# تفعيل مبدأ عالمية النص الجنائي

# في التصـــدي للجريـــــمة المعلــوماتية

تاريخ استلام المقال: 22 فيفري 2017 تاريخ القبول النهائي: 19 أفريل 2017

الدكتور شوقي يعيش تمام الدكتورة عزيزة شبري

أستاذ محاضر "أ" أستاذة محاضرة "ب"

جامعة محمد خيضر - بسكرة (الجزائر)

yaichtemem@yahoo.com chebri80@yahoo.fr

**الملخص:**

يتناول المقال إمكانية تطبيق مبدأ عالمية النص الجنائي في مجال التصدي مكافحة الجرائم المعلوماتية، حيث يلاحظ في هذا الصدد أن التسليم بمبدأ العالمية أضحى ضرورة لمجابهة النشاط الإجرامي المعلوماتي بصوره المختلفة بعد استفحال خطره وانتشار آثاره في أكثر من دولة، في مقابل عجز مبدأ اقليمية النص الجنائي على التصدي لها، مما يكسب الجريمة المعلوماتية في النهاية صفة العالمية، ورغم وجود محاولات وجهود دولية ثنائية ومتعددة لإبرام معاهدات تتضمن أسس التعاون وإجراءاته في مجال محاربة الجريمة المعلوماتية، إلا أن التصدي لهاته الأخيرة بقي تعترضه عدة معوقات أبرزها اختلاف النظم الإجرائية للدول، وعدم توحيد المفاهيم بخصوص مدلول ونطاق الجريمة المعلوماتية، فضلا على عدم التنسيق الكافي والمجدي بين الدول لتكريس أسس التعاون الدولي لمواجهة خطر الإجرام المعلوماتي.

**الكلمات المفتاحية:** مبدأ العالمية، النص الجنائي، الجرائم المعلوماتية، مكافحة، المعوقات، التعاون الدولي.

**Résumé:**

L’article traite la possibilité d’appliquer le principe de l’internationalisation du texte pénal en matière de lutte contre la cybercriminalité, attendu que dans ce cas, il importe de se pencher vers le principe de l’internationalisation, désormais indispensable pour faire face aux activités cybercriminelles dans ses différentes formes, suite à l’accroissement de sa gravité et la propagation de ses effets dans plus d’un pays. Le principe de territorialisation du texte pénal à prouver son échec dans cette lutte, donnant ainsi à la cybercriminalité une qualité internationale. Nonobstant les diverses tentatives et efforts internationaux, bilatéraux et multinationaux pour la conclusion de conventions portant principes et procédures de coopération en matière de lutte contre la cybercriminalité, ce domaine demeure entravé par plusieurs obstacles, notamment la distinction des différents systèmes de procédures des pays et l’hétérogénéité des définitions de la cybercriminalité, outre la coordination internationale insuffisante et insatisfaisante.

**Mots-clés:** principe de l’internationalisation, le texte pénal, cybercriminalités, Lutte, obstacles, coopération internationale.

**مقدمة:**

من المتعارف عليه أن أي حركة تجريم أو عقاب يجب أن تستند إلى مصدر قانوني سابق تحت طائلة مبدأ الشرعية الجنائية الذي يفترض أن لا توجه إجراءات المتابعة الجزائية، أو أن يطبق جزاء جنائي معين إلا بموجب قانون يحدد ويضبط ذلك، مع مراعاة احترام مبدأ سيادة الدولة في المسائل الجنائية(مبدأ إقليمية النص الجنائي).

إن عبارة قانون المقترنة بمبدأ الشرعية توظف بمعناها الواسع الذي يقتضي وجوب الرجوع إلى مصادر القانون الجنائي (قانون العقوبات والقوانين التكميلية له)، وغني عن البيان القول أن النصوص القانونية التي تحدد دائرة التجريم والعقاب تطال كل النصوص التشريعية الصادرة عن البرلمان بوصفه جهة تشريع أصلية أو السلطة التنفيذية بوصفها جهة تشريع استثنائية، كما تطال كذلك الاتفاقيات، والجهود الدولية التي تعكس التفاف إرادة مجموعة من الدول حول قواعد وآليات جنائية مشتركة في الجانبين الموضوعي والإجرائي لمجابهة بعض الجرائم الخطيرة والعابرة للحدود على غرار الجرائم المعلوماتية، والتي أضحت تهدد وتضر ليس بدولة واحدة فحسب بل بمجموعة من الدول بالنظر إلى خصوصيتها التي تجعلها عابرة لحدود الدول، وهو الأمر الذي يؤكد أهمية إضفاء صفة العالمية والتدويل على الأحكام والقواعد التي تؤطر هاته الجريمة، وبناء عليه نثير الإشكالية التالية:

هل من شأن إلحاق صفة العالمية على النصوص الجنائية المتعلقة بالجريمة المعلوماتية توفير آليات فعالة وكفيلة بمكافحتها؟.

