كلية القانون
College of Law
QATAR UNIVERSITY جامعة قطر

دار نشر جامعة قطر
Qatar University Press

OPEN ACCESS

Submitted: 1 October 2017
Accepted: 8 March 2018

مقالة بحثية

إشكالية الاختصاص في الجرائم الإلكترونية

أنور محمد صدقي المساعدة
أستاذ القانون الجنائي المشارك، قسم القانون، كلية أحمد بن محمد العسكرية – الدوحة
masadeh@abmmc.edu.qa

ملخص

انتشرت في الآونة الأخيرة الجرائم الإلكترونية بشكل كبير جدًا، مما استدعى ضرورة وجود التشريعات التي تستطيع مكافحتها والوقوف في وجهها، وأكثر ما يواجه القضاء خلال عملية الملاحقة موضوع الاختصاص، إذ إن هذه الجرائم من الجرائم العابرة للحدود التي تُرتكب في فضاء إلكتروني، الأمر الذي يتم استغلاله من قبل مرتكبي هذا النوع من الجرائم للإفلات من العقاب. وقد قام المشرع في كل من دولة قطر والمملكة الأردنية الهاشمية وإنجلترا بوضع تشريعات معاصرة لضمان عدم إفلات هؤلاء المجرمين من العقاب، وبالرغم من ذلك فإن هذه التشريعات لا زالت بحاجة لمزيد من التعديل والتصويب. وقد قامت هذه الدراسة بإجراء مقارنة بين هذه التشريعات وتحليل موقف كل منها، فيما يتعلق بموضوع الاختصاص في الجرائم الإلكترونية، كما قامت بوضع التوصيات الملائمة، سواء من الناحية الوطنية أو من الناحية الدولية. وفي النهاية، رأت الدراسة أن وجود محكمة دولية للجرائم الإلكترونية – خاصة الخطيرة منها – أصبح ضرورة ملحة وأمرًا لا مفر منه، للحفاظ على أمن المجتمع الدولي، واقترحت الدراسة تنظيمًا خاصًا بهذه المحكمة.

الكلمات المفتاحية: جريمة، جريمة إلكترونية، اختصاص قضائي، محكمة جنائية دولية، قانون جنائي

للاقتباس: المساعدة أ.، «إشكالية الاختصاص في الجرائم الإلكترونية»، المجلة الدولية للقانون، المجلد 2018، العدد الرابع الخاص بالحصار

دار نشر جامعة قطر
Qatar University Press

كلية القانون
College of Law
QATAR UNIVERSITY جامعة قطر

OPEN ACCESS

Submitted: 1 October 2017
Accepted: 8 March 2018

Research Article

Electronic Crimes and Jurisdiction

Anwar M. S. Masadeh
Associate Professor of Criminal Law, Law Department, Ahmad Bin Mohammed Military College
masadeh@abmmc.edu.qa

Abstract

Since cybercrime has recently become widespread, the need for necessary legislations to combat it has become an imperative issue. Cybercrimes are cross-border crimes committed in the cyberspace and this is the first obstacle that faces the judicial bodies. However, perpetrators exploit it to avoid punishment. Legislators in the State of Qatar, the Hashemite Kingdom of Jordan, and England have enacted contemporary legislations to ensure the punishment of cybercriminals. Such legislations still require further amendments and revisions. This study makes a comparison between these legislations, analyzes their respective positions with regard to the jurisdiction in cybercrime, and provides appropriate recommendations at the national and international levels. Finally, this study found that the existence of an international tribunal for cybercrime has become an urgent necessity to maintain the security of the international community. In addition, it proposes the structure of this tribunal.

