaging) والتي تقوم على إنشاء نسخة طبق الأصل من وسيط التخزين دون التأثير في البيانات الأصلية، ويتم ذلك غالبا باستعمال أدوات متخصصة تمنع الكتابة مثل أدوات منع الكتابة (Write Blockers) على الوسيط الأصلي، مع احتساب القيم الرقمية للتحقق أو ما يعرف بقيم التجزئة (Hash Values) مثل MD5 أو SHA، وذلك لإثبات أن النسخة المطابقة لم تتعرض لأي تغيير منذ استخراجها إلى غاية تقديمها أمام القضاء.

كما تشمل عملية التحليل الرقمي فحص سجلات الدخول والملفات المحذوفة أو المشفرة والبرمجيات المثبتة، وسجل المتصفح، بيانات الاتصال، البريد الإلكتروني، الوسائط المتعددة، البيانات الوصفية التي تكشف معلومات مهمة حول تاريخ إنشاء الملفات وتعديلها ومصدرها، وتساعد هذه المعطيات في بناء التسلسل الزمني للوقائع، وتحديد هوية المستخدمين المحتملين وربط السلوك الرقمي بالفعل الإجرامي محل المتابعة، وتتم هذه العملية ضمن إطار ما يعرف بسلسلة الحيازة (Chain of Custody)، وهي مجموعة من الإجراءات التوثيقية التي تبين كل مرحلة مر بها الدليل الرقمي منذ ضبطه أو استخراجه، مرورا بتخزينه وتحليله وصولا إلى عرضه أمام الجهة القضائية المختصة، ويجب أن تتضمن سلسلة الحيازة بيانات دقيقة حول هوية الشخص الذي تولى التعامل مع الدليل وتاريخ ووقت كل إجراء، وطبيعة العملية التي تمت عليه ومكان حظه وأي خلل في هذه السلسلة قد يثير الشك في سلامة الدليل، ويفتح المجال للطعن في حجيته[1].

ثانيا: ضوابط احترام خصوصية الأشخاص والبيانات.

رغم الأهمية البالغة للأدلة الرقمية في كشف العصابات الرقمية وملاحقتهم فإن جمعها لا يجوز أن يتم على حساب الحقوق والحريات الأساسية للأفراد، فالتفتيش أو الولوج إلى الأجهزة والحسابات الإلكترونية يمس بطبيعته الحق في الخصوصية وسرية المراسلات، وحماية البيانات الشخصية وهي حقوق مكرسة في التشريعات الوطنية والمواثيق الدولية.

لذلك تشترط أغلب التشريعات ضرورة الحصول على إذن قضائي مسبق ومسبب قبل مباشرة إجراءات التفتيش أو الحجز الإلكتروني، خاصة إذا تعلق الأمر بالدخول إلى أجهزة الحاسوب أو الهواتف الذكية أو الحسابات البريدية، أو قواعد البيانات، أو خدمات التخزين الحسابي، ويجب أن يحدد الإذن القضائي نطاق

[1] إسماعيل أمحمد، عبد الحليم زوبير، مرجع سابق، ص82.

الإجراء من حيث الزمان والمكان والموضوع، ذلك حتى لا يتحول التفتيش الرقمي إلى إجراء عام وغير محدد يمس بيانات لا علاقة لها بالفعل الإجرامي الرقمي[1].

يقتضي احترام الخصوصية الالتزام بمبدأ التناسب بحيث لا يجوز توسيع نطاق التفتيش أو الحجز إلى بيانات لا صلة لها بالفعل محل التحقيق، كما ينبغي مراعاة مبدأ الضرورة فلا يتم اللجوء للوسائل الأكثر تدخلا إلا حالة كانت لازمة لكشف الحقيقة، كما لابد من حماية بيانات الغير الذين قد تظهر معطياتهم عرضا أثناء عملية التحليل خاصة إذا تعلق الأمر بأسرار مهنية أو مراسلات خاصة أو معلومات حساسة.

أما على المستوى الدولي فساهمت اتفاقية بودابست المتعلقة بالجريمة السيبيرانية في إرساء مبادئ عامة لتبادل الأدلة الرقمية والتعاون القضائي بين الدول، خاصة في الحالات التي تكون فيها البيانات مخزنة خارج إقليم الدولة التي تباشر التحقيق، وتبرز أهمية هذا التعاون في ظل الطبيعة العابرة للحدود التي تمتاز بها أنشطة العصابات الرقمية مع صعوبة الحصول على البيانات من مزودي الخدمات الأجانب دون إطار قانوني واضح[2].

الفرع الثالث: إجراءات الضبط والحجز الإلكتروني.

أدى التطور التكنولوجي لإعادة النظر في إجراءات الضبط والحجز التقليدي، إذ الجرائم الالكترونية يكون محل الضبط فيها بيانات أو برمجيات أو رسائل الكترونية أو سجلات دخول ومحتوى منشور على موقع الكتروني، والتي تتسم بأنها عناصر غير مادية.

ويقصد بالضبط الالكتروني تلك العملية التي تقوم بها السلطة المختصة لرصد وتحديد وجمع وتأمين الأدلة الرقمية المتعلقة بالهجوم الرقمي المحتمل، وتكون موجودة في أجهزة الكترونية أو شبكات رقمية أو وسائط تخزين، مع ضرورة المحافظة على سلامة محتواها وخصائصها التقنية، إذ يتعدى الضبط الالكتروني من حجز الجهاز المادي ليشمل أيضا نسخ البيانات أو حفظها أو استخراجها بطرق فنية تضمن عدم تغييره[3].

[1] إسماعيل أمحمد، عبد الحليم زوبير، مرجع سابق، ص83.

[2] المرجع نفسه، ص83.

[3] المرجع نفسه، ص84.

وتكمن أهمية هذا الإجراء في أن الدليل الرقمي قد يكون حاسما في إثبات الهجمات الرقمية أو نفيها خاصة في تلك التي تكون آثارها رقمية دقيقة، كتحديد مصدر الاختراق أو تتبع العناوين الشبكية، إثبات التحويل المالي أو كشف هوية صاحب الحساب المستخدم في الابتزاز أو التشهير.

أولا: شرعية الضبط الالكتروني للعصابات الرقمية.

يعد الضبط الالكتروني إجراء تمهيدي ذا طبيعة حساسة لأنه يوازن بين مقتضيات البحث عن الحقيقة وحماية الحقوق والحريات الفردية، لذلك يخضع هذا الإجراء لمبدأ الشرعية الإجرائية فلا يجوز مباشرته إلا استنادا لنص قانوني يجيزه، ووفق إجراءات وضمانات يحددها القانون، لكن كأصل عام لا يجوز إجراء التفتيش أو الحجز الالكتروني إلا بإذن قضائي مسبق، باستثناء الحالات التي يقررها القانون صراحة، مثل حالة التلبس أو الضرورة الإجرائية العاجلة، ويكون الإذن محددا وواضحا فيمكن من تبيين طبيعة الجريمة محل التحقيق والأجهزة أو الأنظمة المراد تفتيشها، والبيانات المطلوب ضبطها والمدة الزمنية التي يشملها الإجراء.