سوف نعالج هذا الموضوع من خلال محورين على النحو التالي:

المحور الأول: الإطار التأصيلي لمبدأي:عالمية النص الجنائي، وعالمية الجريمة المعلوماتية.

المحور الثاني: الآليات والجهود الدولية في مجال عالمية مكافحة الجريمة المعلوماتية بين الإمكانيات والتحديات

## المحور الأول: الإطار التأصيلي لمبدأي عالمية النص الجنائي وعالمية الجريمة المعلوماتية

لم يعد يقتصر تطبيق النصوص الجنائية على أساس أنها مظهر للدولة في فرض سيادتها على إقليمها بل تجاوزه إلى إمكانية تطبيقه بصفة عالمية أي على كل جريمة حتى وإن ارتكبت خارج إقليم الدولة،غير أن هذا الأمر ليس على إطلاقه بل يخضع لضوابط محددة (أولا)، والملاحظ من ناحية أخرى أن عولمة النصوص الجنائية أضحت ضرورة لا بد منها خاصة

مع تنامي خطر العديد من الجرائم كما هو الحال بالنسبة للجريمة المعلوماتية التي اصطبغت هي الأخرى بصفة العالمية (ثانيا).

أولا / ضوابط إعمال مبدأ عالمية النص الجنائي:

يمكن التمييز بين ثلاث ضوابط كما يأتي:

1- يعد مبدأ عالمية النص الجنائي صورة عاكسة للتضامن الدولي في مكافحة الجريمة التي تفنن المجرمون في اقترافها بالاستفادة من التطور العلمي الذي أتاح لهم ممارستها على مستوى دولي كالاتجار في المخدرات والقرصنة والجريمة المنظمة،وعليه فلا يوجد ما يبرره سوى فكرة حماية المصالح العامة والمشتركة للبشرية، وهو ما أدى إلى انحصار هذا المبدأ في نطاق ضيق من الجرائم[1].

2- يفترض تطبيق مبدأ العالمية أن يقبض على المتهم في إقليم دولة معينة،أو يقبض عليه في مكان لا يخضع لسيادة دولة أخرى كالبحر العام[2]، كما يلزم ألا يكون استرداد الأجنبي قد طلب أو قبل على أساس أن المقصود بهذا النص هو مواجهة الإجرام الدولي بتقرير قاعدة تسري بصفة احتياطية على الجرائم التي تخضع في الأصل لقوانين أجنبية، فإذا طلبت الدولة صاحبة السلطان الأصلي استرداد المجرم فلا يجوز إعمال النص الاحتياطي[3].

3- يشترط أن تكون الجريمة المرتكبة جناية أو جنحة معاقب عليها في شريعة الدولة التي اقترفت في أرضها هذه الجرائم[4].

ثانيا / مسوغات وآثار عالمية الجريمة المعلوماتية:

لم يلق مفهوم الجريمة المعلوماتية موقفا موحدا بين الكثير من المحاولات الفقهية لضبط مدلولها وعناصرها،وربما ما يقف وراء ذلك حسب اعتقادنا هو ارتباط هذا النوع من الجرائم بتقنية المعلومات التي هي في تطور مستمر سواء من حيث الوسيلة المستخدمة بشأنها أو الهدف من توظيفها، لهذا فلن نخوض في هذا الجدل التعريفي بقدر ما يجب أن نركز على أهم التعاريف

---

[1] – عبد الله أوهايبية، شرح قانون العقوبات الجزائري( القسم ال عام)، المؤسسة الوطنية للفنون المطبعية: الجزائر، 2011، ص ص 157، 158.

[2] – أمين مصطفى محمد، قانون العقوبات– القسم العام، نظرية الجريمة، منشورات الحلبي الحقوقية: بيروت، 2010، ص 101.

[3] – أنظر في هذا الصدد: محمد زكي أبو عامر، قانون العقوبات (القسم العام)، الدار الجامعية: بيروت، 1993، ص 57./ محمد صبحي نجم، شرح قانون العقوبات الأردني، مكتبة دار الثقافة للنشر والتوزيع: عمان، الأردن، 1991، ص 47.

[4] – محمد زكي أبو عامر، مرجع سابق، ص 57.

التي تتناسب والغرض من هذه الدراسة والذي ينظر إلى الجريمة المعلوماتية على أساس أنها "سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها"[1]، وعرفت أيضا بأنها "أي سلوك غير مشروع يرتكب بواسطة نظام حاسوبي، أو شبكة حاسوبية بغرض حيازة المعلومات أو عرضها أو توزيعها بصورة غير مشروعة"، وهي كذلك " الأعمال الإجرامية المرتكبة باستخدام شبكات الاتصالات الالكترونية وأنظمة المعلومات أو ضد هذه الأنظمة والشبكات"[2].

