مجلة جامعة دمشق للعلوم القانونية

اسم المقال: السياسة الجنائية الإجرائية المتبعة في إحداث محاكم متخصصة بجرائم المعلوماتية والاتصالات
اسم الكاتب: د. عيسى المخول
رابط ثابت: https://political-encyclopedia.org/index.php/library/1874
تاريخ الاسترداد: 2026/11/02 02:07 +03

الموسوعة السياسيّة هي مبادرة أكاديمية غير هادفة للربح، تساعد الباحثين والطلاب على الوصول واستخدام وبناء مجموعات أوسع من المحتوى العلمي العربي في مجال علم السياسة واستخدامها في الأرشيف الرقمي الموثوق به لإغناء المحتوى العربي على الإنترنت.
لمزيد من المعلومات حول الموسوعة السياسيّة - Encyclopedia Political، يرجى التواصل على info@political-encyclopedia.org

استخدامكم لأرشيف مكتبة الموسوعة السياسيّة - Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام المتاحة على الموقع https://political-encyclopedia.org/terms-of-use

تم الحصول على هذا المقال من موقع مجلة جامعة دمشق للعلوم القانونية ورفده في مكتبة الموسوعة السياسيّة مستوفياً شروط حقوق الملكية الفكريّة ومتطلبات رخصة المشاع الإبداعي التي ينضوي المقال تحتها.

السياسة الجنائية الإجرائية المتبعة في إحداث محاكم متخصصة بجرائم المعلوماتية والاتصالات

د. عيسى المخول*

الملخص

يتلخص هذا البحث في بيان القواعد القانونية الجزائية الإجرائية التي استند إليها المشرع السوري في تنظيم المحاكم المختصة بالجرائم الإلكترونية وجرائم الاتصالات، حيث ازدادت أهمية هذه القواعد في ظل الحرب التي تمر بها الجمهورية العربية السورية حيث كثر ارتكاب الجرائم الالكترونية من خلال الشبكة العنكبوتية، مما دعا المشرع إلى سن قانون خاص بهذه الجرائم من خلال سياسة تجريمية وعقابية تتلاءم مع طبيعة هذه الجرائم. ولم يكتفِ بذلك، بل أنشأ محاكم مختصة بمحاكمة مرتكبي هذه الجرائم، ولذلك فإن دراسة السياسة الإجرائية لمكافحة هذه الجرائم لا تقل أهمية عن دراسة السياستين التجريمية والعقابية، وإن ذلك يتم من خلال دراسة القانون رقم 9 لعام 2018 الخاص بتشكيل محاكم متخصصة للجرائم المعلوماتية وجرائم الاتصالات.

* أستاذ مساعد في قسم القانون الجزائي – كلية الحقوق– جامعة دمشق

La politique pénale procédurale en création des tribanuax spécifique pours les cyber infractions

Dr. Issa ALmakhoul*

Résumé

Cette recherche consiste dans l′explication de règles pénales procédurales auxquelles le législateur syrien organize des tribunaux compétents aux infractions électroniqes et aux infractions de communication dans la mesure où l′importance de ces tribunaux augmente dans la crise syirienne. L′ influence d′ internet dans cette crise apparaît de manière que les infractions électronique et les infractions de communications font une grande augmentation . Pour cela, cette étude sur la création des tribanuax spécifiqus pours les cyber infractions par la loi 9 /2018 est très important car l′examen de la politique procédurale n′ est pas moins importance de la poiltique punitive.

* Faculté de Droit université de Damas

المقدمة

أفرز عصر تقنية المعلومات ما يعرف بالجرائم المعلوماتية على اختلاف أنواعها[1]، وقد صدرت عدة تشريعات تهدف إلى مكافحة جرائم المعلوماتية وجرائم الاتصالات، وعلى رأسها القانون الأم، وهو قانون تنظيم التواصل من خلال الشبكة ومكافحة الجريمة المعلوماتية لعام 2012 ، وقانون الإعلام لعام 2011 الذي تضمن العقوبات على الجرائم المرتكبة من خلال الصحافة الالكترونية، وقانون التوقيع الالكتروني لعام 2009 وعدد من التشريعات الأخرى التي تضمنت نصوصاً عقابية تطال الجرائم المعلوماتية. إضافة إلى ذلك، تضمّن قانون الاتصالات لعام 2010 آليات تنظيم قطاع الاتصالات والجرائم التي تستهدف هذا القطاع.

وأمام الانتشار الواسع للجرائم المعلوماتية، راحت تعرض على قضائنا يومياً عدد من هذه القضايا التي تتراوح عقوباتها بين الجناية والجنحة، وأسوة بعدد من دول العالم، كان لابد من إحداث القضاء المتخصص المؤهل والمدرب للفصل في قضايا جرائم المعلوماتية وجرائم الاتصالات. فالدراسة الأكاديمية القانونية لم تعد كافية للقاضي لتمكنه من الفصل في هذا النوع من القضايا التي يحتاج النظر فيها إلى دراية تقنية تمكنه من فهم آليات استقصاء جرائم المعلوماتية وكيفية تفتيش الحواسيب والمخدمات، واستعادة المعلومات والبيانات المحذوفة ، وماهية الدليل الرقمي وشروط حجيته في الإثبات ، الأمر الذي يجب معه تأهيل السادة القضاة وتدريبهم لاكتساب المعرفة والمهارة اللازمة للتعامل مع هذه القضايا .وتحقيقاً لهذه الرؤية فقد عمدت وزارة العدل بالتعاون مع وزارتي الاتصالات والتقانة والداخلية إلى تدريب المجموعة الأولى من السادة القضاة من مختلف الدرجات القضائية على مكافحة

[1] د. عمر عيسى الفقمي ، الجرائم المعلوماتية ، دار النهضة العربية ، القاهرة ، 2005 ، ص 30، د. محمد علي العريان ، الجرائم المعلوماتية ، دار النهضة العربية ، القاهرة ، 2000، ص 43 ، د. محمد عبدالله سلامة ، جرائم الكمبيوتر والإنترنت ، منشأة المعارف ، الاسكندرية ، 2006 ، ص 51 ، د. خالد ابراهيم ، الجرائم الإلكترونية ، دار الفكر الجامعي، القاهرة ، 2009 ، ص 23.

الجريمة المعلوماتية وحجية الدليل الرقمي، وذلك تمهيداً لإحداث هذا القضاء المتخصص الذي يحتاج إلى تدريب مستمر يتماشى مع التسارع اليومي للتطور التقني.

أهمية البحث:

تظهر أهمية هذا البحث في بيان القواعد القانونية الجزائية الإجرائية التي استند إليها المشرع السوري في تنظيم المحاكم المختصة بالجرائم الإلكترونية وجرائم الاتصالات. حيث تزداد هذه الأهمية في ظل الحرب التي تمر بها الجمهورية العربية السورية مما أدى إلى تأثير الإنترنت تأثيراً مباشراً في هذه الحرب من خلال ما يرتكب من خلال الشبكة العنكبوتية من جرائم إلكترونية، مما دعا المشرع إلى سنّ قانون خاص بهذه الجرائم من خلال سياسة تجريمية وعقابية تتلاءم مع طبيعة هذه الجرائم ، ولذلك فإن دراسة السياسة الإجرائية لمكافحة هذه الجرائم لا تقل أهمية عن دراسة السياستين التجريمية والعقابية.

منهج البحث:

اعتمدنا في كتابة هذا البحث الأسلوب التحليلي لنصوص القوانين المتعلقة بالموضوع حيث نقوم بتحليل هذه النصوص القانونية التي أوردها المشرع في صلب قانون مكافحة الجرائم المعلوماتية رقم 17 لعام 2012 وفي قانون إحداث المحاكم الخاصة بالجرائم المعلوماتية رقم 9 لعام 2018.