Keywords: Crime; Cybercrime; Jurisdiction; Criminal international court; Criminal law

للاقتباس: المساعدة أ.، «إشكالية الاختصاص في الجرائم الإلكترونية»، المجلة الدولية للقانون، المجلد 2018، العدد الرابع الخاص بالحصار

مقدمة

يلخص مؤسس شركة مايكروسوفت[1] كل ما تعانيه حياتنا المعاصرة من مشاكل بسبب التكنولوجيا الحديثة بقوله: «إن أجهزة الحاسوب وُجدت لتحل المشاكل التي لم تكن موجودة سابقًا»، وفي هذا القول من التندر بقدر ما فيه من الحقيقة، فقد أوجدت التكنولوجيا الحديثة العديد من المشاكل لحياة الإنسان، ولكنها وفي الوقت ذاته حلت له العديد من المشاكل والمعوقات التي تواجهه، سواء على الصعيد المهني أم الشخصي، كما يقول: «إن الإنترنت أصبح بمثابة وسط البلدة (town square) لهذه القرية الكونية الصغيرة».[2]

غزت التكنولوجيا الحديثة جميع مناحي حياتنا، فاختزلت الوقت وقَصَّرت المسافات، حتى غدت بالكاد تتسع لتفكير الإنسان. أصبحت التجارة والتسوق الإلكترونيين رائجين، وأصبح بمقدور الفرد أن يختار من بين آلاف السلع ما يناسب ذوقه ويلائم ميزانيته، فيشتريه ويصل لباب بيته. كما أصبح بمقدور المؤسسات والشركات ووكالات الأنباء والنوادي والمصانع أن يصلوا لكل إنسان على وجه البسيطة، وأن يطرحوا عليه سلعهم لحظة بلحظة، مما يحقق الفائدة والربح والرواج، سواء للشركة أم للفرد نفسه، وذلك من خلال المواقع الإلكترونية التي تنشئها.

ناهيك عن مواقع التواصل الاجتماعي التي اقتحمت بيوتنا وكل ثنايا حياتنا، الخاصة منها والعامة، وقد حمل هذا الأمر بين طياته الكثير من المخاطر، ذلك أن هناك مسؤولية كبيرة تقع على كاهل من يمتلك هذه المواقع الإلكترونية؛ بأن يحافظ عليها من كل عبث ومن كل اختراق قد يؤدي إلى تشويه الحقيقة أو ضياع الحقوق أو التكسب غير المشروع.

من أحدث عمليات القرصنة أو الاختراق ما حدث في شهر مايو 2017، حين تعرضت مجموعةٌ كبيرةٌ من المؤسساتِ والأفرادِ في نحو 74 دولة لهجمات إلكترونية ضخمة، في عملية تُعتبرُ الأكبرَ في التاريخ. من بين الدول التي طالها الهجوم بريطانيا وروسيا وفرنسا وألمانيا وإيطاليا وبلجيكا والولايات المتحدة، واُسْتُخْدِم في الهجوم فيروس «وانا ديكربتر» الذي يعتمد على تشفير محتويات الحاسوب، ويطالب صاحبه بفدية عن طريق نقود البيتكوينز (Bitcoin)[3] مقابل فك التشفير. بحسب محللي «Forcepoint Security Labs» فإن الهجوم كان «ذا بعد عالمي» وطال منظمات في أستراليا وبلجيكا وفرنسا وألمانيا وإيطاليا والمكسيك، وتَمَثَّلَ في «حملة كبيرة منَ الرسائل الإلكترونية المؤذية». أما في إسبانيا فقد طال الهجوم الإلكتروني العديد من الشركات من بينها شركة الاتصالات الأولى في البلاد «تليفونيكا»[4]، هذا بالإضافة إلى ما تم إعلانه مؤخَّرًا من تَعَرُّضِ وكالة الأنباء القطرية للاختراق الذي أدى بدوره لأزمة؛ أَلقت بظلالها على جميع دول الخليج العربيّ.[5] كما تَعَرَّض موقع قناة العربية لاختراق مماثل[6]، بالإضافة إلى محاولات كثيرة لاختراق العديد من المواقع الإخبارية الأخرى.

لم تكن هذه الموجةُ من الهجماتِ الإلكترونية التي طالت العديدَ من المواقعِ الإلكترونيةِ عَبْر العالم، هي الوحيدة ولكنها

---

1. ويليام هينرى جيتس الثالث (William Henry Gates III) المشهور ببيل جيتس، رجل أعمال، ومبرمج أمريكي مؤسس شركة مايكروسوفت مع بول الان (Paul Allen)سنة 1975 ويملك أكبر نصيب فردي من أسهمها. انظر: www.gatesnotes.com.