ولما كان من المسلم به أن الجرائم التقليدية تتسم بطابعها المحلي، على اعتبار أنها ترتكب في إقليم دولة محددة، وتحدث أثرها في حدود إقليم تلك الدولة[3]، الأمر الذي يسهل معه مواجهتها ومتابعة مرتكبيها وفقا للتشريع الجنائي الداخلي لتلك الدولة[4]، فإنه مع التطورات التكنولوجية التي شهدها عالمنا المعاصر في مجال المعلوماتية والاتصال لجأ الكثير من المجرمين إلى ارتكاب جرائم تقليدية بطرق حديثة، وذلك من خلال الاستخدام غير المشروع لشبكة الإنترنيت أو بواسطتها[5]، مما دفع المشرعين إلى التفكير الجدي في وضع قوانين داخلية لمواجهتها، وهو ما تحقق من خلال تجريم بعض الأفعال المرتبطة بها وتحديد العقوبات المقررة لها، غير أن ذلك اصطدم بطابع العالمية التي تتميز به تلك الجرائم.

ويقصد بطابع العالمية في هذا الإطار أن الجرائم المعلوماتية من الجرائم العابرة للحدود الدولية، إذ غالبا ما ترتكب في إقليم دولة معينة ويكون ضحاياها في دولة واحدة أو أكثر بحسب نوع الجريمة[6]، ويفهم من ذلك أنه يمكن أن يحصل على سبيل المثال اختراق كمبيوتر يوجد في أي نقطة من العالم أو إتلاف معطياته، دون أن تكون الحدود الجغرافية حائلا أمام

---

[1] – معاشي سميرة (ماهية الجريمة المعلوماتية)، مجلة المنتدى القانوني، قسم الكفاءة المهنية للمحاماة، كلية الحقوق والعلوم السياسية، جامعة بسكرة، العدد السابع، 2010، ص 278.

[2] – م. مشتاق طالب وهيب، (مفهوم الجريمة المعلوماتية ودور الحاسوب بارتكابها)، مجلة العلوم القانونية والسياسية، جامعة تكريت، العراق، المجلد الثالث، العدد الأول 2014، ص 420.

[3] – نوفل علي عبدالله الصفو،(جريمة إنشاء موقع أو نشر معلومات مخلة بالآداب العامة بوسائل تقنية المعلومات، دراسة مقارنة)، المجلة المصرية للدراسات القانونية والاقتصادية، العدد الثالث، يناير 2015، ص 23.

[4] –Xingan Li , « **International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene**", Webology, Volume 4, Number 3, Received August 28, 2007; Accepted September 26, 2007, Available at: http://www.webology.org, at the date of March 2, 2015.

[5] – نبيلة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، مصر، ص 30.

[6] – رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الأنترنيت"، مذكرة مقدمة لنيل شهادة الماجستير في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد– تلمسان،2012/2011، ص 43.

ذلك[1]، طالما أن هذا الفعل يتم في فضاء معلوماتي لا يعترف بالحدود، الأمر الذي يشكل تحديا كبيرا لكل دول العالم دون استثناء.

ولعل مما يترتب على خاصية العالمية هنا صعوبة الكشف عن الجريمة وإثباتها طالما أن محلها في أغلب الحالات هو بيانات ومعطيات تغير أو تعدل أو تمحى من أي مكان، كما تظهر الصعوبة على صعيد آخر في إثبات مكان ارتكابها وما يترتب على ذلك كون الجريمة المعلوماتية لا تترك أي أثر خارجي لها أو أي أثر كتابي ملموس لما يجري عند تنفيذ الأفعال والأنشطة الإجرامية المرتبطة بها[2].

ولا شك أن خاصية العالمية التي تتميز بها الجرائم المعلوماتية، هي التي استدعت ضرورة التوجه والتفكير نحو تكريس عالمية النص الجنائي من أجل معالجة هذه الجرائم بفعالية، لاسيما أنه كثيرا ما تكون إجراءات المتابعة المحددة في القوانين الداخلية للدول عاجزة عن معالجتها لوحدها.علاوة على ذلك بات اختلاف القواعد الموضوعية والإجرائية المتعلقة بهذه الجرائم، من أهم الإشكالات التي تقف حائلا أمام إمكانية متابعة مرتكبيها خارج إقليم الدولة.

وهكذا يبدو أن خاصية العالمية المرتبطة بالجرائم المعلوماتية، من أهم السمات التي أضفت الخصوصية على تلك الجرائم، وأدت إلى عدم فعالية مواجهتها بتطبيق النصوص الجنائية الداخلية للدول، لذلك أضحى من الأهمية بمكان تظافر الجهود على المستويين الدولي والإقليمي في سبيل وضع قانون دولي موحد لمكافحتها.