إشكالية البحث:

تتمحور إشكالية هذا البحث حول إيضاح السياسة الإجرائية للمشرع السوري في إحداثه للمحاكم المختصة بالجرائم المعلوماتية وجرائم الاتصالات من خلال سنه للقانون رقم 9 لعام 2018، ومدى تطور هذه السياسة وتماشيها مع خصوصية الجرائم المعلوماتية لنصل من حيث النتيجة إلى تقدير مدى تحقيق هذا القانون للعدالة الجزائية في إطار ملاحقة مرتكبي الجرائم المعلوماتية وجرائم الاتصالات. وانطلاقاً من هذه الإشكالية سنقسم البحث وفقاً للخطة الآتية.

خطة البحث:

المبحث الأول: ملاءمة القواعد العامة للاختصاص القضائي لخصوصية الجرائم المعلوماتية

المطلب الأول: خصوصية قواعد الاختصاص المكاني

المطلب الثاني: خصوصية قواعد الاختصاص النوعي

المبحث الثاني: ملاءمة صلاحيات النيابة وقضاة التحقيق لخصوصية جرائم المعلوماتية

المطلب الأول: تقلص صلاحيات النيابة العامة

المطلب الثاني: تفريد صلاحيات قاضي التحقيق

المبحث الأول

ملاءمة القواعد العامة للاختصاص القضائي لخصوصية الجرائم المعلوماتية

وضع قانون أصول المحاكمات الجزائية باباً خاصاً للاختصاص هو الباب الأول من الكتاب الثاني من هذا القانون من المادة 163 إلى 183 .

ويعرّف الاختصاص بأنه السلطة التي خولها القانون للمحكمة للبت في الدعوى، أي سلطة المحكمة الجزائية في نظر قضية جزائية معينة والفصل فيها [2]. وقد نصت الفقرة أ من المادة الأولى من القانون رقم 9 لعام 2018 على أنه: " تُحدث في كل محافظة من محافظات الجمهورية العربية السورية نيابة عامة ودوائر تحقيق تختص كل منها بالنظر في جرائم المعلوماتية وجرائم الاتصالات تُملأ وظائفها من الملاك العددي للوظائف القضائية".

وبناءً على ذلك سندرس في هذا المبحث خصوصية قواعد الاختصاص القضائي المكاني والنوعي في القانون رقم 9 لعام 2018. لذلك لابد لنا من تقسيم هذا المبحث إلى مطلبين ندرس في المطلب الأول خصوصية قواعد الاختصاص المكاني، ونخصص المطلب الثاني لدراسة خصوصية قواعد الاختصاص النوعي.

[2] د.بارعة القدسي ، أصول المحاكمات الجزائية ، الجزء الأول . مطبوعات جامعة دمشق ، 2013 ، ص 59

المطلب الأول: خصوصية قواعد الاختصاص المكاني:

نص القانون رقم 9 لعام 2018 على إحداث نيابة عامة ودوائر تحقيق مختصة في النظر في جرائم المعلوماتية وجرائم الاتصالات في كل محافظة. إن ذلك يدل على أن المشرع السوري أراد تكريس قواعد الاختصاص المكاني بالنسبة إلى الإجراءات الواجب اتباعها في مكافحة هذه الجرائم.

ولفهم كيفية تطبيق هذه القواعد على الجرائم المعلوماتية وجرائم الاتصالات، لابد من العودة إلى قواعد الاختصاص المكاني المنصوص عليها في قانون أصول المحاكمات الجزائية فقد نص هذا القانون في الفقرة الأولى من المادة 3على أن الدعوى العامة تقام أمام المحكمة التي يتبع لها موطن المدعى عليه أو موطن وقوع الجريمة أو مكان إلقاء القبض على الفاعل [3].

وإن كنا لا نجد إشكالية في تحديد موطن المدعى عليه أو مكان إلقاء القبض على الفاعل في جرائم المعلوماتية وجرائم الاتصالات، إلا أن المشكلة تظهر في تحديد مكان وقوع الجريمة بالنسبة إلى هذه الجرائم لكونه مرتبطاً بالركن المادي لها. ولذلك لابد من دراسة هذا المطلب من خلال التحليل القانوني لأحد الاحتمالين الآتيين: أولاً: تحقيق عناصر الركن المادي في الإقليم السوري، وثانياً : تحقيق أحد عناصر الركن المادي خارج الإقليم السوري.

أولاً: تحقيق عناصر الركن المادي في الإقليم السوري:

تتميز جرائم المعلوماتية وجرائم الاتصالات في أن الأفعال التنفيذية للجريمة قد تقع في مكان، في حين أن النتيجة الجرمية تحدث في مكان آخر، على عكس كثير من الجرائم التقليدية التي تحدث عناصر الركن المادي كلها في مكان واحد.

[3] د.بارعة القدسي ، أصول المحاكمات الجزائية ، الجزء الأول . مطبوعات جامعة دمشق ، 2013 ، ص 64

ومن الممكن أن نطرح مثالاً على ذلك جريمة البريد الواغل حيث يُرسل البريد الإلكتروني من مكان في حين أن النتيجة الجرمية المتمثلة باستقبال البريد الإلكتروني تقع في مكان آخر، أو جريمة الدخول غير المشروع لمنظومة معلوماتية وإتلاف ما فيها، حيث يدخل من جهاز حاسوبي في مكان ويحدث الإتلاف في جهاز حاسوبي في مكان آخر، وكذلك الأمر في جريمة الاحتيال الإلكتروني حيث يقوم أحد الأشخاص باستعمال الإنترنت وهو في منزله لاختراق المنظومة المعلوماتية لأحد المصارف ثم يُحول أرصدة بعض الحسابات إلى حسابه المصرفي.

وبذلك يكون لهذه النوع من الجرائم أكثر من مكان تقع فيه الجريمة، ويكون للنيابة العامة ولقضاة التحقيق في كل هذه الأمكنة الاختصاص المكاني لتحريك الدعوى العامة، والبدء في التحقيق الابتدائي للتوصل إلى فاعل الجريمة.

ثانياً: تحقيق أحد عناصر الركن المادي خارج الإقليم السوري:

الجريمة المعلوماتية جريمة عابرة للحدود، ومن ثَمَّ فإن عناصر الركن المادي للجريمة قد تتوزع على أكثر من دولة. ولمعالجة هذه الإشكالية، لابد من العودة إلى نصوص قانون العقوبات، وقانون مكافحة الجريمة المعلوماتية.

أ . المعالجة وفقاً لنصوص قانون العقوبات:

وجد المشرع السوري وفقاً لنصوص قانون العقوبات أن الجريمة المعلوماتية أو جريمة الاتصالات تعد مقترفة في الأرض السورية في الحالات الآتية[4] :

❖ إذا تم على الأرض السورية أحد العناصر التي تؤلف الجريمة المعلوماتية أو جريمة الاتصالات: ومثال ذلك أن يقوم شخص موجود في سورية بإنشاء موقع للاحتيال عبر الإنترنت، ثم وقع ضحية هذا الموقع شخص مقيم في لبنان.

[4] د. عبود السراج ، شرح قانون العقوبات العام ، منشورات جامعة دمشق ، 2014 ، ص 177

❖ إذا تم على الأرض السورية فعل من أفعال جريمة غير متجزئة. ويدخل في مفهوم الجريمة غير المتجزئة الجريمة المستمرة، والجريمة المتتابعة، وجريمة العادة، ومثال ذلك أن يقوم شخص في سورية بالاحتيال إلكترونياً عدة مرات على الشخص ذاته الموجود في لبنان.

❖ إذا وقع على الأرض السورية فعل اشتراك أصلي أو فرعي. ومثال ذلك لو قام شخص موجود في سورية بتقديم معلومات إلى شخص آخر موجود في الأردن ليتمكن من اختراق المنظومة المعلوماتية العائدة لأحد المصارف الأمريكية من خلال الإنترنت.