2. www.brainyquote.com

3. طرح فكرة «بيتكوين» للمرة الأولى كورقة بحثية شخص أطلق على نفسه الاسم الرمزي "Satoshi Nakamoto"، ووصفها بأنها نظام نقدي إلكتروني يعتمد في التعاملات المالية على مبدأ الند للند (peer-to-peer)، وهو مصطلح تقني يعني التعامل المباشر ما بين مُستخدِم وآخر دون وجود وسيط. توصف "بيتكوين" بأنها عملة رقمية ذات مجهولية (Anonymous)، بمعنى أنها لا تمتلك رقمًا متسلسلًا ولا أي وسيلة أخرى من أي نوع كانت؛ تتيح تتبع ما تم إنفاقه للوصول إلى البائع أو المشتري. انظر تفصيلًا: أنس المعراوي، **ماهي عملة Bitcoin الإلكترونية؟**، البوابة العربية للأخبار التقنية، aitnews، 26 أغسطس 2013، http://goo.gl/nlSY4E. تاريخ آخر زيارة للموقع 21 يونيو 2019.

4. **أكبر عملية قرصنة إلكترونية في التاريخ تهاجم 74 دولة حول العالم، آمن...نحو توعية شاملة**، 15 مايو 2017، http://amenn.net/index.php?s=id&2=cat&1=978 ، تاريخ آخر زيارة للموقع 21 يونيو 2019.

5. **موقع وكالة الأنباء القطرية يتعرض للاختراق**، بي بي سي نيوز. www.bbc.com/arabic/middleeast-40026894. 24 مايو 2017، تاريخ آخر زيارة للموقع 21 يونيو 2019.

6. **اختراق موقع قناة العربية عبر ثغرة زيمبرا الأمنية**، عالم التقنية، 3 إبريل 2014، تاريخ آخر زيارة للموقع 21 يونيو 2019.

الأَحدث، فقد أصبحت القرصنة مهنة منظمة تُمارسُ في بيئة أكثرَ تطورًا، ومن طَرَف أشخاص محترفين يستهدفون كل المجالات الحيوية؛ لا سيَّما صناعة البرمجيات، والنوتات الموسيقية، والبيانات الشخصية للأَفراد، ومصَنَّفات النشر الإلكتروني.[7] رغم كل الجهود التي تُبذل لحماية المواقع الإلكترونية إلا أنَّ احتمال تعرضها للاختراق والقرصنة أمرٌ لا زال يُشَكِّل حقيقةً صادمةً؛ لعل في موقع تويتر (Twitter)، وهو من مواقع التواصل الاجتماعي الأكثر شهرة في العالم، مثالًا كبيرًا على ذلك، إذ قامت صحيفة نيويورك تايمز بإجراء استطلاع حول هذا الموضوع، أعَدَّه الباحثان الإيطاليان؛ آندريا سْتروبا وكارلو دي ميكايلي، وكشف الاستطلاع عن حقائق وأرقام مثيرة خلال شهرين من بحثهما، فقد توصلا إلى أن عدد الحسابات الوهمية على تويتر يقدر بـ 20 مليون حساب. إن هناك تجارة وهمية لزيادة أعداد المتابعين، حيث إن عدد الأيام التي يستغرقها بائعو هذه الخدمة لإنشاء ما يصل إلى 100 ألف متابع وهمي جديد، هي خمسة أيام فقط، ويمكن أن يتحصل أصحاب الحسابات الوهمية خلال أسبوع واحد على مليون دولار؛ إذ إن متوسط سعر 1000 مُتابع وهمي هو 18 دولارًا، كما يمكنك الحصول على 125 إعادة لتغريداتك يوميًا ولمدة شهر بسعر 150 دولارًا، ولمن يبحث عن الجانب الأقل تكلفةً، هناك من يقوم بخمس إعادات للتغريدة مقابل 9 دولارات في اليوم الواحد، وتتراوح مكاسب أصحاب مشاريع الحسابات الوهمية بين 40 مليون دولار إلى 360 مليون دولار؛ حيث إن نسبة مستخدمي تويتر الحقيقيين الذين نتابعهم هي 40% فقط.