## المحور الثاني: الآليات والجهود الدولية في مجال عالمية مكافحة الجريمة المعلوماتية (الإمكانيات والتحديات)

الواقع أن خاصية العالمية التي تميز جرائم المعلوماتية قد دفعت رجال القانون والفقهاء إلى الدعوة لضرورة مواجهة هذه الجرائم من خلال وضع قواعد اتفاقية تعبر عن تصور دولي موحد من شأنه تدارك النقائص والثغرات التي تعتري منظومة القوانين الداخلية للدول وذلك بهدف التقليل من حدة آثار هذه الجريمة إن لم نقل القضاء عليها نهائيا.

---

[1] – عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية، دراسة مقارنة، رسالة ماجستير في القانون العام، جامعة الشرق الأوسط، 2014، ص 20.

[2] – عادل يوسف عبد الغني الشكري،(الجريمة المعلوماتية وأزمة الشرعية الجزائية)، مجلة مركز دراسات الكوفة، كلية القانون الكوفة، العدد السابع 2008، ص 116.

وفي هذا الإطار تظافرت الجهود على المستوى العالمي من أجل وضع إطار قانوني اتفاقي يسمح بمتابعة مرتكبي جرائم المعلوماتية ومعاقبتهم، وهو الأمر الذي تجسد في إبرام الكثير من الاتفاقيات الثنائية والمتعددة الأطراف المتعلقة بالمسألة، سواء على المستويين الدولي أو الإقليمي(أولا)، ولكن هذا لا ينكر أو يحجب الصعوبات والتحديات التي تعترض عولمة النص الجنائي في مجال مكافحة الجريمة المعلوماتية(ثانيا).

أولا / الآليات والجهود الدولية المتخذة بصدد مكافحة الجريمة المعلوماتية:

من المعلوم أن الجرائم المعلوماتية ظهرت في الدول المتقدمة، ولا غرابة في ذلك على اعتبار أن تلك الدول كانت سباقة إلى استخدام البيئة الرقمية في تعاملاتها العادية والتجارية والمالية وغيرها[1].

لذا برزت الحاجة إلى توحيد الجهود الدولية في هذا المجال، وهو ما تجسد فعلا بعقد الكثير من المؤتمرات المتعلقة بالموضوع وإبرام اتفاقيات تخص المسألة، وعلاوة على ذلك تم وضع قوانين نموذجية لمواجهة هذه الجرائم في مجالات متعددة، ومن أجل بيان تلك الجهود من الأهمية بمكان الإشارة إلى بعضها بإيجاز فيما يأتي[2]:

أ- المؤتمر الدولي لحقوق الإنسان الخاص لسنة 1968[3]:

يعتبر هذا المؤتمر من أول المؤتمرات التي تعكس الجهود الدولية في مكافحة جرائم الأنترنيت، حيث عقد بالعاصمة الإيرانية في نهاية ستينيات القرن الماضي، وقد أكدت الفقرة 18 من هذا الإعلان صراحة إلى أن التقدم العلمي والتقني يمكن أن يعرض حقوق وحريات

---

[1] - ذلك أن خطر الجريمة المعلوماتية يمس جميع الميادين، فمن المتصور أن تتسبب في خلق شلل كامل للأنظمة المدنية والعسكرية والأرضية والفضائية، وتعديل المعدات الإلكترونية، واختراق النظم المصرفية، وإرباك حركة النقل وشل محطات الطاقة بواسطة قنابل معلوماتية ترسلها على مسافات تتعدى ألاف الأميال، مشار إليه: أحمد عبد الرحمان البعادي، دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول، المؤتمر الثالث لرؤساء المحاكم العليا بالدول العربية، أيام 23 و24 و25 سبتمبر 2012، الخرطوم، السودان، ص 03.

[2] - راجع: سيناء عبدالله محسن، المواجهة التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية والوطنية، مداخلة مقدمة ضمن أشغال الندوة الإقليمية حول الجرائم المتصلة بالكومبيوتر"، المنظمة من طرف برنامج الأمم المتحدة الإنمائي – برنامج إدارة الحكم في الدول العربيةPOGAR –UNDP ، يومي 19 و20 يونيو 2007، المملكة المغربية، ص 54 وما بعدها.

[3] - La proclamation de Téhéran, l'Acte final de la Conférence internationale des droits de l'homme, Téhéran, du 22 avril au 13 mai 1968, U.N. Doc. A/CONF. 32/41 à 3 (1968), disponible sur le site: www1.umn.edu, en date du 15 mai 2015.

الفرد للخطر[1]، وهو الأمر الذي لقي صدى واسعا من طرف الغالبية العظمى من الدول المتقدمة،وذلك من خلال التجسيد الفعلي لمضمون هذه التوصية في تشريعاتها الداخلية.