❖ إذا حصلت النتيجة الجرمية على الأرض السورية أو كان متوقعاً حصولها فيها. ومثال ذلك إذا قام شخص موجود في فرنسا بإنشاء موقع للاحتيال على الإنترنت لتداول الأسهم الوهمية فوقع ضحية هذا الموقع شخص موجود في سورية، فتكون النتيجة الجرمية وقعت في سورية. وتكون النتيجة متوقعاً حصولها في سورية، كما لو قام شخص موجود في الإمارات بتصميم إحدى البرمجيات الخبيثة لترويجها في المنظومات المعلوماتية للمصارف السورية إلا أنه لم يتمكن من نشرها لظروف خارجة عن إرادته.

ب . المعالجة وفقاً لنصوص قانون مكافحة الجريمة المعلوماتية:

لابد من الإشارة إلى أن المشرع السوري عدّ في الفقرة ب من المادة 33 من قانون مكافحة الجريمة المعلوماتية رقم 17 لعام 2012 أن النطاق العلوي السوري في حكم الأرض السورية في معرض تطبيق هذا القانون.

وقد حددت المادة الأولى من قانون مكافحة الجريمة المعلوماتية اسم النطاق العلوي الوطني للجمهورية العربية السورية بكلمة " سورية " و " .Sy " أو أي نطاق إضافي يعتمد لاحقاً.

في الواقع إن حسبان تلك المساحة من الإنترنت خاضعة لإرادة الدولة السورية وفقاً للاختصاص المكاني يعود إلى سببين. فمن جهة أولى، إن المبررات المتعلقة بسيادة الدولة

على إقليمها والتي دفعت المشرع الجزائي إلى عَدِّ الطائرة أو السفينة بحكم الأرض السورية متوافرة في ذلك النطاق العلوي السوري على الإنترنت المنتهي بتعبير " .Sy ". ولذلك فإن عَدُّه بحكم الأرض السورية يتفق مع فلسفة المشرع السوري. ومن جهة ثانية، هناك مبررات عملية تدفع إلى عَدِّ النطاق العلوي السوري على الانترنت خاضعاً للاختصاص المكاني السوري، وهي أن هناك جرائم من الممكن أن ترتكب من خلال هذا النطاق السوري دون أن تطالها قواعد الاختصاص الجزائي ومثال ذلك : إذا أنشأت شركة إيطالية موقعاً الكترونياً لها على النطاق السوري ثم احتالت من خلال هذا الموقع على بعض الفرنسيين الموجودين في فرنسا، فإن هذه الجريمة لا تخضع في حال عدم اعتبار النطاق العلوي السوري بحكم الأرض السورية لأحكام القانون السوري على الرغم من أنها تمت من خلال النطاق السوري على الإنترنت .

المطلب الثاني: خصوصية قواعد الاختصاص النوعي:

حددت الفقرة أ من المادة الأولى من القانون رقم 9 لعام 2018 الاختصاص النوعي للنيابة العامة ولدوائر التحقيق المحدثة في الجرائم المعلوماتية وجرائم الاتصالات. ولتحديد هذه الجرائم، لابد من العودة إلى تعداد الجرائم المعلوماتية المحددة في القانون رقم 17 لعام 2012 وقانون الاتصالات رقم 18 لعام 2010. لذلك لابد لنا من دراسة هذا المطلب من خلال أولاً: بيان الجرائم المعلوماتية، ثانياً: بيان جرائم الاتصالات، ثالثًا: فقدان محاكم الصلح من الهيكل التنظيمي للمحاكم المختصة بالجرائم المعلوماتية والاتصالات، رابعاً: عدم اختصاص المحاكم المتخصصة بالجرائم المعلوماتية بالجرائم المتلازمة بالجرائم المعلوماتية، خامساً: إحالة الدعاوى المنظورة إلى المحاكم المختصة بجرائم المعلوماتية وجرائم الاتصالات.

أولاً: الجرائم المعلوماتية:

عرّف المشرع السوري في المادة الأولى من القانون رقم 17 لعام 2012 لمكافحة الجريمة المعلوماتية هذه الجريمة بأنها: " كل جريمة ترتكب باستعمال الأجهزة الحاسوبية أو الشبكة أو تقع على المنظومات المعلوماتية أو الشبكة ".

وقد عدد المشرع السوري في الفصل الثالث من القانون ذاته النماذج القانونية لمختلف صور الجريمة المعلوماتية وهي: جريمة الدخول غير المشروع إلى منظومة معلوماتية، جريمة شغل اسم موقع الكتروني ، جريمة إعاقة الوصول إلى الخدمة ، جريمة اعتراض المعلومات ، جريمة تصميم البرمجيات الخبيثة واستعمالها ، جريمة إرسال البريد الواغل، جريمة الاحتيال عن طريق الشبكة ، جريمة الاستعمال غير المشرع لبطاقات الدفع ، وجريمة انتهاك حرمة الحياة الخاصة .

وانطلاقاً من ذلك فإن الاختصاص النوعي للنيابة العامة ولقضاة التحقيق وفقاً للقانون رقم 9 لعام 2018 الخاص بتشكيل محاكم متخصصة للجرائم المعلوماتية وجرائم الاتصالات ينحصر فقط في هذه النماذج التسعة المحددة في الفصل الثالث من قانون مكافحة الجريمة المعلوماتية وذلك للأسباب الآتية:

أ . احترام مبدأ الشرعية:

كرس الدستور والقانون مبدأ الشرعية الجزائية، حيث نص قانون العقوبات بصورة صريحة على أنه لا جريمة من دون نص قانوني. وتبعاً لذلك فقد وضع المشرع السوري عنواناً واضحاً في الفصل الثالث من القانون رقم 17 لعام 2012 وهو " مكافحة الجريمة المعلوماتية " معدداً الجرائم المعلوماتية على سبيل الحصر، ومن ثَمَّ لا يجوز عَدُّ غيرها من الجرائم المعلوماتية ولو ارتكبت باستعمال المنظومة المعلوماتية أو الشبكة. وإن تعريف الجريمة المعلوماتية في المادة الأولى إنما هو لإسقاطه على هذه الجرائم بصورة حصرية .

ب . عدُّ الوسيلة الإلكترونية ظرفاً مشدداً:

إذا كان تعريف الجريمة المعلوماتية المحدد في المادة الأولى من قانون مكافحة الجريمة المعلوماتية رقم 17 لعام 2012 يكفي لعدِّ أي جريمة تقليدية ترتكب بوسيلة إلكترونية هي جريمة معلوماتية فهذا يعني أن وسيلة ارتكاب الجريمة أصبحت تدخل ضمن أركان الجريمة لأنه بانعدامها تنتفي الجريمة، بينما الحقيقة هي على خلاف ذلك لأن المشرع السوري عدّ الوسيلة الالكترونية ظرفاً مشدداً للعقاب فقط لأي جريمة تقليدية ومن ثمَّ لم يعدّ الجريمة التقليدية جريمة معلوماتية لمجرد ارتكابها بوسيلة الكترونية، ومثال ذلك لو افترضنا أن شخصاً قام بارتكاب جرم ذم عن طريق الإنترنت فهذه جريمة تقليدية ارتكبت بوسيلة إلكترونية، وفي هذه الحالة تشدد العقوبة .

وتبعاً لذلك فإن الاختصاص النوعي للنيابة العامة في تحريك الدعوى العامة ولقضاة التحقيق في البدء بالتحقيق الابتدائي يرتبط فقط بالنماذج التسعة المنصوص عليها في القانون رقم 9 لعام 2018، ولا يشمل هذا الاختصاص النوعي الجرائم التقليدية المرتكبة بوسائل الكترونية المنصوص عليها في قانون العقوبات أو التشريعات الجزائية الخاصة.