تشمل عملية الضبط الالكتروني عادة حجز الحواسيب والهواتف الذكية، الأقراص الصلبة، بطاقات الذاكرة والخوادم، أجهزة التخزين الخارجية، كلها تضبط في حالة كانت تحتوي على بيانات يشتبه في صلتها بالهجوم الرقمي للعصابات الرقمية، كما يمكن الاكتفاء بنسخ جنائي للبيانات محل التحقيق حفاظا على استمرارية المرفق أو النشاط الاقتصادي لخوادم المؤسسات أو أنظمة حيوية[1]، وذلك باستعمال أدوات جنائية رقمية متخصصة تسمح بأخذ نسخة مطابقة للأصل دون المساس بالبيانات الأصلية، وهذا تطبيقا لمبدأ "النسخ دون تعديل"، كما يجب توثيق كل خطوة ضمن سلسلة الحيازة ابتداء من لحظة اكتشاف الدليل أو ضبط الجهاز إلى غاية تقديم التقرير الفني أمام المحكمة. ويفضل أن يتضمن التقرير الفني بيان الأدوات المستعملة وطريقة التحليل والقيم الرقمية للتحقق، والنتائج المستخلصة حتى يكون قابلا للمناقشة القضائية.

ثانيا: صعوبات وتحديات الضبط الالكتروني.

تواجه إجراءات الضبط الالكتروني عدة صعوبات عملية وقانونية ترجع معظمها إلى الطبيعة الخاصة للبيانات الرقمية، ومن أبرز تلك الصعوبات نجد قابلية البيانات للمحو أو التغيير خلال وقت قصير، سواء

[1] إسماعيل أمحمد، عبد الحليم زوبير، مرجع سابق، ص84.

بفعل الجاني أو بفعل أنظمة الحذف الآلي أو التشفير أو التخزين المؤقت، كما أن بعض التطبيقات تعتمد على الرسائل ذاتية الاختفاء أو التشفير التام بين الأطراف مما يزيد من صعوبة الوصول للدليل.

ومن التحديات المهمة أيضا تخزين البيانات في خدمات سحابية تقع خارج إقليم الدولة، وهو ما يثير إشكالات مرتبطة بالاختصاص القضائي والسيادة الوطنية، إذ لا تستطيع السلطات الوطنية غالبا الحصول على البيانات مباشرة، بل يتعين عليها اللجوء لآليات التعاون القضائي الدولي مثل الإنابة القضائية، المساعدة القانونية المتبادلة، الاتفاقيات الثنائية أو متعددة الأطراف، والتعاون مع مزودي الخدمات الرقمية وفق القنوات القانونية المعتمدة[1].

المطلب الثالث: الأجهزة الدولية للتصدي للعصابات الرقمية.

يشهد النسق الجنائي المعاصر تحولا بنيويا جوهريا مع بروز ظاهرة العصابات الرقمية المستحدثة عن الجريمة المنظمة العابرة للحدود، فلم تعد هذه العصابات مجرد تجمعات افتراضية عابرة بل أضحت كيانات إجرامية ذات هياكل معقدة، تستغل الثغرات التقنية والفجوات التشريعية لتنفيذ أنشطتها الإجرامية، مستفيدة من طبيعة الفضاء اللامركزي السيبيراني وإشكالات الاختصاص القضائي.

وفي إطار هذا التوجه العالمي تتنوع الأجهزة الدولية المعنية بمكافحة العصابات الرقمية لتشمل منظمات شرطية كبرى، ووحدات متخصصة في مراقبة الشبكة العنكبوتية، ومراكز تقنية لتلقي البلاغات وتحليل البيانات، ويمكن تأطير هذه الأجهزة خلال دراستنا في هذا المطلب.

الفرع الأول: المنظمة الدولية للشرطة الجنائية (الأنتربول).

في ظل تسارع التحولات الرقمية تبرز منظمة الأنتربول كخط الدفاع الأول ضد العصابات الرقمية التي أعادت صياغة مفهوم الجريمة المنظمة عبر استغلال الفضاء السيبيراني للانتشار دون قيود جغرافية، ولا يكتفي دور المنظمة بالتنسيق السياسي بل يتجه فعالية نحو توحيد جهود إنفاذ القانون، وذلك عبر منصات ذكية لتبادل البيانات الاستخباراتية حول الهجمات والعمليات غير المشروعة، كما تزود الأجهزة الوطنية بأدوات تحليلية وتدريب متخصص لرصد الشبكات الإجرامية الافتراضية، وتتبع تدفقات الأموال المخفية، بهدف تفكيك بنياتها المعقدة وضمان أمن المجتمعات الرقمية أمام التهديدات التي تتجاوز الحدود

[1] إسماعيل أمحمد، عبد الحليم زوبير، مرجع سابق، ص85.

السياسية، وفيما يلي سنبرز دور منظمة الدولية للشرطة الجنائية في التصدي للعصابات الرقمية والهجمات السيبيرانية.

أولا: نشأة المنظمة الدولية للشرطة الجنائية.

تُعزى فكرة إنشاء المنظومة الدولية للشرطة لجنائية إلى بدايات القرن العشرين بوصفها استجابةً لحاجة ملحّة إلى التعاون عبر الحدود لملاحقة الجرائم ذات الطابع العادي؛ فقد شهدت في 1904/05/18 صدور المبادرة الأولى الرامية إلى تنظيم هذا التعاون في قالب مؤسسي يتيح تبادل المعلومات الشرطية، غير أنّ اندلاع الحرب العالمية الأولى سنة 1914 حال دون استمرارية هذا المسعى، بما ترتّب عليه من توقف عملي. وبعد تجاوز آثار الحربين، أعيد بناء الإطار التنسيقي تدريجياً، إذ عُقدت سنة 1923 خطوة مركزية لبعث التنظيم الدولي للشرطة الجنائية، ثم عادت الديناميكية من جديد في أعقاب الحرب العالمية الثانية سنة 1946، على نحو مكّن من ترسيخ قواعد التعاون وآلياته. وتوِج هذا التطور باعتماد قواعد وتنظيمات أكثر وضوحاً، فتم في سنة 1956 استكمال جانب مهم من النظام الأساسي وترتيب الوظائف المؤسسية، مع الإشارة إلى أن تطبيق بعض الأحكام التنظيمية قد تم لاحقاً. وفضلاً عن التأصيل التاريخي فإن عمل المنظمة يقوم على ضوابط قانونية تقيد اختصاصها؛ إذ تتركز في مكافحة الجرائم العادية وتيسير إجراءات البحث والتبادل الشرطي، مع حظر أن تتحول إلى أداة للنزاع السياسي أو العسكري أو ما يماثله من مجالات لا تدخل ضمن غايتها، كما تُمارس وظائفها عبر أجهزة المنظمة والجهات الوطنية المختصة، بما يكفل وحدة منهج العمل وفعاليته على المستوى الدول[1]، وهذه الأجهزة تتمثل في الجمعية العامة، والأمانة العامة، والمكاتب المركزية الوطنية، واللجان المتمثلين في اللجنة التنفيذية للأنتربول ولجنة الرقابة على محفوظات الأنتربول، إذ يقوم كل جهاز بمهامهم بما يحقق أهداف المنظمة[2].

ثانيا: اختصاصات منظمة الأنتربول.

استنادا إلى الإطار القانوني المنظم لعمل الأنتربول المتجسد في قانونها الأساسي، تسند لهذه المنظمة لجملة من الاختصاصات التي يمكن تلخيصها على النحو الآتي:

[1] قاسم محجوبة، " الأنتربول آلية دولية لمكافحة الجريمة المنظمة العابرة للحدود"، **مجلة البحوث في الحقوق والعلوم السياسية**، م09، ع01، جويلية 2023، ص141.

[2] المرجع نفسه، ص ص146، 145.

1- الاختصاصات العامة.