**ب- قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية لسنة 1996[2]:**

علاوة عن المؤتمر السابق الإشارة إليه، يعد هذا القانون من أهم الجهود الدولية في مجال مكافحة الجرائم المتعلقة بالمعلوماتية على المستوى الدولي، وقد كان لبنة للعمل الكبير الذي قامت به لجنة الأمم المتحدة للقانون التجاري الدولي "الأنسترال" في سبيل وضع نصوص نموذجية لتزويد المشرعين الوطنيين بمجموعة قواعد مقبولة دوليا ترمي إلى تذليل العقبات القانونية وتعزيز القدرة على التنبّؤ بالتطورات القانونية في مجال التجارة الإلكترونية لمواجهة جرائم المعلوماتية في مجال التجارة الإلكترونية، وقد لقي هذا القانون قبولا من طرف مشرعي الدول والمتعاملين، لاسيما بعد أن اعتمدته لجنة الأمم المتحدة سنة 1996.

**ج- القانون النموذجي المتعلق بالتوقيع الإلكتروني لسنة 2001[3]:**

حيث يعتبر هذا القانون تكملة للجهود التي بذلتها لجنة " الأونسترال" في سبيل مكافحة الجرائم المعلوماتية المتعلقة بالتجارة الدولية، حيث تكفل بوضع قواعد موحدة من شأنها حماية التوقيع الإلكتروني، وهو ما كرسته الكثير من الدول في تشريعاتها الداخلية.

علاوة عن الجهود الدولية لمواجهة الجرائم المعلوماتية عكفت الكثير من الدول إلى معالجة هذه الجرائم على المستوى الإقليمي، وهذا ما يتضح من خلال النموذجين التاليين:

**د- الاتفاقية الأوروبية لجرائم الانترنيت لسنة 2001:**

دخلت هذه الاتفاقية حيز التنفيذ سنة 2004، ويطلق عليها البعض تسمية اتفاقية بودابست، وقد جاءت تتويجا للجهود التي بذلها المجلس الأوروبي في سبيل التوصل إلى وضع إطار اتفاقي فعال لمكافحة الجرائم المعلوماتية، ومن أهم الدول التي وقعت عليها خارج دول الاتحاد الأوروبي نذكر جنوب إفريقيا واليابان والولايات المتحدة الأمريكية[4].

وتنبع أهمية هذه الاتفاقية في كونها اتفاقية تهدف إلى توفير إطار دولي مشترك للتعامل مع الجرائم الالكترونية حيث تلتزم الدول الموقعة عليها بتعديل تشريعاتها لمواجهة

---

[1] - Le 18 alinéa de la proclamation de Téhéran dit que: « Si les découvertes scientifiques et l'évolution de la technique ont récemment ouvert dévastes perspectives au développement économique, social et culturel, ces progrès peuvent néanmoins mettre en danger les droits et libertés de l'individu et requièrent donc une attention vigilante ».Ibid.

[2] - Loi type de la CNUDCI sur le commerce électronique (1996), disponible sur le site: https://www.uncitral.org/pdf/french/texts/.../05-89451_Ebook.pdf, en date du 04 mai 2015.

[3] - Loi type de la CNUDCI sur les signatures électroniques (2001), disponible sur le site:https://www.uncitral.org/pdf/french/texts/electcom/ml-elecsign-f.pdf, en date du 22 avril 2015.

[4] - أحمد عبد الرحمان البعادي،المرجع السابق، ص 12.

التحديات التي تفرضها تكنولوجيا المعلومات إذ تولت تحديد الجرائم المعلوماتية، واعتماد أدوات إجرائية لمكافحة الجريمة المعلوماتية وضبط مرتكبيها[1].

هـ- قانون عربي استرشادي لمكافحة الجريمة المعلوماتية:

لقد تم اعتماد مشروع هذا القانون في الدورة التاسعة عشر لمجلس وزراء العدل العرب سنة 2003، قبل أن يعتمده وزراء الداخلية العرب سنة 2004[2].

والملاحظ أن هذا القانون قد أشار لأنواع الجرائم التي تقع عن طريق الكمبيوتر والانترنت بصفة عامة، وأحال إلى التشريعات الداخلية كلما يتعلق الأمر بأركان هذه الجرائم وكذلك العقوبات التي تطبق عليها، وفي هذا السياق تضمن الباب السابع من هذا القانون فصلا خاصا يتعلق بالجرائم المعلوماتية الواقعة على حقوق الأشخاص، حيث أدرجت فيه أربعة مواد (من المادة461إلى المادة 464 منه)، وأشارت إلى حماية خصوصية الأشخاص من خطر الجرائم المعلوماتية وكيفية تتبع المجرمين والعقوبات المقررة لهذه الجرائم[3]، ومن المفيد الإشارة في هذا الصدد إلى أن هذا القانون فضفاض ولم يعط الجريمة المعلوماتية ما تستحقه من الاهتمام[4]، الأمر الذي جعل أحكامه عاجزة عن مواجهة خطر الجرائم المعلوماتية.