ثانياً: جرائم الاتصالات:

عدد المشرع السوري في قانون الاتصالات رقم 18 لعام 2010 جرائم الاتصالات في الباب الرابع عشر، وهي: إنشاء شبكات الاتصالات أو تقديم خدمات الاتصالات من دون ترخيص، تخريب شبكات أو تجهيزات الاتصالات، إساءة استعمال الترددات الراديوية، إساءة تقديم خدمات الاتصالات، استعمال الوسائل الاحتيالية، استيراد وتصنيع وحيازة تجهيزات غير مرخصة.

تبعاً لذلك فإن هذه الجرائم هي التي تدخل في الاختصاص النوعي للنيابة العامة وقضاة التحقيق المحدثين بموجب القانون رقم 9 لعام 2018 الخاص بتشكيل محاكم متخصصة للجرائم المعلوماتية وجرائم الاتصالات.

ثالثاً: فقدان محاكم الصلح من الهيكل التنظيمي للمحاكم المختصة بالجرائم المعلوماتية والاتصالات:

نصت المادة الثانية من القانون رقم 9 لعام 2018 على الآتي: " تحدث م

حاكم جزائية بدائية واستئنافية للنظر في قضايا جرائم المعلوماتية وجرائم الاتصالات تملأ وظائفها من الملاك العددي لكل محافظة وتوزع بقرار من مجلس القضاء الأعلى ".

تقسم المحاكم الجزائية إلى محاكم درجة أولى من صلح وبداية تختص بالمخالفات والجنح، ومحكمة درجة ثانية وهي الاستئناف، ومحكمة درجة أخيرة وهي محكمة الجنايات [5]، وقد رغب المشرع السوري وفقاً للمادة الثانية السالفة الذكر أن يخصص محاكم جزائية بدائية واستئنافية للنظر في الجرائم المعلوماتية وجرائم الاتصالات.

إن هذا النص القانوني يدل على أن قانون مكافحة الجريمة المعلوماتية يتضمن جنحاً فقط ولم ينص على مخالفات أو جنح معاقب عليها بالغرامة فقط أو بالحبس لمدة أقل من سنة أو على الجنايات، وإن كان صحيحاً أن المشرع السوري لم يفرض عقوبات تكديرية بحق مرتكبي الجرائم المعلوماتية والاتصالات، إلا أنه جعل عقوبة جرم الاحتيال المشدد عقوبة جنائية الوصف، كما أن هناك عدداً من الجرائم الجنحية الوصف المعاقب عليها بالغرامة فقط ، ومثال ذلك جرم الدخول غير المشروع إلى منظومة معلوماتية حيث عاقب المشرع بموجب المادة 15 من قانون مكافحة الجريمة المعلوماتية رقم 17 لعام 2012 على ارتكاب هذه الجريمة بالغرامة من عشرين ألف إلى مئة ألف ليرة سورية.

[5] المواد 165 و169 و 172 من قانون أصول المحاكمات الجزائية رقم 112 لعام 1950 ، والمواد 32 و38 و40 و42 من قانون السلطة القضائية رقم 98 لعام 1961 .

وقد نصت المادة 166 من قانون أصول المحاكمات الجزائية[6] على اختصاص محكمة الصلح : " تحكم محكمة الصلح في الجنح المنصوص عليها في قانون العقوبات والقوانين الأخرى متى كانت هذه الجنح معاقباً عليها بالإقامة الجبرية أو بالغرامة أو بالحبس مدة لا تتجاوز السنة أو بهما معاً " .

وتبعاً لذلك فإن جرائم المعلوماتية والاتصالات المعاقب عليها بالغرامة، ومنها جرم الدخول غير المشروع إلى منظومة معلوماتية أو المعاقب عليها بالحبس لمدة لا تتجاوز السنة ستكون من اختصاص محكمة البداية وليس من اختصاص محكمة الصلح خلافاً للقواعد العامة المنصوص عليها في قانون أصول المحاكمات الجزائية.

وإذا كان من الممكن الرد على ذلك من خلال ما نصت عليه المادة 25 من قانون السلطة القضائية : " المحاكم على اختلاف أنواعها ودرجاتها تفصل في جميع الدعاوى والمعاملات التي تفرض عليها في حدود اختصاصها إلا ما استثني بنص خاص " ، إلا أنه يجب أن لا يغيب عن فكرنا أن السياسة الجنائية الإجرائية للمشرع السوري فرضت تخصيص محكمة الصلح بالجرائم البسيطة في حين حُدد اختصاص محكمة البداية بالجنح المعاقب عليها بالحبس أكثر من سنة. وتكمن فلسفة المشرع من ذلك في عدم إشغال محاكم البداية بالجنح البسيطة وتركها لاختصاص محكمة الصلح هذا من جهة، ومن جهة أخرى بالعودة للأسباب الموجبة لصدور القانون رقم 9 لعام 2018 لا نجد أي سبب لإدخال هذه الجنح البسيطة في اختصاص محاكم البداية، ومن ثمَّ لم يعلل المشرع رغبته في الخروج عن القواعد العامة، ولذلك فإنه يتوجب إعادة ترتيب الهيكل التنظيمي للمحاكم المختصة بالجرائم المعلوماتية والاتصالات لتجد محاكم الصلح مكانها في هذا الهيكل.

[6] قانون أصول المحاكمات الجزائية رقم 112 لعام 1950

رابعاً: عدم اختصاص المحاكم المتخصصة بالجرائم المعلوماتية بالجرائم المتلازمة بالجرائم المعلوماتية:

نصت الفقرة ب من المادة الخامسة من القانون رقم 9 لعام 2018 الخاص بتشكيل محاكم متخصصة للجرائم المعلوماتية وجرائم الاتصالات: " تبقى جرائم المعلوماتية المرتبطة بجرائم تمويلية أو مالية أو إرهابية أو متعلقة بأمن الدولة من اختصاص المحاكم الناظرة بها موضوعاً" .

وتبعاً لذلك فإنه إذا كانت الجريمة المعلوماتية تتعلق بجريمة تمويلية أو مالية أو إرهابية أو بأمن الدولة فإن الاختصاص يبقى للمحاكم الناظرة بهذه الجرائم وليس للمحاكم المحدثة للجرائم المعلوماتية، ومثالها جرائم الاحتكار والاختلاس وتمويل العمل الإرهابي والخيانة.

ولابد من الإشارة بداية إلى أن الجرائم التمويلية هي الجرائم المنصوص عليها في القانون الخاص بحماية المستهلك رقم 20 لعام 2014 ، في حين أن الجرائم المالية تشمل الجرائم الاقتصادية المنصوص عليها في القانون رقم 3 لعام 2013 الخاص بالجرائم الاقتصادية والمالية وجرائم الصرافة وغسل الأموال، أما الجرائم الإرهابية فهي الجرائم المنصوص عليها في قانون مكافحة الإرهاب، والجرائم الماسة بأمن الدولة وهي الجرائم المعددة في قانون العقوبات من المادة 260 حتى المادة 311 سواء المتعلقة بأمن الدولة الداخلي أو الخارجي.

وبالرجوع إلى نص الفقرة ب من المادة الخامسة من القانون رقم 9 لعام 2018 نجد أن المشرع استعمل عبارة: " جرائم المعلوماتية المرتبطة بجرائم ....". إن هذا المصطلح وهو: " مرتبطة " أو "الارتباط" هو مصطلح غير منصوص عليه في قانون أصول المحاكمات الجزائية السوري، في المقابل نجد أن الفقه المصري استعمل مصطلح: " الجرائم المرتبطة"[7] ،

[7] د. رؤوف عبيد ، مبادئ الإجراءات الجنائية ، دار النهضة العربية ، القاهرة ، 1983 ، ص 582

إلا أن المشرع السوري استعمل مصطلح " الجرائم المتلازمة "[8] ، حيث نص قانون أصول المحاكمات الجزائية على حالات الجرائم المتلازمة ومن هذه الحالات الجرائم التي يكون بعضها توطئة للبعض الآخر أو تمهيداً لوقوعه وإكماله أو لتأمين بقائه دون عقاب. وفي هذه الحالة يوجد تتابع أفعال يشتق بعضها من بعض وتقوم بينها علاقة السبب والنتيجة دون أن يؤخذ الزمن أو المكان أو الأفراد بعين النظر، فقد يكون مرتكب هذه السلسة من الجرائم شخصاً واحداً كما قد يكونوا أشخاصاً متعددين[9]. ويمكن طرح الأمثلة الآتية:

إن التلازم من الممكن أن يكون بين جريمة معلوماتية وهي جريمة الدخول غير المشروع إلى منظومة معلوماتية وجناية سرقة معلومات ماسة بأمن الدولة وهي إحدى جرائم التجسس إذا كان الدخول توطئة وتسهيلاً لسرقة المعلومات.