تتمحور الاختصاصات العامة للمنظمة حول تعزيز التعاون الدولي في مجال تبادل المعلومات والبيانات الجنائية بين الدول الأعضاء، بوصفها ركيزة أساسية لملاحقة الجريمة العابرة للحدود في مرحلتي التحقيق والمحاكمة[1]، وتضطلع المنظمة بمكافحة طائفة واسعة من جرائم القانون العام ذات الطابع الدولي، لاسيما الجرائم المنظمة والجرائم السيبرانية، حيث ينظر إلى هذه المهام كاختصاص أصيل للمنظمة يهدف إلى حماية الأمن الدولي وصون استقرار المجتمعات، وهذا عبر توفير بيانات شاملة لرصد تحركات المجرمين وتعقب الأنشطة الإجرامية والوثائق المزورة والممتلكات المسروقة، وعمليات الاختراق[2].

2- الاختصاصات الخاصة.

تنصرف الاختصاصات الخاصة للمنظمة إلى الجوانب العملية والتقنية والتدريبية الداعمة لأجهزة الأمن الوطنية، إذ تعمل المنظمة على رفع كفاءة الكوادر البشرية وتطوير المؤسسات الشرطية عبر برامج تدريبية متخصصة[3]، وتقديم الدعم الميداني في مجالات الإجرام ذات الأولوية كالإجرام المالي والتقني الذي تقوم به العصابات الرقمية، كما توفر المنظمة خدمات الاتصالات الشرطية المأمونة الذي يقوم على ثلاثة مرتكزات وهي (I-24/7) تعمل وفق نظام أساسي، فتتيح التبادل الفوري للمعلومات الحساسة على مدار الساعة، مدعومة بقواعد بيانات تقنية متطورة تشتمل على الأدلة الجنائية البيومترية كالبصمات والحمض النووي، وبيانات وثائق السفر المسروقة وسجلات الأشخاص المطلوبين، مما يسهم في تنسيق الجهود الدولية لضبط المجرمين الفارين وتحقيق العدالة الجنائية المرجوة[4].

ثالثا: دور الأنتربول في التصدي للعصابات الرقمية.

تعتمد هذه المنظمة على نظام اتصال مركزي من خلال مراكز اتصالات مع الدول المركزية فيتم من خلال الجمعية العامة واللجنة التنفيذية بواسطة السكرتارية العامة، ونظام اتصال عبر مراكز اتصال إقليمية، حيث أنشأت المنظمة الدولية للشرطة الجنائية سنة 2003م وحدة خاصة لمكافحة جرائم التكنولوجيا، كما قامت مع الدول الثماني الكبرى بوضع استراتيجيات لمجابهة هجمات العصابات الرقمية بذلك تتمحور إستراتيجية التعاون الأمني الدولي في تعزيز آليات مكافحة الجريمة المنظمة والمعلوماتية من خلال أربعة

[1] قاسم محجوبة، مرجع سابق، ص343.

[2] المرجع نفسه، ص344.

[3] المرجع نفسه، ص344.

[4] المرجع نفسه، ص345.

ركائز أساسية، تبدأ بالتأسيس الهيكلي عبر إنشاء مراكز وقنوات اتصال شبكية مؤمنة لضمان سرية وتبادل التدفق المعلوماتي بين الدول الأطراف، وتنتقل إلى الدعم الفني والتقني من خلال تفعيل قواعد البيانات المركزية والتحليل الأوتوماتيكي للأدلة الرقمية[1]، كما ترتكز المنظومة على بناء القدرات البشرية عبر توفير الأدلة الإرشادية والبرامج التدريبية التخصصية في التحقيق الجنائي الرقمي، وصولا إلى التفعيل الإجرائي الميداني المتمثل في نظام النشرات الدولية الملونة لتسريع وتيرة الملاحقة والبحث الجنائي العابر للحدود، بما يضمن إيجاد إطار قانوني وتقني متكامل لتقويض أنشطة الجماعات الإجرامية المنظمة المتمثلة في العصابات الرقمية[2].

الفرع الثاني: جهود المنظمات الإقليمية.

تعد المنظمات الإقليمية من أكثر الفاعلين الدوليين انخراطا في معالجة إشكالات الأمن السيبيراني ومكافحة الأنشطة الإجرامية الرقمية، بالنظر إلى قربها من الدول الأعضاء وقدرتها على إنشاء آليات تعاون قانونية ومؤسساتية أكثر فاعلية، وقد بادرت العديد من المنظمات الإقليمية والدولية ذات الطابع المتخصص إلى تبني برامج واتفاقيات تهدف إلى تعزيز التعاون في مواجهة الإجرام المعلوماتي.

وعليه، سيتم التركيز على ثلاثة نماذج إقليمية رئيسية فاعلة في التصدي للأنشطة التي تقوم بها العصابات الرقمية وهي:

أولا: المنظمات الأوروبية.

يشكل الإطار الأوروبي أحد أبرز النماذج الإقليمية في مجال مكافحة العصابات الرقمية سواء من حيث البناء المؤسسي أو من حيث إرساء القواعد القانونية المنظمة للتعاون الدولي، فقد أنشأ جهاز اليوروبول سنة 2013 المركز الأوروبي لمكافحة الجرائم الالكترونية، ذلك بهدف تعزيز قدرات أجهزة إنفاذ القانون داخل الاتحاد الأوروبي في التصدي للجرائم والأنشطة السيبيرانية لاسيما تلك العابرة للحدود.

كما تم إنشاء هيئة التعاون القضائي الأوروبي المعروفة ب "يوروجست" في فيفري 2002، وتم افتتاحها رسميا في أفريل 2003 بغرض دعم التنسيق القضائي بين الدول الأعضاء في الاتحاد الأوروبي،

[1] محمد السعيد بوفليح، "أطر التعاون الدولي للتصدي للتهديدات السيبرانية "، **مجلة الدراسات القانونية التطبيقية**، م01، ع02، جوان 2024، ص16.

[2] عائشة عبد الحميد، "النظام القانوني للمنظمة الدولية للشرطة الجنائية (الانتربول) ودورها في مجال التعاون القضائي الشرطي"، **المجلة الأكاديمية للأبحاث والنشر العلمي**، م11، ع34، مارس 2020، ص09.

وتيسير التعاون في التحقيقات والملاحقات المتعلقة بالجرائم الخطيرة التي أصبحت أنشطت العصابات الرقمية جزء منهم[1].

وفي السياق ذاته، اعتمد مجلس أوروبا اتفاقية بودابست بشأن الجريمة المعلوماتية سنة 2001، والتي تعد أول معاهدة دولية متخصصة في تجريم الأفعال المرتكبة ضد أنظمة وشبكات الحاسوب أو بواسطة هذه الأنظمة. أما على المستوى الشرطي فقد أنشأت الشرطة الأوروبية على غرار منظمة الأنتربول بوصفها آلية تنسيق بين أجهزة الشرطة في الدول الأوروبية، وذلك من أجل تسهيل ملاحقة مرتكبي الجرائم العابرة للحدود بما في ذلك الجرائم ذات الطابع المعلوماتي والسيبيراني[2].

ثانيا: المنظمات الإفريقية.

سعى الاتحاد الإفريقي إلى وضع إطار قانوني موحد لتعزيز الأمن السيبيراني وحماية البيانات الشخصية داخل القارة الإفريقية، وقد توج هذا التوجه باعتماد اتفاقية الاتحاد الإفريقي بشأن الأمن السيبيراني وحماية البيانات ذات الطابع الشخصي، وذلك خلال القمة الثالثة والعشرين(23) للاتحاد الإفريقي المنعقدة في "مالابو" بغينيا الاستوائية بتاريخ 27 جويلية 2014، وتهدف هذه الاتفاقية أساسا لتعزيز التشريعات الوطنية للدول الأعضاء في مجال تكنولوجيات الإعلام والاتصال، ووضع القواعد الأمنية الضرورية لبناء فضاء رقمي موثوق، بما يضمن سلامة المعاملات الالكترونية ويحمي البيانات الشخصية فضلا عن مكافحة العصابات الرقمية[3].