وعلى أية حال يتضح من كل ما سبق أن الدول قد استشعرت خطورة الجرائم المرتبطة بالمعلوماتية، لذا بذلت جهودا كبيرة من أجل إيجاد تنظيم موحد لمواجهتها، وذلك من خلال إبرام العديد من الاتفاقيات على المستويين الدولي والإقليمي، لكن كل تلك الجهود تظل بدون فعالية طالما لم يتم تكريس البنود التي أقرتها الاتفاقيات في صلب القوانين الداخلية للدول، بما يفسح المجال أمام التنسيق والتعاون القضائي بين الدول.

---

[1] - Conseil de l'Europe, Convention sur la cybercriminalité, STE n° 185 , Budapest, 23.XI.2001, pp.1-26, disponible sur le site:http://www.aedh.eu/, en date du 01 mars 2016.

[2] – قشقوش هدى حامد، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، مصر، ص 102 وما بعدها.

[3] – تركي بن عبد الرحمان المويشر، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته"، رسالة مقدمة لنيل درجة دكتوراه في الفلسفة الأمنية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ص 175.

[4] – حسن بن أحمد الشهري، قانون دولي موحد لمكافحة الجرائم الإلكترونية، الملتقى الدولي الأول حول التنظيم القانوني للأنترنت والجريمة الالكترونية، المنظم من طرف كلية الحقوق والعلوم السياسية، يومي 27 و28 أفريل 2009، جامعة الجلفة،ص 40.

**ثانيا / التحديات التي تواجه عالمية النص الجنائي المتعلق بالجريمة المعلوماتية:**

**إن عولمة النص الجنائي المتعلق بالجريمة المعلوماتية من أصعب الأمور التي يمكن تحقيقها في الوقت الراهن على الأقل، وذلك بالنظر إلى عدة صعوبات تقف حائلا أمام هذا المسعى، والمتمثلة أساسا في اختلاف المفاهيم المتعلقة بجرائم المعلوماتية(أ)، وكذا التباين الموجود بين النظم الإجرائية للدول(ب)، إلى جانب إشكالية الاختصاص(ج)، نقص التنسيق والتعاون بين الدول لمكافحة الجرائم المعلوماتية (د)، وسنتولى تفصيل كلا منها فيما يلي:**

**أ – اختلاف المفاهيم المتعلقة بالجرائم المعلوماتية:**

**من المسلم به أن جميع الأنظمة القانونية المعروفة في العالم تعتبر أن الأفعال غير المشروعة المرتبطة بالمعلوماتية جرائم يعاقب عليها، لكنها تختلف من حيث نطاق هذا التجريم، حيث لا ينطبق هذا الوصف على جميع الأفعال المتصلة بهذا المجال،وذلك بالنظر إلى اختلاف المفاهيم التي يتأسس عليها كل نظام.**

**ويفهم منه أن أفعالا معينة يمكن أن تبقى خارج دائرة هذا الوصف إذا لم يوجد نص يؤكد صراحة على شمولها بها، فعلى الرغم من تزايد خطر هذه الجرائم على الأشخاص والأموال والمصلحة العامة جراء التزايد المضطرد لحجمها،إلا أن بعض الدول لم تدرج بعض الأفعال في دائرة التجريم، فمن المتصور مثلا أن الأفعال التي تدخل في دائرة الأفعال المخلة بالآداب العامة في دولة ما تعد من الأفعال المباحة في دول أو دولة أخرى. ومن ثمة فمن الصعوبة بمكان وضع نصوص قانونية داخلية موحدة لمواجهة جرائم الانترنيت.**

**ويتعزز هذا الطرح في ظل عجز التشريعات الداخلية للدول عن تحديد مفهوم موحد وشامل للجريمة المعلوماتية[1]، لذا يكون من الأهمية بمكان التوصل إلى تعريف جامع، من أجل الإحاطة بجميع الأفعال الإجرامية المرتبطة بالمعلوماتية[2].**

**ب – تباين النظم الإجرائية للدول:**

**فضلا على اختلاف المفاهيم المتعلقة بالجرائم المعلوماتية بين الدول، يعد تباين النظم الإجرائية من العوائق التي يصعب معها وضع قانون موحد لمكافحة الجرائم المعلوماتية، فكثيرا**

---

[1] – إيهاب ماهر السنباطي، الجرائم الإلكترونية (الجرائم السيبيرية ) قضية جديدة أم فئة مختلفة؟التناغم القانوني هو السبيل الوحيد"، مداخلة مقدمة ضمن أشغال الندوة الإقليمية حول الجرائم المتصلة بالكومبيوتر"، المنظمة من طرف برنامج الأمم المتحدة الإنمائي – برنامج إدارة الحكم فيا الدول العربيةPOGAR –UNDP ، المرجع السابق، ص 19.