وقد يكون التلازم موجوداً بين جريمة معلوماتية وهي جنحة تغيير معلومات ضمن منظومة معلوماتية وجناية غسل الأموال، وهي جريمة مالية، إذا كان تغيير المعلومات تسهيلاً لارتكاب جناية غسل الأموال.

وقد يكون التلازم أيضاً بين جريمة معلوماتية وهي جنحة استعمال برمجية خبيثة وجنحة احتكار المواد الغذائية، وهي جريمة تموينية، إذا كان استعمال هذه البرمجية بقصد تسهيل جرم الاحتكار.

وأخيراً قد يكون التلازم موجوداً بين جريمة معلوماتية وهي جنحة اعتراض المعلومات وجناية القيام بعمل إرهابي إذا كان هذا الاعتراض توطئة للقيام بعمل إرهابي. وقد حكمت الغرفة الجنائية في محكمة النقض السورية في هذا الصدد بأنه: " تنظر محكمة الإرهاب

[8] د. عبد الوهاب حومد ، اصول المحاكمات الجزائية ، المطبعة الجديدة ، دمشق ، 1987 ، ص 467

[9] د.بارعة القدسي ، اصول المحاكمات الجزائية ، الجزء الأول . مطبوعات جامعة دمشق ، 2013 ، ص 70

أيضاً بباقي الجرائم المحالة إليها من قبل نيابة الإرهاب، والتي تكون متلازمة مع جرم إرهابي أو جرائم لها صلة بالإرهاب [10]".

ولذلك كان يفضل أن يستعمل المشرع السوري مصطلحاً يتفق مع قانون أصول المحاكمات الجزائية السوري، وهو مصطلح الجرائم المتلازمة. هذا من جهة أولى، ومن جهة ثانية استعمل المشرع السوري مصطلح الجرائم المالية وهو مصطلح غير دقيق، فهو واسع التفسير وغير واضح المعالم، ولا يوجد أي معيار يمكن من خلاله تحديد ما هي الجرائم المالية. فهل هو محل الجريمة كما هو الحال في الجرائم الواقعة على الأموال المنصوص عليها في قانون العقوبات كالسرقة وإساءة الائتمان؟ أم هو معيار وسيلة ارتكاب الجريمة كجرائم الصرافة مثلاً؟ أم هو المال العام كما نص عليه قانون العقوبات الاقتصادية؟

إضافة إلى ذلك تثور مشكلة أخرى تتعلق بما إذا كانت الجريمة المعلوماتية متلازمة مع جريمة أخرى وكان كل منهما من اختصاص محكمة مختلفة عن الأخرى. ولتوضيح ذلك يُمكن طرح المثال الآتي: إذا كانت الجريمة المعلوماتية جنحية الوصف ومعاقباً عليها بالحبس أكثر من سنة كالاحتيال البسيط، في حين كان الجرم المرتبط معها جنحوي الوصف ولكن معاقب عليه بالحبس أقل من سنة وهو من اختصاص محاكم الصلح، فكيف يمكن ملاحقة الجريمة المعلوماتية المعاقب عليها بعقوبة جنحية أكثر من سنة أمام محكمة الصلح؟ وكذلك الأمر إذا كانت الجريمة المعلوماتية جنائية الوصف كالاحتيال المشدد في حين كان الجرم المرتبط معها جنحوي الوصف، وهو من اختصاص محاكم الصلح أو البداية، فكيف يمكن ملاحقة الجريمة المعلوماتية المعاقب عليها بعقوبة جنائية أمام محكمة الصلح أو البداية؟

[10] قرار محكمة النقض السورية رقم 519 تاريخ 2018/3/27 ، منشور في مجلة المحامون لعام 2019 ، ص 123

خامساً: إحالة الدعاوى المنظورة إلى المحاكم المختصة بجرائم المعلوماتية وجرائم الاتصالات:

نصت الفقرة أ من المادة الخامسة من القانون رقم 9 لعام 2018 على أن: " تحال القضايا المتعلقة بجرائم المعلوماتية وجرائم الاتصالات القائمة بوضعها الراهن إلى المحاكم المختصة المحدثة بموجب أحكام هذا القانون وفقاً لقواعد الاختصاص المكاني " .

راعى المشرع السوري من خلال أحكام الفقرة أ من المادة الخامسة النصوص الجزائية الموضوعية الواردة في القسم العام من قانون العقوبات. فمن المبادئ العامة أن القانون الجزائي لا يسري بأثر رجعي، إلا أن المشرع السوري لم يطبق ذلك على القواعد الجزائية الإجرائية حيث تسري هذه القواعد بأثر فوري ومباشر على جميع الدعاوى التي ما تزال قائمة أمام الدوائر القضائية ولم يصدر فيها حكم مبرم[11]. ويمكن أن نبرر نص الفقرة أ من المادة الخامسة من القانون رقم 9 لعام 2018 في ثلاثة أمور: فمن جهة أولى إن قواعد الاختصاص القضائي من القواعد الإجرائية، ومن جهة ثانية إن الغاية من تعديل القوانين المتعلقة بالاختصاص هو تأمين أفضل السبل وأيسرها لتحقيق العدالة الجزائية، ومن جهة ثالثة إن قواعد الاختصاص تهدف لضمان مصلحة المدعى عليه ما دامت الغاية منها إدانة المجرم وبراءة البريء[12] .

ومن ثمَّ فإن ما جاء به القانون رقم 9 لعام 2018 لا يشكل أي مساس بمبدأ عدم رجعية القوانين الجزائية. هذا من جهة ، كما أنه ،ومن جهة أخرى، لا يشكل أي عقبة في إطالة سير الإجراءات الجزائية كون نص المادة الخامسة تضمن عبارة " تحال القضايا.....بوضعها الراهن "، أي إن المحكمة المختصة نوعياً ومكانياً والتي ستحال إليها الجريمة المعلوماتية أو جريمة الاتصالات ستتابع القضية من حيث ما وصلت إليه المحكمة

[11] د. بارعة القدسي ، مرجع سابق ، ص 12

[12] J.Pradel, Droit pénal général , éd. Dalloz, 2005, p.204

التي كانت في حوزتها هذه الدعوى ولن تبدأ الإجراءات من جديد ، وتعدّ كافة الإجراءات المتخذة سابقاً صحيحة ويمكن للمحكمة الجديدة أن تعتمدها في إصدار قراراها ، إلا أن ذلك لا يمنع المحكمة الجديدة من إعادة بعضها في حال رأت أن ذلك يتلاءم مع قواعد العدالة الجزائية ،ومثال ذلك إعادة الاستماع إلى أحد الشهود لاستيضاح بعض النقاط الغامضة أو استيضاح بعض الأمور عن الأدلة الرقمية من الخبراء المختصين بالجرائم المعلوماتية.