برزت فكرة إنشاء منظمة التعاون الشرطي الإفريقي "أفريبول" خلال مؤتمر وهران سنة 2013، وذلك باعتبارها آلية إفريقية لتعزيز التعاون الشرطي بين الدول الأعضاء، ولا يقتصر دورها على مكافحة الجريمة التقليدية بل يمتد إلى دعم القدرات التحليلية في تقييم التهديدات الإجرامية، وتطوير الاستجابات الأمنية المناسبة، إضافة لتقديم المساعدة التقنية في مجال مكافحة الجرائم المعلوماتية خاصة في سياق دعم عمليات السلم والأمن داخل القارة.

[1] محمد السعيد بوفليح، مرجع سابق، ص16.

[2] المرجع نفسه ص17.

[3] المرجع نفسه، ص17.

ثالثا: المنظمات العربية.

على المستوى العربي اعتمد مجلس وزراء العدل العرب سنة 1966 القانون الجزائي العربي النموذجي، والذي أفرد نصوصا خاصة لمعالجة الاعتداءات المرتبطة بالمعالجات المعلوماتية، وعالج هذا القانون الاعتداء على حقوق الأشخاص الناتج عن استخدام الوسائل المعلوماتية مع التأكيد على ضرورة حماية الحياة الخاصة والبيانات الشخصية للأفراد، كما أقر عقوبات جزائية تشمل الحبس والغرامة في مواجهة الأفعال التي تمس الخصوصية المعلوماتية، كما أكد الإطار القانوني العربي أهمية التعاون القضائي وتبادل المعلومات بين الدول العربية، وذلك من خلال آليات المساعدة القضائية والإنابة القضائية في مجال مكافحة العصابات الرقمية والجريمة المعلوماتية، وهذا ما يسمح بتجاوز الإشكالات المرتبطة بالطابع العابر للحدود لهذه الجرائم[1].

ومن الناحية المؤسساتية أنشأ مجلس وزراء الداخلية العرب سنة 1965 المكتب العربي للشرطة الجنائية وهذا إلى جانب المكتب العربي لمكافحة الجريمة، بهدف دعم التنسيق الأمني بين الدول العربية وتعزيز الجهود المشتركة في الحفاظ على الأمن الاجتماعي ومكافحة الجريمة بشتى صورها، وتشمل في ذلك الجرائم المستحدثة ذات الصلة بالتقنيات المعلوماتية التي تمارسها العصابات الرقمية[2].

المطلب الرابع: آليات الوقاية والمواجهة المستقبلية للعصابات الرقمية.

يتطلب التصدي لطبيعة الجريمة الرقمية المتطورة خاصة فيما يتعلق بتنظيمات العصابات الرقمية الانتقال بمفهوم الأمن الجنائي من رد الفعل العقابي إلى الوقاية الإستراتيجية الاستباقية، وهو ما تؤسس له هذه الدراسة في إطار محوري يجمع بين أبعاد المواجهة المستقبلية، إذ ينطلق التصدي أولا من وضع التوعية كأداة وقائية مسبقة تهدف إلى تحصين المجتمع معرفيا وسلوكيا قبل انجرافه نحو هذه الممارسات، ثم ينتقل لاستعراض الضوابط والتقنيات الحديثة التي تشكل خط الدفاع التقني الأول ضد التهديدات السيبيرانية، ليختتم بالفصل ببحث السبل العلاجية والتشريعية الضرورية لإزالة العوائق الإجرامية والقضائية، وسندرسهم فيما يلي.

[1] محمد السعيد بوفليح، مرجع سابق، ص18.

[2] المرجع نفسه، ص19.

الفرع الأول: التوعية كآلية قبلية للوقاية.

لم يعد الفضاء الرقمي ساحة للابتكار فحسب تحول إلى ميدان لمواجهة منظمة مع عصابات تقنية تمتلك أدوات متطورة لاختراق الأنظمة والسطو على البيانات، وأمام هذا الواقع المتسارع لم تعد الحلول الأمنية التقليدية كافية، لذا سنتطرف خلال هذا العنصر لأساليب الدفاع الاستباقي والتقنيات الحديثة التي تهدف لتحصين البنية التحتية، وبناء درع تقني يصعب على تلك التنظيمات اختراقه.

أولا: تقنية تشفير المعلومات.

تعمل تقنية تشفير المعلومات على توفير الأمن وسرية البيانات للصفقات التي تتم عبر شبكة الانترنت، كما تشمل دعم وتسهيل إجراءات الإثبات الالكتروني للرسائل الرقمية والأدلة في الأنشطة الإجرامية المنظمة من طرف العصابات الرقمية وذلك عبر عمليات التشفير التي تقوم بها.

يعد التشفير عبر الانترنت مصطلحا يفيد إخفاء المعلومات في أساس بياناتها، بحيث تفرض عليها شيفرة تحجب المعنى الحقيقي لها عن غير المخولين بالإطلاع عليها، وذلك من خلال تحويل البيانات المعالجة الكترونيا لرموز حتى لا يتمكن الغير من انتهاك سريتها[1]، ويتم عبر خوارزمية تسمى "المفتاح" ثم يتم فكها بمفتاح "فك الشيفرة" لضمان السلامة عبر الشبكة الافتراضية.

يصنف التشفير لنوعين رئيسيين فالأول هو تقنية التشفير المتماثل التي تقوم على مبدأ استخدام مفتاح خصوصي واحد، حيث يتولى عملية التشفير وفك التشفير معا فيكون نفس المفتاح عند المرسل والمتلقي، إذ يستلزم عدم إرسال المفتاح مع الرسالة بل يتعين إيصاله بطرق تحفظه وتحميه من الاطلاع عليه من قبل الغير[2]. أما ثاني صنف هو تقنية التشفير غير المتماثل التي توظف مفتاحين مستقلين لكل مستخدم يخصصان التشفير وفكر التشفير، إذ أن المفتاح العام يكون معلن ومتاح للعموم تصدره جهة مشروعة أو هيئة عامة، ويصادق عليه مهنيا لاستخدامه من طرف المستخدم، أما المفتاح الخاص فهو يكون سري لا يكشف عنه ومرتبط بصاحبه ومستقل عن المفتاح العام[3].

تبرز أهمية التشفير بوصفه أداة وقائية فاعلة في مواجهة الجرائم الالكترونية التي تمارسها العصابات الرقمية وذلك من خلال ضمان أمن المعلومات وسريتها، ودعم الإثبات الالكتروني فيكون ركيزة أساسية في

[1] ميرفت محمد حبايبة، مرجع سابق، ص126.

[2] المرجع نفسه، ص128.

[3] المرجع نفسه، ص129.

منظومة الأمن المعلوماتي الشامل، كما يعزز الأمن الالكتروني بتحقيقه لأمن المعلومات المتبادلة والتسديد الالكتروني، وأمن الرسائل الالكترونية وكافة المعاملات التقنية[1].

ثانيا: الجدار الناري.

يعرف الجدار الناري في أدبيات أمن المعلومات بأنه خط الدفاع الأول والركيزة الأساسية في هندسة الشبكات، فهو عبارة عن نظام تقني سواء كان برمجيا أو جهازا ماديا، يعمل كحاجز انتقائي بين الشبكة الداخلية الموثوقة والشبكة الخارجية المتمثلة في الانترنت غير الموثوقة، تكمن وظيفته الجوهرية في ممارسة سلطة التحكم في تدفق البيانات وذلك من خلال السماح أو المنع وفقا لمجموعة من القواعد والسياسات الأمنية المحددة مسبقا، فيضمن هكذا تقليص المخاطر التي تتعرض لها الأنظمة المعلوماتية من طرف العصابات الرقمية[2].