[2] – Mohamed CHAWKI, **Essai sur la notion de cybercriminalité**, IEHEI, France, juillet 2006, p.06 et s.

ما تثار إشكالية اختلاف إجراءات التحري والتحقيق في الجرائم بين الدولة التي ارتكب على إقليمها الفعل الإجرامي والدولة التي حصل على إقليمها الضرر،ويتجلى ذلك في ناحيتين على الأقل.

تتمثل أولهما في إمكانية عدم إتاحة التشريع الإجرائي الجزائي للدولة الأخرى مباشرة بعض إجراءات التحري أو التحقيق،وتتمثل ثانيهما في صعوبة تطبيق إجراءات الملاحقة خارج إقليم الدولة[1]، على اعتبار أنه من المتصور جدا أن تلك الإجراءات تختلف من دولة إلى أخرى،الأمر الذي يؤدي في نهاية المطاف إلى عجز السلطات المختصة عن القيام بالإجراءات اللازمة لتحديد المشتبه بهم ومحاكمتهم، ولا تفوتنا الإشارة إلى أنه يمكن تجاوز هذا المشكل من خلال وضع قانون اتفاقي موحد يعالج المسألة.

ج- إشكالية تنازع القوانين وتنازع الاختصاص القضائي:

نتيجة القدرة على التنقل الكترونيا من شبكة لأخرى والنفاذ إلى قواعد البيانات عبر قارات ودول مختلفة تبقى معه محاكم وقوانين عدة دول مختصة بنظر ذات الفعل الإجرامي وهو الأمر الذي يشكل تحديا أمام القانون الواجب التطبيق على الجريمة[2]، وما إذا كان القاضي يحتكم إلى قانون الدولة التي إرتكب الفعل المجرم على إقليمها أم قانون الدولة التي حصل الضرر على إقليمها.

فضلا على ذلك عادة ما تثار مسألة الاختصاص القضائي بنظر النزاع المتعلق بجريمة معلوماتية، وفي هذا الصدد يضرب البعض مثلا بالجريمة التي ترتكب من طرف أجنبي على إقليم دولة ما، حيث يعود الاختصاص القضائي في هذا الفرض إلى الدولة التي أرتكب الفعل المجرم على إقليمها تطبيقا لمبدأ الإقليمية، كما يعود أيضا إلى الدولة التي يحمل الجاني جنسيتها تطبيقا لمبدأ الاختصاص الشخصي، وعلاوة على ذلك من المتصور أن يحصل تنازع الاختصاص القضائي في حالة ارتكاب الجريمة من طرف أحد المواطنين على إقليم الدولة التي يتبعها،وحصول الضرر على إقليم دولة أخرى،إذ وفقا لمبدأ الاختصاص الإقليمي يؤول اختصاص النظر في النزاع إلى قضاء الدولتين دون مفاضلة بينهما[3]، ومثل هذا الوضع لا يستبعد أن يطبق على الجريمة المعلوماتية.

---

[1] - عبد الله دغش العجمي، المرجع السابق، ص 20 وما بعدها.

[2] - كريستينا سكولمان، "الإجراءات الوقائية والتعاون الدولي لمحاربة الجريمة الإلكترونية"، مداخلة مقدمة ضمن أشغال الندوة الإقليمية حول الجرائم المتصلة بالكومبيوتر"، المنظمة من طرف برنامج الأمم المتحدة الإنمائي، برنامج إدارة الحكم في الدول العربية POGAR -UNDP ، المرجع السابق، ص 119.

[3] - صغير يوسف، المرجع السابق، ص 136.

وعلى أية حال يمكن القول أن تنازع القوانين وتنازع الاختصاص القضائي، يعتبران من المسائل المتعلقة بسيادة الدولة[1]، لكن ذلك لا يحول دون تكريس مبدأ عالمية القانون الجنائي، الذي يسمح بتطبيق القانون الجنائي للدولة على كل جريمة معلوماتية يقبض على مرتكبيها في إقليم الدولة أيا كان الإقليم الذي ارتكب فيه وأي كانت جنسية مرتكبها، وذلك بتضمين التشريعات الداخلية للدول نصوص تخضع بموجبها الجرائم المعلوماتية المرتكبة داخل إقليم الدولة أو خارجه لقانون العقوبات ولاختصاص المحاكم التي قبض على إقليمها المتهم، بالنظر إلى صفة العالمية التي تتمتع بها هذه الجرائم.