ومن جهة ثالثة، لا تستطيع المحكمة الناظرة في الدعوى قبل صدور القانون رقم 9 لعام 2018 أن تكمل سيرها في الإجراءات، لأن النص القانوني جاء آمراً ملزماً حيث استعمل المشرع مصطلح " تحال "، وهذا التعبير يدل على الوجوب وليس على الجواز، وفي حالة مخالفة ذلك فإن هذه الإجراءات تعدّ باطلة بطلاناً مطلقاً، وعلى المحكمة الجديدة أن تبطلها وأن تعيدها من جديد.

ومن جهة رابعة، لا يطبق نص المادة الخامسة في حال كانت المحكمة قد فصلت في موضوع النزاع لأن القضية تكون قد خرجت من حوزتها ولم يبق لها أي اختصاص عليها، ومن ثَمَّ ليس لها أن تحيلها إلى المحكمة المختصة بالجرائم المعلوماتية وجرائم الاتصالات.

ومن جهة خامسة، كان من الأنسب أن يستعمل المشرع مصطلح "الدعاوى" وليس "القضايا"، وذلك تماشياً مع المصطلح القانوني الوارد في قانون أصول المحاكمات الجزائية، حيث جاء في هذا القانون كلمة الدعوى وليس القضية في مختلف مواده، فالنيابة العامة تقوم بتحريك الدعوى ومباشرتها[13] وليس القضية، والمحكمة تنظر في الدعوى وليس القضية .

[13] د.بارعة القدسي ، اصول المحاكمات الجزائية ، الجزء الأول . مطبوعات جامعة دمشق ، 2013 ، ص 91

المبحث الثاني

ملاءمة الصلاحيات الممنوحة للنيابة ولقضاة التحقيق لخصوصية جرائم المعلوماتية

تضمن قانون أصول المحاكمات الجزائية مواداً خاصة بصلاحيات النيابة العامة وصلاحيات قضاة التحقيق. وعند صدور القانون رقم 9 لعام 2018 ، توقع العاملون بالشأن القانوني تفريد هذه الصلاحيات لتتلاءم مع الطبيعة الخاصة للجرائم المعلوماتية وجرائم الاتصالات، إلا أن نص المادة الأولى في فقرتيها ب و ج لم يحقق هذه الرغبة . لذلك لابد من تقسيم هذا المبحث إلى مطلبين ندرس في المطلب الأول تقلص صلاحيات النيابة العامة، وفي المطلب الثاني نعالج تفريد صلاحيات قاضي التحقيق.

المطلب الأول: صلاحيات النيابة العامة:

النيابة العامة جهاز مستقل من أجهزة القضاء مهمتها إقامة الدعوى العامة باسم المجتمع، وواجبها البحث عن الحقيقة وليس السعي إلى إدانة المدعى عليه إذا لم تقتنع بمسؤوليته، لأنها ليست خصماً شخصياً له، وإنما هي خصم شكلي فقط، ويترتب على ذلك أن يتصرف عضو النيابة العامة كما يتصرف الحرس الشريف في حدود الحق وقواعد إثباته[14].

وقد حددت المادة 15 من قانون أصول المحاكمات الجزائية مهماتها فنصت: " يراقب النائب العام سير العدالة ويشرف على الدوائر القضائية والسجون ودور التوقيف وعلى تنفيذ القوانين، ويمثل السلطة القضائية لدى المحاكم والدوائر القضائية، ويخابر وزير العدل رأساً، وهو الذي يحرك دعوى الحق العام وينفذ الأحكام القضائية" . وقد وسع المشرع هذه الصلاحيات في حال الجرم المشهود وفقاً لنصوص المواد 29 وما يليها من قانون أصول المحاكمات الجزائية حيث منحها صلاحية الانتقال إلى موقع الجريمة، ومنع الأشخاص الموجودين في مسرح الجريمة من الابتعاد، وضبط الأدلة المساعدة على إظهار الحقيقة،

[14] Graven , Organisation et function du ministère public, R.S.C. , 1964 , p.71

والانتقال إلى المساكن للتفتيش عن الأشياء التي تؤدي إلى إظهار الحقيقة، وضبط هذه الأدلة[15] .

ووسع المشرع صلاحية النيابة العامة في الجرائم الواقعة داخل المساكن وفقاً للمادة 42 من قانون أصول المحاكمات الجزائية: " يتولى النائب العام التحقيق وفقاً للأصول المعينة للجرائم المشهودة إذا حدثت جناية أو جنحة وإن لم تكن مشهودة داخل بيت وطلب صاحب البيت إلى النائب العام إجراء التحقيق بشأنها".

وقد جاءت الفقرة ب من المادة الأولى من القانون رقم 9 لعام 2018 لتؤكد هذه الصلاحيات : " تمارس النيابة العامة المحدثة وفقاً لأحكام الفقرة أ من هذه المادة سائر الصلاحيات المخولة للنيابة العامة بمقتضى النصوص القانونية النافذة"، حيث لم يمنح المشرع في هاتين الفقرتين للنيابة العامة ولقضاة التحقيق سوى الصلاحيات الممنوحة لهم بمقتضى النصوص القانونية النافذة وفي مقدمتها قانون أصول المحاكمات الجزائية الذي لا يمكن أن تتلاءم قواعده مع الطبيعة الخاصة لهذه الجرائم نظراً إلى طبيعة الدليل الرقمي الذي يعد الدليل الأساسي في إثبات ارتكابها . فالدليل الرقمي دليل غير مرئي، إضافة إلى وجود حجم كبير من المعلومات والبيانات التي يوجد فيها هذا الدليل. وسندرس هذا المطلب من خلال أولا: التفتيش وثانياً: الضبط.

أولاً : التفتيش:

التفتيش هو البحث عن أشياء تفيد الكشف عن جريمة وقعت ونسبتها إلى المشتبه به [16]. وقد حدد المشرع السوري في قانون أصول المحاكمات الجزائية قواعد يجب اتباعها عند التفتيش وخاصة للأماكن، وهذا يدل على أن هذه القواعد تتطلب وجود قاضي التحقيق في

[15] د.بارعة القدسي ، اصول المحاكمات الجزائية ، الجزء الثاني . مطبوعات جامعة دمشق ، 2013 ، ص 39

[16] د.بارعة القدسي ، اصول المحاكمات الجزائية ، الجزء الثاني . مطبوعات جامعة دمشق ، 2013 ، ص 123

مسرح الجريمة للقيام بالتفتيش، إلا أن طبيعة الدليل الرقمي ربما لا تسمح بذلك فالسرعة في اكتشاف هذه الدليل تتطلب إعطاء صلاحية خاصة بالتفتيش عن بعد عن طريق اختراق الجهاز الحاسوبي المراد تفتيشه من دون علم صاحبه وتفتيشه، على أن يكون التفتيش له علاقة بالأدلة المطلوب اكتشافها[17]. ولم يكن قانون مكافحة الجريمة المعلوماتية رقم 17 لعام 2012 منسجماً مع هذه الحاجة الملحة لتطوير قواعد التفتيش حيث نص في المادة 26: " يجوز تفتيش الأجهزة والبرمجيات الحاسوبية المتصلة بأجهزة المشتبه فيه أياً كان مكان وجودها ضمن حدود الواقعة المسندة إلى المشتبه فيه".

كما أن المشرع السوري لم يتطرق إلى مشكلة وجود الأجهزة المطلوب تفتيشها خارج سورية كأن يقوم مرتكب الجريمة المعلوماتية بتخزين المعلومات والبيانات المتعلقة بالجريمة في أنظمة تقنية خارج سورية فلا يجوز في هذه الحالة للنيابة العامة أن تباشر صلاحية التفتيش خارج حدود سورية، ففي هذه الحال لابد من أخذ موافقة الدولة التي توجد هذه البيانات في أنظمتها. وطبعاً لا يخفى من هذا الإطار الدور المهم لاتفاقيات التعاون الدولي في مكافحة الجريمة المعلوماتية في ضبط هذه البيانات بالسرعة المطلوبة[18].

ثانياً: الضبط :

يقصد بالضبط وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الجريمة [19].