يعمل الجدار الناري وفق مجموعة من التقنيات والخصائص التي تعزز أمن الشبكة، فمن أبرزها نجد فحص حزم البيانات حيت يتم تحليل البيانات التي تعبر الشبكة على مستوى الطبقات التقنية ومقارنتها بقواعد بيانات محددة للتأكد من سلامتها، وأيضا إدارة الوصول والتحكم من خلال منع الوصول غير المصرح به وحجب المواقع الضارة أو غير المرغوب فيها عبر خاصية تصفية الروابط، ونجد أنه يوفر الخصوصية بعمله كخادم وسيط يخفي هوية الشبكة الداخلية ويتحكم في مسار البيانات فيحد من الهجمات المباشرة، كما يدعم البروتوكولات الآمنة لتشفير البيانات العابرة للحدود، ويوفر أدوات لرصد التهديدات وتسجيل ومراقبة الأحداث الأمنية بإصدار تنبيهات عن اكتشاف محاولات اختراق أو نشاط مريب[3].

ثالثا: استخدام كلمة السر.

تعد كلمة السر أبرز الآليات الوقائية المعتمدة في مجال حماية النظم المعلوماتية، إذ تؤدي وظيفة أساسية تتمثل في تقييد الوصول إلى البيانات والأنظمة بحيث لا يتاح استخدامها إلا للمخولين قانونيا وتقنيا، وتكتسب هذه التقنية أهمية خاصة لما تؤديه من دور في إرساء مبدأ السرية ومنع الدخول غير المشروع

[1] ميرفت محمد حبابية، مرجع سابق، ص ص131، 130.

[2] المرجع نفسه، ص133.

[3] المرجع نفسه، ص136.

للمعلومات المحمية. وتشتمل كلمة السر كل من الحروف والأرقام والرموز وتتوسع إلى الوسائل البيومترية كالبصمة والصوت والوجه[1].

تعيين كلمة السر كأداة حماية لابد من توفر ضوابط تقنية تعمل على ضمان فاعليتها بالتحديث الدوري بتغيير كلمة السر بصفة دورية لتلافي انكشافها، كما يجب أن تمتاز الكلمة بالتعقيد والطول فلا يقل طولها عن خمسة أحرف أو رموز كحد أدنى مما يرفع من مستوى صعوبة اختراقها تقنيا، ويمنع إعادة استخدام نفس الكلمة القديمة لضمان عدم استغلالها مجددا، مع ضرورة البعد عن النمطية في التخمين بالاستعانة بأحرف مبعثرة[2].

الفرع الثاني: سبل الوقاية والعلاج للقضاء على الصعوبات.

تعد الجريمة الالكترونية التي تقوم بها العصابات الرقمية من أبرز التحديات القانونية والأمنية التي تواجه المجتمعات المعاصرة نظرا لما تخلف من أثار سلبية غلى الأفراد والمؤسسات والدول، وقد أدى التطور السريع لتقنيات المعلومات والاتصالات لتسارع نطاقها وتنوع أساليب ارتكابها، الأمر الذي يستدعي اعتماد سياسات وقائية وعلاجية متكاملة تجمع بين الجوانب القانونية والتقنية والتربوية والاجتماعية.

أولا: التوعية والتثقيف الرقمي.

تتميز التوعية الرقمية بأنها أهم الوسائل الوقائية للحد من الأنشطة الإجرامية الالكترونية، إذ أن ضعف الوعي التقني لدى المستخدمين يمثل أحد أهم الأسباب التي تستغلها العصابات الرقمية، ومن ثم ينبغي تنظيم برامج تدريبية وورش عمل تهدف لرفع مستوى الثقافة الرقمية لدى الأفراد، وتعريفهم بسبل الاستخدام الآمن لشبكة الانترنت. وتشمل هذه البرامج تدريب الأفراد على إنشاء كلمات مرور قوية وتجنب مشاركة البيانات الشخصية، والحذر من الروابط المشبوهة ورسائل التصيد الاحتيالي الالكتروني، فضلا عن تنمية القدرة على تمييز المواقع الحقيقية والمزيفة، كما ينبغي أن تمتد هذه التوعية لمختلف الفئات العمرية ولاسيما فئة الشباب والأطفال باعتبارهم الأكثر استخداما للوسائل التقنية[3].

[1] ميرفت محمد حبايبة، مرجع سابق، ص138.

[2] المرجع نفسه، ص139.

[3] عبد الحميد بودیار، رشید طبال، " الجریمة السیبرانیة وتأثیرها على الفرد والمجتمع في عصر التكنولوجیا "، **مجلة الباحث في العلوم الإنسانية والاجتماعية**، م16، ع01، جانفي 2025، ص22.

ثانيا: تعزيز الأمن السيبيراني الشخصي.

تحقيق الحماية الفعالة للأفراد في البيئة الرقمية يقتضي اتخاذ تدابير أمنية تقنية متقدمة تقلل من احتمالات الاختراق وسرعة البيانات، لذلك لابد من استخدام برامج الحماية وتحديثها بصورة دورية لمواجهة الفيروسات والبرمجيات الخبيثة وبرامج التجسس. كما تعد المصادقة الثنائية من الوسائل الحديثة التي تعزز حماية الحسابات الالكترونية إذ توفر طبقة إضافية من الأمان من خلال الجمع بين كلمة المرور ووسيلة تحقق أخرى، كرمز التحقق المرسل للهاتف المحمول أو البريد الالكتروني، كما تستدعي الضرورة للنسخ الاحتياطي الدوري للبيانات واستخدام الشبكات الآمنة، وأيضا تعزيز المسؤولية الفردية للمستخدم في التعامل مع البيانات الرقمية فيلتزم بإتباع قواعد الحذر الرقمي وعدم التهاون بحماية بياناته.

ثالثا: تأمين المؤسسات والهيئات العامة والخاصة.

تمثل المؤسسات الحكومية والخاصة هدفا رئيسيا للهجمات السيبيرانية نظرا لما تملكه من قواعد بيانات ومعلومات حساسة، وهذا ما يفرض عليها اعتماد أنظمة حماية متطورة تضمن سلامة المعلومات واستمرارية العمل. لذلك عليها بتحديث الأنظمة والبرمجيات بشكل دوري لسد الثغرات الأمنية واستخدام جدران الحماية، وأنظمة كشف التسلل والتشفير الالكتروني لحماية البيانات المتداولة والمخزنة، كما ينبغي إجراء اختبارات واختراقات تجريبية دورية لتقييم مدى فعالية الأنظمة الأمنية وقدرتها على التصدي للهجمات السيبيرانية.

رابعا: الشراكة بين القطاعين العام والخاص.

تتطلب مواجهة الأنشطة الإجرامية الالكترونية تكاملا مؤسسيا بين الجهات الحكومية والقطاع الخاص باعتبار أن الأمن الرقمي مسؤولية مشتركة تتجاوز الحدود التقليدية للسلطات العامة، لذلك ينبغي تعزيز التعاون في مجال تبادل المعلومات المتعلقة بالتهديدات الالكترونية وتنسيق الجهود لوضع استراتيجيات وطنية فعالة للأمن السيبيراني. فيمكن أن تسهم الشركات التقنية ومزودو خدمات الانترنت في تطوير أنظمة حماية أكثر كفاءة والإبلاغ عن الأنشطة المشبوهة، وتقديم الدعم الفني للجهات المختصة[1].