د- نقص التنسيق والتعاون بين الدول لمكافحة الجرائم المعلوماتية:

على الرغم من الخطورة التي تكتسيها الجرائم المعلوماتية، إلا أن التنسيق والتعاون الدوليين بشأنها لم يبلغ درجة الاهتمام الذي شهدته بعض الجرائم الدولية على غرار الجرائم الإرهابية،إذ ثمة نقص يشوب سبل التعاون الدولي ؛ويوفر ذلك للمجرمين ملاذا آمنا يتيح لهم ارتكاب جرائمهم دون محاسبتهم في شتى أنحاء العالم"[2]، لذا يتعين توسيع نطاق هذا التنسيق إلى الجرائم المعلوماتية، وتوطيده من خلال فتح قنوات الاتصال بين الدول[3]، بما يتيح إمكانية الكشف عن الجرائم الإلكترونية وتسهيل إجراءات التحقيق وجمع الأدلة[4].

## خاتمة:

توجت دراستنا لهذا الموضوع بالنتائج التالية:

- أضحى مبدأ إقليمية النص الجنائي مبدأ تقليدي وعاجز عن استيعاب مختلف صور النشاط الإجرامي للجريمة المعلوماتية،وهذا الأمر يعكس خصوصية الجريمة المعلوماتية التي يتجاوز مفهومها المدلول المادي للجرائم العادية، والذي يعتبر محو أساسي في تطبيق مبدأ الإقليمية، لهذا ظهرت الحاجة نحو محاولة إرساء أسس تسمح بتفعيل مبدأ عالمية النصوص الجنائية في مجال مكافحة الجريمة المعلوماتية.

---

[1] -Andrew M. Colarik, « Why we need new ideas in the fight against cybercrime", Tuesday 24 March 2015, Available on http:// www.weforum.org, at the date of June 5, 2015.

[2] – راسل تاينر، " جرائم الإنترنت:التحدي لإنفاذ القانون"، مداخلة مقدمة ضمن أشغال الندوة الإقليمية حول الجرائم المتصلة بالكومبيوتر"، المنظمة من طرف برنامج الأمم المتحدة الإنمائي – برنامج إدارة الحكم في الدول العربية POGAR -UNDP ، المرجع السابق، ص 87.

[3] – Dan Robel, I**nternational Cybercrime Treaty:Looking Beyond Ratification**, SANS Institute InfoSec Reading Room, 2007,p.43.

[4] –Xingan Li , Op.Cit.

• غياب مدلول واضح ومتكامل بين جميع النظم القانونية حول تحديد مجال وعناصر الجرائم المعلوماتية، وهو الأمر الذي صعب من إمكانية تفعيل مبدأ عالمية النص الجنائي لمكافحتها.

• غياب التنسيق الكافي والمجدي بين الدول في مجال ملاحقة وتتبع مرتكبي الجرائم المعلوماتية، الأمر الذي يزيد ويصعد من خطرها.

وانطلاقا من النتائج المبينة أعلاه نقترح ما يلي:

– ضرورة أن تبادر كل دول العالم إلى توطيد التعاون بينها من أجل اتخاذ التدابير اللازمة لمكافحة الجرائم المعلوماتية، أو على الأقل ربط اتفاقيات ثنائية بين الدول المتقاربة جغرافيا، والتي تشهد انتشارا واسعا للجريمة المعلوماتية.

– ضرورة أن تبادر وتسارع كل دولة بوضع إطار قانوني خاص يجرم استعمال أنظمة المعلوماتية لغايات غير مشروعة، وتحديد أشكال هذا النوع من الجرائم بشكل مفصل ومتجانس بين دول العالم يستوعب نطاق الأفعال المشكلة في الواقع لجرائم معلوماتية، بما من شأنه خلق تجانس بخصوص هذا النوع من الجرائم، وبالتالي إصباغ صفة العالمية على الجرائم المعلوماتية.

– تعزيز مكافحة الجرائم المعلوماتية بمبادرة الدول لإبرام لاتفاقية دولية ثنائية لمكافحة كافة صور الإجرام المعلوماتي، شريطة التقيد ببنودها في تشريعاتها الداخلية.

– يتعين أن تتبنى كل دولة تدابير إجرائية تربط صلات تعاون وتنسيق مع دول العالم، من خلال إبرام اتفاقيات متعددة الأطراف تتعلق بملاحقة المجرمين وتسليمهم والتعاون القضائي في الميدان الجنائي فيما يتعلق بالجرائم المعلوماتية.

– ضرورة التفكير في إنشاء مرصد دولي يهتم بمتابعة التطورات الحاصلة في مجال المعلوماتية وما قد يقترن بها من سلوكات وأفعال غير مشروعة، وذلك بهدف إعطاء صورة واضحة حول مختلف صور الجريمة المعلوماتية بما يسمح للأنظمة القانونية الداخلية رسم صورة وإطار تشريعي متكامل في هذا الخصوص.