وقد تضمن قانون أصول المحاكمات الجزائية قواعد قانونية خاصة بضبط الأشياء المادية، أما فيما يتعلق بالمعطيات الإلكترونية فإن الجدل ثار حول ما إذا كان يجوز ضبط

[17] د. عبد الفتاح بيومي حجازي ، مبادئ الاجراءات الجنائية في جرائم الكمبيوتر والانترنت ، دار الكتب القانونية ، المحلة الكبرى، مصر ، 2007، ص 380

[18] د. طوني عيسى ، التنظيم القانوني لشبكة الانترنت ، منشورات الحلبي الحقوقية ، بيروت ، 2001 ، ص 78

[19] د.بارعة القدسي ، اصول المحاكمات الجزائية ، الجزء الثاني . مطبوعات جامعة دمشق ، 2013 ، ص 130

هذه المعطيات من معلومات وبرامج وما تحتويه صناديق البريد الإلكتروني من رسائل وصور وبيانات؟

ذهب اتجاه فقهي إلى أنه من غير الممكن ضبط البيانات الإلكترونية لانتفاء الطابع المادي لها ذلك أن هذه البيانات ليست أشياء محسوسة ومن ثمَّ لا يصلح أن يقع الضبط عليها[20]، إلا أن اتجاهاً آخر ذهب إلى إمكانية وقوع الضبط عليها فإن كان لا يتصور ضبطها باعتبارها أشياء غير محسوسة فإنه من الممكن ضبطها ونقلها إلى مكان آخر إذا أصبح لها كيان مادي كطباعة البيانات المراد ضبطها على ورق أو نسخها على دعامات مادية ، إذ في هذه الحالة تتحول المكونات المعنوية للحاسب إلى أشياء مرئية ومقروءة وتكتسب كياناً مادياً يمكن من خلاله ضبطها ونقلها من مكان إلى آخر. والقول نفسه يطبق بشأن الرسائل الإلكترونية، فللمحقق أن يضبط الرسائل المخزنة بالبريد الإلكتروني عن طريق طباعة الرسالة التي يريد ضبطها أو تسجلها في ملف أو قرص[21] . وهناك اتجاه ثالث يرى أنصاره بأنه لا فائدة من تطبيق نصوص الإجراءات الحالية المتعلقة بالضبط على البيانات المعالجة إلكترونياً بصورتها المجردة عن دعامتها المادية، بل لابد من تدخل المشرع لتوسيع دائرة الأشياء التي يمكن أن يرد عليها الضبط ليشمل البيانات المعالجة بصورتها غير الملموسة[22] .

وفي هذا الإطار، نصت المادة 26 من قانون مكافحة الجريمة المعلوماتية رقم 17 لعام 2012: " تعد البرمجيات الحاسوبية من الأشياء المادية التي يجوز تفتيشها وضبطها وفق القواعد المنصوص عليها في قانون أصول المحكمات الجزائية ". وبذلك لم يضع هذا القانون

[20] د. جميل عبد الباقي الصغير ، أدلة الإثبات الجنائي والتكنولوجيا الحديثة ، دار النهضة العربية ، القاهرة ، 2002 ، ص 87

[21] د. خالد ابراهيم ، فن الحقيق الجنائي في الجرائم الالكترونية ، دار الفكر الجامعي ، القاهرة ، 2009 ، ص 67

[22] د. هشام محمد فريد رستم ، الجوانب الإجرامية للجرائم المعلوماتية ، الطبعة الأولى ، مكتبة الآلات الحديثة ، أسيوط ، مصر ، 1992 ،ص 96 .

أي قواعد خاصة لضبط هذه البرمجيات، بل عدّها من ضمن الأشياء المادية وتطبق عليها القواعد الخاصة بهذه الأشياء.

المطلب الثاني: صلاحيات قاضي التحقيق:

تعدّ من أهم صلاحيات قاضي التحقيق سماع الشهادة[23]، ومن خلال قراءة النصوص المتعلقة بالشهادة المنصوص عليها في قانون أصول المحاكمات الجزائية، نلاحظ عدم كفاية هذه النصوص للشهادة في الجرائم الإلكترونية وجرائم الاتصالات.

فمن المبادئ العامة في الشهادة أنها كغيرها من وسائل الإثبات تخضع لتقدير قاضي التحقيق، فلا تصح مناقشته في قناعته الشخصية ولقاضي التحقيق أن يأخذ بأقوال شاهد واحد ويطرح أقوال الآخرين لأن العبرة في الاقتناع وليس بعدد الشهود وإنما بالاطمئنان إلى ما يدلي به الشهود سواء أقلَّ عددهم أم كثر[24].

إلا أن هذه الصلاحية تحتاج إلى إعادة نظر في الجرائم المعلوماتية وجرائم الاتصالات، فمن المؤكد أن الشاهد في هذه الجرائم له دور مهم في الإثبات ذلك أن شهادته وخبرته والمعلومات التي يقدمها لقاضي التحقيق ستكون مفاتيح لحل لغز الجريمة وكشف اللثام عن فاعلها، لذلك لابد من إعادة النظر في السلطات الممنوحة لقاضي التحقيق وخاصة أن هذه الشهادة ستقترب من الخبرة، ومن ثمَّ فإن سلطة القاضي في عدم الاستناد إلى شهادة الشاهد المعلوماتي لا يمكن أن تدحض إلا بشهادة شاهد آخر لها القوة ذاتها أو أكبر منها[25].

ومن الممكن تعريف الشاهد المعلوماتي بأنه: " الشخص الفني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسب الآلي، والذي تكون لديه معلومات جوهرية لازمة

---

[23] د. علي محمد جعفر ، مبادئ المحاكمات الجزائية ، المؤسسة الجامعية للدراسات والنشر والتوزيع ، بيروت ، 1994 ، ص 238 .

[24] د.بارعة القدسي ، أصول المحاكمات الجزائية ، الجزء الثاني ، منشورات جامعة دمشق ، 2013 ، ص 141 ، د. عبد الوهاب حومد ، شرح قانون اصول المحاكمات الجزائية ، المطبعة الجديدة ، دمشق ، ص 618

[25] د. حسين الغافري ، السياسة الجنائية في مواجهة جرائم الانترنت ، دار النهضة العربية ، القاهرة ، 2009 ، ص 165

للدخول إلى نظام المعالجة الآلية للبيانات متى كانت مصلحة التحقيق تتطلب التنقيب عن المعلومات بداخله[26] "، وبذلك يمكن تمييزه عن الشاهد التقليدي. ولتوضيح ذلك لابد من طرح المثال الآتي : لو افترضنا أن أحد الأشخاص ارتكب جرم الدخول غير المشروع إلى منظومة معلوماتية وقام بتغيير بعض المعلومات بداخلها، فإذا علم أحد الأشخاص بهذه المعلومة ودعي إلى الشهادة وذكر بأنه سمع بأن المدعى عليه قد قام بذلك ولا يعلم أي معلومات إضافية فيعد شاهداً تقليدياً وتنطبق عليه الأحكام العامة للشهادة، أما إذا صرح بأنه يستطيع إثبات روايته عن طريق اختراق الحاسب الآلي للمدعى عليه فإنه يصبح شاهداً معلوماتياً، وعندها يمكن لقاضي التحقيق أن يسمح له بهذا الاختراق، إلا أن هذه الصلاحية لقاضي التحقيق يجب أن تتطلبها مصلحة التحقيق في الحصول على المعلومات الجوهرية اللازمة والمهمة لاختراق الحاسب الآلي من أجل البحث عن الأدلة التي يمكن أن تنتج عن الجريمة المعلوماتية أو جريمة الاتصالات والتي تكون بداخل الحاسب[27] . وفي حال قناعة القاضي بأن الشاهد يستطيع ذلك ولا يريد القيام به فمن الممكن إلزامه بذلك وهذا ما نصت عليه المواد 62 و 109 و138 من قانون الإجراءات الجنائية الفرنسي حيث يمكن لقاضي التحقيق إلزام الشاهد بالإفصاح عن كلمات السر التي يعلمها، وفي حال رفضه ذلك فإنه يكون عرضة للعقاب.