[1] عبد الحميد بوديار، رشيد طبال، مرجع سابق، ص23.

خامسا: الإطار القانوني والتنظيمي.

يشكل الإطار القانوني حجز الأساس في مكافحة الأنشطة الإجرامية الالكترونية فلا يمكن مواجهة هذا النوع من الجرائم بفعالية دون تشريعات حديثة تتلاءم مع طبيعتها التقنية المتجددة، لذلك يتعين على الدول تطوير قوانينها المتعلقة بالعصابات الرقمية بما يضمن تجريم الأفعال المستحدثة وفرض عقوبات رادعة تتناسب مع خطورتها، كما لابد من أن تتضمن تلك التشريعات أحكاما واضحة لحماية البيانات الشخصية والخصوصية الرقمية، وتنظيم آليات جمع الأدلة الالكترونية وحجيتها أمام القضاء، مع ضرورة تعزيز قدرات الأجهزة الأمنية والقضائية عبر تدريب الكوادر المختصة على تقنيات التحقيق الرقمي والتحليل الالكتروني للبيانات بما يسمح بتتبع العصابات الرقمية وجمع الأدلة الرقمية.

سادسا: الدعم النفسي والاجتماعي للضحايا.

تمتد أثار الأنشطة الإجرامية من الأضرار المادية لتشمل الجوانب النفسية والاجتماعية بحيث قد يتعرض الضحايا لحالات من القلق أو الابتزاز أو فقدان الثقة بالوسائط الرقمية، وهذا ما يستدعي لضرورة إنشاء مراكز متخصصة وخطوط مساعدة لتلقي البلاغات وتقديم الاستشارات القانونية والنفسية، فضلا عن توفير برامج تأهيل تساعد الضحايا على تجاوز الآثار السلبية الناجمة عن تلك الأنشطة، كما ينبغي تشجيع الضحايا على الإبلاغ عن الجرائم الالكترونية دون خوف أو تردد بتوفير الحماية القانونية والسرية اللازمة لهم[1].

سابعا: تعزيز ثقة الأمن الرقمي في المجتمع.

يتطلب لبناء مجتمع رقمي آمن لابد من نشر ثقافة الوعي السيبيراني بين مختلف فئات المجتمع عبر الإعلام والمؤسسات التعليمية ومنظمات المجتمع المدني، وذلك من خلال إطلاق حملات توعوية تهدف لتعريف الأفراد بمخاطر أنشطة العصابات الرقمية في الجرائم الالكترونية وسبل الوقاية منها.

وعليه، فإن مكافحة العصابات الرقمية تستوجب اعتماد مقاربة شاملة تقوم على التكامل بين التوعية والتشريع والتقنية والتعاون المؤسسي والدولي، وذلك بما يضمن حماية الأفراد والمؤسسات من المخاطر الرقمية المتزايدة ويعزز الثقة في البيئة الالكترونية باعتبارها ركيزة أساسية للتنمية المعاصرة[2].

[1] عبد الحميد بوديار، رشيد طبال، مرجع سابق، ص ص24، 23.

[2] المرجع نفسه، ص24.

ملخص الفصل الثاني

يتضح من خلال هذا الفصل أن الإطار القانوني الدولي لمكافحة العصابات الرقمية قد تطور تدريجيا عبر مسار تراكمي، يمتد من اتفاقية بودابست 2001 مرورا بالاتفاقية العربية 2010، وصولا لاتفاقية الأمم المتحدة 2024، وعلى الرغم من تلك الجهود الدولية المبذولة لمكافحة الجرائم الالكترونية التي تكون العصابات الرقمية فاعلة فيها، لا تزال ثمة تحديات هيكلية تتعلق بإشكاليات الاختصاص القضائي وصعوبات الإثبات الرقمي والموازنة بين متطلبات التعاون الدولي ومقتضيات السيادة الوطنية.

ولعل المقاربة الأمثل لتحقيق تلك المساعي تكمن في تبني منهج شامل للأبعاد الثلاثة، بداية بالبعد التشريعي المتمثل في الاتفاقيات الدولية والإقليمية بتطويرها وتوحيدها، والبعد الإجرائي المتجلي في آليات التحقيق بتطوير تقنياته مواكبة لتطور الأساليب الإجرامية والإثبات الرقمي، والبعد المؤسسي المتجسد في هياكل التعاون القضائي والتقني الدولي الفعال كالأنتربول لتنسيق الاستجابة الجماعية للتهديدات السيبيرانية المنظمة، إضافة لاستثمار التقنيات الحديثة كالذكاء الاصطناعي في خدمة العدالة الجنائية الرقمية، وذلك بما يحقق التوازن بين فعالية المحاكمة واحترام الحقوق والحريات الأساسية والسيادة الوطنية لمواجهة إجرام العصابات الرقمية التي تتكيف مع المستجدات التكنولوجية.

الخاتمة

الخاتمة

تمثل العصابات الرقمية تطورا نوعيا في أشكال الجريمة المنظمة، كونها أضحت مرتبطة بالجرائم الالكترونية لتشكل بذلك أخطر التهديدات الأمنية في الفضاء السيبيراني، إذ تعد ظاهرة إجرامية متطورة تنشأ في فضاء الانترنت والأنظمة الرقمية، وتتميز بطابعها العابر للحدود الوطنية وقدرتها على استغلال التقدم التقني والمالي الرقمي لتحقيق مكاسب إجرامية ضخمة، فالعصابات الرقمية لم تعد مجرد تجمع إجرامي تقليدي بل نشأت وتطورت في سياق الانتشار الواسع للاتصالات الرقمية، وتنامي الاقتصاد الرقمي وزيادة الاعتماد على الخدمات المالية الالكترونية.

فخرجت تلك التجمعات بقالب كيانات تنظيمية معقدة أفرزتها الثورة التكنولوجية، وهذا ما وفر أرضية خصبة لتكوين شبكات إجرامية غير تقليدية تتخذ من الفضاء السيبيراني بيئة حاضنة لها، تتسم هذه الكيانات الرقمية بخصائص فريدة كاللامركزية التنظيمية واستخدام تقنية التشفير ، والسرعة في تنفيذ العمليات، والبنى التحتية السحابية، والقدرة الفائقة على التخفي والهوية الزائفة لمرتكبيها، معتمدة في ذلك على أدوات تقنية متطورة كالبرامج الضارة وشبكات الانترنت المظلم، واستعمال البلوك تشين والعملات المشفرة، حيث تعمل العصابات الرقمية وفق هيكل تنظيمي محكم ومتناسق في شكل فرق متخصصة منها المبرمجين ومحللي البيانات والمخططين الماليين، في حين تتجلى دوافعها في تحقيق الربح السريع والتهرب من الملاحقة القضائية، على غرار دوافع أخرى سياسية وأيديولوجية.

تمتد الأنشطة الإجرامية للعصابات الرقمية لتشمل طيفا واسعا من الجرائم التي تتجاوز بكثير الأطر التقليدية للجريمة المنظمة، فتشمل أنماطا مستحدثة تمس بالأموال والأشخاص والأمن الدولي والاقتصادي وحتى على الشبكة المعلوماتية بحد ذاتها، فأثمر تنوع خصائصها والأدوات المستعملة في أنشطتها إلى بروز أنشطة الاحتيال الالكتروني والاحتيال عبر بطاقات الائتمان وسرقة البيانات المصرفية، إضافة والابتزاز للأموال رقميا عبر برامج الفدية التي تستهدف الشركات والهيئات العامة والحكومات. كما تمارس هجماتها على الأشخاص من خلال الاتجار بالبيانات الشخصية وسرقة الهوية والتشهير والملاحقة الالكترونية. وتمتد لتشمل جرائم واقعة على أمن الدولة السيبيراني بالهجمات على البنى التحتية الحيوية واستغلال الفضاء الرقمي في الاتجار بالبشر عبر الانترنت، والاتجار بالمخدرات الالكترونية وهجمات الإرهاب الالكتروني لتجنيد وتمويل الجماعات غير المشروعة، ومن الملاحظ أن هذه الأنشطة تتم بالتعقيد التقني والتوزيع الجغرافي ما يجعل تتبع مرتكبيها ومصادر عائداتها عملية قانونية وتقنية صعبة ومعقدة.

وإدراكا لحجم هذا التهديد المتزايد لمواجهة عصابات الجرائم الرقمية بذلت جهود إقليمية ودولية متزايدة بإرساء ترسانة قانونية تهدف لتوحيد التجريم والعقاب، فعلى المستوى الدولي اتفاقيات مكافحة الجريمة السيبرانية خاصة اتفاقية بودابست 2001 فتعد إطار قانوني مهم يحدد السلوك الإجرامي، ويشجع الدول على تحديث تشريعاتها الجنائية والإجرائية بما يتلاءم مع الطبيعة الرقمية للجريمة، فبرز ذلك بوضوح في المحاكمة الإجرائية ضمن الاتفاقيات الدولية لاسيما في اتفاقية مجلس أوروبا بشأن الجرائم السيبيرانية، وهذا من خلال رسم قواعد إجرائية موحدة تضبط طرق جمع الدليل الرقمي وملاحقة الجناة، وتحديد الاختصاص القضائي وضبط العائدات المالية العابرة للحدود.

ولتفعيل هذه القواعد تم تأسيس آليات التعاون القضائي الدولي كركيزة أساسية لذلك عبر تطبيق إجراءات تسليم المجرمين والمساعدة القانونية المتبادلة، والإنابة القضائية الدولية وتبادل المعلومات الاستخباراتية والأدلة الالكترونية عبر الحدود. إلا أن فعالية هذه القواعد لا تزال محدودة بفعل الفجوات التشريعية والتقنية، واختلاف النظم القانونية والعوائق الدبلوماسية في متطلبات ازدواج التجريم وحماية الخصوصية للأفراد.

على الرغم من تلك الجهود تظل المكافحة تحفوا بتحديات قانونية معقدة يبرز في طليعتها تنازع الاختصاص القضائي بين الدول والتمسك بمبدأ السيادة الوطنية، فتنعكس هذه التحديات على الإجراءات الجنائية والتحقيقية التي تصطدم بصعوبة التفتيش الالكتروني، ومشكلات هوية مرتكبي الجرائم في البيئات المشفرة والمجهولة، كما يطرح الإثبات الرقمي إشكاليات تتعلق بتخزين البيانات في سحب خارج الحدود والولاية القضائية، وتدمير الأدلة أو تعديلها عن بعد أو إتلافها أو تشفيرها، فضلا عن تعقيدات تتبع المسارات المالية المشفرة. تلعب الأجهزة الدولية دورا استراتيجيا في التصدي للعصابات الرقمية مثل الأنتربول واليوروبول ومجلس أوروبا، إضافة لآليات التعاون الأمني بين الأجهزة الاستخباراتية الوطنية، عبر توفير الدعم التقني والاستخباراتي وبناء القدرات، رغم ما يعتري ذلك من قضايا تتعلق بالشفافية والمساءلة.

ومن خلال ما تم ذكره سابقا في خاتمة هذه المذكرة توصلنا مجموعة من الاستنتاجات:

1- أظهرت الدراسة أن العصابات الرقمية ليست نسخة رقمية بسيطة للجريمة المنظمة التقليدية، هي كيانات إجرامية متخصصة تعمل عبر فرق لامركزية لتحقيق ربح مالي سريع والتهرب من الملاحقة القضائية، ما يستدعي تحديث الأطر القانونية الجنائية والتنظيمية لإعطاء تعريف قانوني موحد للعصابات الرقمية.

2- ثبت أن نشاط العصابات الرقمية يتسم بترابط وتكامل عالي بين أنواع الجرائم، مما يجعلها سلاسل إجرامية تتطلب رصدا مستمرا وتحليلا تنبؤيا، لذلك ينبغي على الدول والمنظمات الأممية تبني استراتيجيات أمنية رقمية متكاملة تشمل أنظمة إنذار مبكر، وتحليل البيانات الضخمة واستعمال الذكاء الاصطناعي لتتبع الأنماط الإجرامية.

3- بينت الدراسة أن الاتفاقيات الدولية مثل اتفاقية بودابست2001 واتفاقية الأمم المتحدة 2024 توفر إطار قانوني فعال، إلا أن التطبيق العملي يواجه فجوات كبيرة وهذا ما يستدعي تعزيز التعاون القضائي الدولي الفوري والمرن بتبسيط إجراءات طلبات المساعدة، وتوحيد الحد الأدنى من معايير قبول الأدلة الرقمية بما يحمي الخصوصية.

4- كشفت الدراسة أن أبرز التحديات تتمثل في صعوبة تحديد الاختصاص القضائي في الجرائم العابرة للحدود، ومشكلات الهوية للجناة، وقيود تقنية وإجرائية في التفتيش الرقمي والمصادرة الالكترونية، بذلك لابد على الدول والمنظمات الدولية من تبني استراتيجية شاملة ومستدامة بتحديث التشريعات الوطنية لمواكبة التطور التقني والتكنولوجيا المتنامية.

قائمة المصادر والمراجع

قائمة المصادر والمراجع.

المصادر.

1- النصوص القانونية.

أ- النصوص التشريعية.

1. اتفاقية المجلس الأوروبي المتعلقة بمواجهة الجرائم الالكترونية 2001، الموقعة في بودابست، بتاريخ 23 نوفمبر 2001، دخلت حيز التنفيذ 01 جويلية 2004.

2- المعاجم والقواميس.

1. معجم لسان العرب، ابن منظور، دار صبح و إديسوفت، بيروت، لبنان، 2006.

المراجع.

1- الكتب.

1. أبو قاسم طاهر محمود، الجرائم المعلوماتية صعوبات وسائل التحقيق فيها وكيفية مواجهتها، مصر: المنظمة العربية للتنمية الإدارية جامعة الدول العربية، ط 01، 2019.
2. جندل جاسم محمد، الجرائم الالكترونية، الأردن: دار المعتز للنشر والتوزيع، ط01، 2022.
3. حسن مظفر الرزو، الفضاء المعلوماتي، لبنان: مركز الدراسات الوحدة العربية، د.ط، 2007.
4. ذيب محمود عبد الله، دراج أسامة إسماعيل، الوجيز في الجرائم الالكترونية القواعد الموضوعية والإجرائية، الأردن: دار الثقافة للنشر والتوزيع، ط01، 2022.
5. طويله جميل حسين، البرمجيات الخبيثة، د.ط، سوريا، 2015، في: https://www.scribd.com/document/551801151/ .
6. علي عبد الحميد، مكافحة الجرائم الالكترونية: بين نظم المعلومات والإعلام البديل، الإسكندرية: مكتبة الوفاء القانونية، ط02، 2024.
7. قطينة فهد، الأمن السيبيراني تعلم الأمن السيبيراني من الصفر حتى الاحتراف، أكاديمية الأمن السيبيراني، ط01، 2025، https://www.ktobati.com/book/ .
8. محمد حبايبة ميرفت، مكافحة الجريمة الالكترونية: دراسة مقارنة في التشريع الجزائري والفلسطيني، الأردن: دار اليازوري العلمية للنشر والتوزيع، ط01، 2023.