[26] د. هلالي عبدالله ، تفتيش نظام الحاسب الالي وضمانات المتهم المعلوماتي ، دار النهضة العربية ، القاهرة ، 2004 ، ص 43

[27] د. سليمان فضل ، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية ، دار النهضة العربية ، القاهرة ، 2007 ، ص 123

الخاتمة

دخلت شبكة الإنترنت إلى المجتمع السوري في السنوات الأخيرة، وفرضت على الجميع الانخراط فيها. ومع توسع استعمالها وانتشارها بصورة واسعة بدأت تظهر الجرائم المعلوماتية، وهي جرائم تتميز بسرعة التنفيذ وتعدد أشكالها، ولم تعد شبكة الإنترنت مجرد وسيلة لتبادل معلومات، بل جعلها البعض وسيلة لارتكاب الجريمة . وهذا ما جعل المشرع يفكر جدياً في إنشاء محاكم مختصة بملاحقة مرتكبي هذه الجرائم، فصدر القانون رقم 9 لعام 2018 الخاص بتشكيل محاكم متخصصة للجرائم المعلوماتية وجرائم الاتصالات.

حاولنا من خلال هذا البحث تسليط الضوء على السياسة الجنائية الإجرائية المتبعة في إحداث محاكم متخصصة بجرائم المعلوماتية والاتصالات، ومن خلال هذه الدراسة يمكن أن نوصي بمجموعة من المقترحات الآتية:

1 . يجب تحديد الاختصاص النوعي للمحاكم المختصة بمحاكمة مرتكبي الجرائم المعلوماتية وجرائم الاتصالات، بحيث يُحصر هذا الاختصاص بالجرائم المنصوص عليها في المرسوم رقم 17 لعام 2012 الخاص بمكافحة الجريمة المعلوماتية والقانون رقم 18 لعام 2010 الخاص بجرائم الاتصالات، وإن ذلك يتطلب في الأساس تعديل تعريف الجريمة المعلوماتية الوارد في المرسوم التشريعي رقم 17 لعام 2012. فوضع تعريف محدد لهذه الجريمة يقطع المجال أمام التفسيرات المتناقضة حول ما يعدّ جرماً معلوماتياً.

2 . عدم إرهاق محاكم بداية الجزاء بكثير من القضايا الخاصة بالجرائم البسيطة التي لا تزيد فيها عقوبة الجريمة المعلوماتية بالحبس على سنة أو بالغرامة، وهذا يتطلب إحداث محاكم صلح خاصة بالجرائم المعلوماتية وجرائم الاتصالات.

3 . تخصيص قاضي إحالة مختص بالجرائم المعلوماتية وجرائم الاتصالات، فمن غير المنطقي في الدعوى الجنائية أن نخصص نيابة عامة مختصة وقاضي تحقيق مختص

بالجرائم المعلوماتية وجرائم الاتصالات، وبعد أن نصل بهذه الدعوى أمام قاضي الإحالة أو أمام محكمة الجنايات فلا نجد هذا التخصص.

4 . تعديل وتحديد بعض المصطلحات ضمن القانون رقم 9 لعام 2018 الخاص بتشكيل محاكم متخصصة للجرائم المعلوماتية وجرائم الاتصالات لتنسجم مع باقي التعابير القانونية المنصوص عليها في قانون أصول المحاكمات الجزائية. ومن ذلك تعديل مصطلح "الجرائم المرتبطة" بمصطلح "الجرائم المتلازمة" وكذلك تعديل مصطلح "القضايا" بمصطلح "الدعاوى".

5 . إزالة الالتباس حول بعض التعابير الواردة في هذا القانون، ومن ذلك مصطلح الجرائم المالية، فإذا كانت الغاية حماية الملكية الخاصة فهناك الجرائم الواقعة على الأموال، وإذا كانت الغاية حماية المال العام فهناك مصطلح الجرائم الاقتصادية أو الجرائم الواقعة على الإدارة العامة. ومن ثمَّ فإن الإبقاء على مصطلح الجرائم المالية من دون تحديد يخالف مبدأ شرعية الجرائم.

6 . تفريد صلاحيات النيابة العامة وقضاة التحقيق في الجرائم المعلوماتية وجرائم الاتصالات. ومن ذلك وضع قواعد خاصة بالشهادة بالنسبة إلى الشاهد المعلوماتي تتميز عن قواعد الشهادة بالنسبة إلى الشاهد التقليدي بحيث يمكن السماح للشاهد المعلوماتي بإحداث اختراق في النظام المعلوماتي الذي يريد إثبات شهادته من خلاله، وكذلك الأمر بالنسبة إلى وضع قواعد خاصة لتفتيش النظام المعلوماتي الموجود خارج سورية.

المراجع:

أولاً: باللغة العربية:

– د. بارعة القدسي ، اصول المحاكمات الجزائية ، الجزء الأول . مطبوعات جامعة دمشق، 2013

– د. بارعة القدسي ، اصول المحاكمات الجزائية ، الجزء الثاني . مطبوعات جامعة دمشق، 2013

– د. حسين الغافري ، السياسة الجنائية في مواجهة جرائم الانترنت ، دار النهضة العربية ، القاهرة ، 2009

– د. خالد ابراهيم ، الجرائم الالكترونية ، دار الفكر الجامعي، القاهرة ، 2009

– د. خالد ابراهيم ، فن الحقيق الجنائي في الجرائم الالكترونية ، دار الفكر الجامعي، القاهرة ، 2009

– د. جميل عبد الباقي الصغير ، أدلة الإثبات الجنائي والتكنولوجيا الحديثة ، دار النهضة العربية ، القاهرة ، 2002

– د. رؤوف عبيد ، مبادئ الإجراءات الجنائية ، دار النهضة العربية ، القاهرة ، 1983

– د. سليمان فضل ، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية ، دار النهضة العربية ، القاهرة ، 2000

– د. طوني عيسى ، التنظيم القانوني لشبكة الانترنت ، منشورات الحلبي الحقوقية ، بيروت، 2001

– د. عبد الوهاب حومد ، اصول المحاكمات الجزائية ، المطبعة الجديدة ، دمشق ، 1987

– د. عبد الفتاح بيومي حجازي ، مبادئ الاجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الكتب القانونية ، المحلة الكبرى، مصر ، 2007

– د. عبود السراج ، شرح قانون العقوبات العام ، منشورات جامعة دمشق ، 2014
– د. علي محمد جعفر ، مبادئ المحاكمات الجزائية ، المؤسسة الجامعية للدراسات والنشر والتوزيع ، بيروت ، 1994 .
– د. عمر عيسى الفقمي ، الجرائم المعلوماتية ، دار النهضة العربية ، القاهرة ، 2005
– د. محمد علي العريان ، الجرائم المعلوماتية ، دار النهضة العربية ، القاهرة ، 2000
– د. محمد عبدالله سلامة ، جرائم الكمبيوتر والانترنت ، منشأة المعارف ، الاسكندرية ، 2006
– د. هشام محمد فريد رستم ، الجوانب الإجرامية للجرائم المعلوماتية ، الطبعة الأولى ، مكتبة الآلات الحديثة ، أسيوط ، مصر ، 1992 .
– د. هلالي عبدالله ، تفتيش نظام الحاسب الالي وضمانات المتهم المعلوماتي ، دار النهضة العربية ، القاهرة ، 2004 .

ثانياً: باللغة الأجنبية :

1- J.Pradel, Droit pénal général , éd. Dalloz, 2005
2 - Graven , Organisation et function du ministère public, R.S.C. , 1964 , p.71