2- المذكرات.

أ- مذكرات الماستر.

1. أمحمد إسماعيل، زوبير عبد الجليم، دور التكنولوجيا الحديثة في ارتكاب الجرائم الالكترونية وسبل مكافحتها، مذكرة لنيل شهادة الماستر في القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة غرداية، 2025.

2. بن أوذينة سندس، الجهود الدولية في مواجهة الجرائم السيبرانية، مذكرة ماستر في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة غرداية، 2025.

3. حمبلي عمار، عثماني دليلة، جرائم تقنية المعلومات في ظل الاتفاقية العربية 2010 وفي التشريع الجزائري، مذكرة ماستر في القانون الجنائي والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2022.

3- المقالات.

1. Encyclopédie Universalisé.

2. الأخنش نورة أمينة، العيداني محمد، " الذكاء الاصطناعي لمجابهة الجريمة الالكترونية Artificial intelligence as a mechanism to confront cybercrime "، مجلة القانون والعلوم البينية، م 02، ع 02، سبتمبر 2023.

3. أرزقي نسيب محمد، " المافيا أداة للجريمة المنظمة"، مجلة كلية_أصول الدين_الصراط، ع03، سبتمبر 2000.

4. بخدة صفيان، وقاص ناصر، " الطبيعة القانونية لجرائم المستحدثة ووسائل ارتكابها جريمة الانترنت كنموذج "، مجلة البحوث القانونية والسياسية، م03، ع16، أفريل2021.

5. البركة الطيبي، "إشكالية الإثبات في الجرائم الالكترونية The issus of proof in cybercri "، مجلة أفاق علمية، م 11، ع 01، أكتوبر 2018.

6. بن شريف أحلام، بوغرارة الصالح، "القرصنة الالكترونية: أنواعها أشكالها وطرق التصدي لها"، المجلة الجزائرية للعلوم السياسية والعلاقات الدولية، م05، ع01، جوان 2012.

7. بوديار عبد الحميد، طبال رشيد، " الجريمة السيبرانية وتأثيرها على الفرد والمجتمع في عصر التكنولوجيا "، مجلة الباحث في العلوم الإنسانية والاجتماعية، م 16، ع 01، جانفي 2025.

8. بوفليح محمد السعيد، "أطر التعاون الدولي للتصدي للتهديدات السيبرانية "، مجلة الدراسات القانونية التطبيقية، م 01، ع 02، جوان 2024.

9. حطابي صادق، " الجريمة الرقمية: تحليل معاصر لتطور الجرائم الالكترونية وتأثيراتها الاجتماعية"، مجلة الحكمة للدراسات الفلسفية، م14، ع01، جانفي2026.

10. خليفي محمد، " إشكالية الاختصاص القضائي الدولي في مكافحة الجريمة المعلوماتية "، مجلة الميزان، د م، ع 01، ديسمبر 2016.

11. دهشان يحي إبراهيم، " قواعد المسؤولية الجنائية عن تطبيقات الذكاء الاصطناعي"، مجلة الشريعة والقانون، الإمارات العربية المتحدة، م 34، ع 82، أفريل 2020.

12. رابحي أحسن، "الجريمة الالكترونية: النقطة "المظلمة" بالنسبة للتكنولوجية المعلوماتية"، المجلة الجزائرية للعلوم القانونية والسياسية، م48، ع01، مارس2011.

13. زواوي لمياء، رملي فهيم، "التهديدات السيبيرانية وأمن المجتمع الرقمي: دراسة حالة الجزائر"، المجلة الجزائرية للأمن والتنمية، م12، ع02، أفريل2023.

14. زيوش سعيد، "ظاهر الابتزاز الالكتروني وأساليب الوقاية منها– قراءة سوسيولوجية وأراء نظرية– "، مجلة العلوم الاجتماعية، د.م، ع22، جانفي2017.

15. طابي نوارة، بوجادي صليحة، "الإنابة القضائية كآلية للتعاون الدولي من أجل استرداد عائدات الفساد"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، م 10، ع 01، جوان 2025.

16. طالة لامية، " المخدرات الرقمية...جريمة الإدمان الجديد في الفضاء السيبيراني قراءة في التأثيرات وأساليب المواجهة "، مجلة للدراسات الإعلامية، م06، عد01، مارس2022.

17. عبد الحميد عائشة، "النظام القانوني للمنظمة الدولية للشرطة الجنائية (الأنتربول) ودورها في مجال التعاون القضائي الشرطي"، المجلة الأكاديمية للأبحاث والنشر العلمي، م11، ع 34، مارس 2020.

18. قطاف سليمان، بوقرين عبدالحليم، "الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري"، المجلة الأكاديمية للبحوث القانونية والسياسية، م 06، ع 01، مارس2022.

19. الكثيري سعيد مسعود، "الجريمة الالكترونية في ضوء اتفاقية بودابست: الإطار المفاهيمي والتصنيفي"، مجلة البحوث القانونية والاقتصادية سلطنة عمان، م 09، ع 01، ديسمبر 2025.

20. كردي نبيلة، "الاتجار بالبشر عبر الانترنت "، مجلة أبحاث، م08، ع02، جوان2022.

21. محجوبة قاسم، " الأنتربول آلية دولية لمكافحة الجريمة المنظمة العابرة للحدود"، مجلة البحوث في الحقوق والعلوم السياسية، م 09، ع 01، جويلية 2023.

22. محمود خالد وليد، "الهجمات عبر الانترنت: ساحة الصراع الالكتروني الجديدة"، المركز العربي للأبحاث ودراسة السياسات، الدوحة قطر، سبتمبر 2013.

23. مرين يوسف، "إرهاب الانترنت عندما تتحول التقنية إلى وسيلة للإجرام"، مجلة الدراسات القانونية والسياسية، جامعة عبد الحميد بن باديس مستغانم، م 04، ع02، جوان2018.

4- المواقع الالكترونية.

1. MOSCA GAETANO " موسكا غايتانو 1858-1941": بعد دراسة القانون والعلوم السياسية، درس غايتانو موسكا هذين التخصصين في جامعة تورينو، ثم في روما، والى جانب عمله الأكاديمي، انخرط في العمل السياسي وانتخب لعضوية مجلس النواب ثم لمجلس الشيوخ، في كتابه الأول ركز على دراسة تكوين وتنظيم الطبقية الحاكمة المعروفة في ايطاليا بالطبقة السياسية (Sulla teorica dei governmenti e sul governento parlamentare ;1884)، https://www.universalis.fr/encyclopedie/gaetano-mosca/.

2. SEARHINFORM, Decoding The Anatomy of Organized Cybercrime , available froum : https://searchinform.com/articles/cybersecurity/cyber-threats/cybercrime/organized-cybercrime .

3. أبرز بنود اتفاقية الأمم المتحدة لمنع الجريمة السيبرانية، 2025/10/26، https://www.aljazeera.net/encyclopedia/.

4. أبوراوي يوسف، القرصنة الأخلاقية: جريمة أم فضيلة ؟، 2024/01/27، https://blogs.lamah.com/.

5. الزاملي ماجد أحمد، الإستراتيجية الوطنية للتعاون الدولي في مجال مكافحة الجريمة، 2021/08/03، https://www.ahewar.org/debat/show.art.asp?aid=727111.

الصافي إبراهيم، أنظمة الإنذار المبكر ودورها في التصدي للإرهاب، 2023/01/08، https://trendsresearch.org/ar/insight/.