تفريعًا عما سبق؛ فإن الجرائم الإلكترونية تتميز بأنها تُرتكب في عالم افتراضي، وسلطانها غير مادي ولا يتقيد بالحدود الجغرافية. إن مرتكبي الجرائم الإلكترونية لا يعترفون بالحدود السياسية والجغرافية، ولا يحترمون الاختصاص القانوني للدول، وهذا ما يُبْرز العديد من التحديات التي تواجه الدول حال ملاحقتها لمرتكبي الجرائم الإلكترونية؛ ذلك أن الجرائم المرتكبة داخل إقليمها من قبل قراصنة محليين، يقومون في معظم الأحيان باستخدام مواقع أو وصلات إلكترونية في دول أخرى، بالإضافة إلى أن هناك الكثير من الدول التي تفتقر لتشريعات تُجَرِّمُ هذا النوع من الجرائم، أو إن التشريعات موجودة ولكنها غير كافية.[8]

وكمثال على هذا النوع من التحديات التي تواجه الجهات القضائية؛ ما حدث في بدايات العام 2000 عندما قام اثنان من القراصنة باختراق المواقع الإلكترونية لعدد من المصارف الأمريكية والحصول على بيانات العملاء ومعلومات لعدد كبير من البطاقات الإلكترونية، واستعملوا هذه البيانات لابتزاز هؤلاء الأشخاص والحصوص على أموال منهم لقاء الحفاظ على بياناتهم، وتبين لاحقًا لجهات التحقيق «FBI» أن شخصان يعيشان في روسيا هما من قاما بارتكاب هذه الأفعال. وقد قدمت السلطات الأمريكية عدة طلبات تسليم لمثيلتها الروسية، ولكنها قوبلت بالتجاهل التام من قبلها، فما كان من الشرطة الفدرالية الأمريكية إلا اتباع الحيلة وإقناع هذين الشخصين بوجود فرصة عمل لهما في الولايات المتحدة، وعندما حضرا وقابلا جهة العمل المزعومة؛ تم الحصول على كافة بياناتهما الإلكترونية، وتم مراقبة أجهزة الحاسوب الخاصة بهما والقبض عليهما[9].

كانت أُولى التشريعات التي جرَّمت الدخول غير المصرح به إلى المواقع الإلكترونية في الولايات المتحدة عام 1984، وعلى مدار العقدين السابقين فقد جرى على هذا القانون خمسة تعديلات، كان أبرزها ما تم عام 2008 والذي أظهر قانونًا متكاملًا أطلق عليه ((Computer Fraud and Abuse Act (CFAA)[10]، وقد ثار خلاف واسع بين فقهاء القانون

7. طه عيساني، القرصنة الإلكترونية، الضرر الاقتصادي والفكري، المجلد الخامس مجلة جيل الأبحاث القانونية المعَمَّقة، ص. 105 (2016).

8. Miquelon Weismann, *Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*, Havana, Cuba, August 27-September 7, 1990, 335 &. Dominic Carucci, David Overhuls & Nicholas Soares, Computer Crimes, 48 AM. CRIM. L. REV. 375, 378, 2011, 417 &.

9. Amalie M. Weber, *The Council of Europe's Convention on Cybercrime*, 18 Berkeley Tech. L.J. 227, 2003.

10. انظر تفصيلًا حول التطور التاريخي للتشريعات الإلكترونية في الولايات المتحدة الأمريكية:
Jonathan Mayer, *Cybercrime litigation*, University of Pennsylvania Law Review, 164 U. Pa. L. Rev. 1453, 10521, May 2016.

في أمريكا حول موضوع الاختصاص الذي تم تكريسه في هذا القانون، فمنهم من رأى بأنه متضارب وغير قابل للتطبيق، ومنهم من رأى أنه بحاجة إلى العديد من الاتفاقيات الدولية لإمكان تنفيذه، فيما رأى فريق آخر أن القانون توسع بامتداده بالاختصاص بشكل كبير، حتى إن بعض الفقهاء وصفه بالقانون الذي يشمل باختصاصه كل أجهزة الحاسوب المتصلة بالإنترنت في العالم.[11]

أما في الاتحاد الأوروبي فقد شهد الميثاق الأوروبي لجرائم الكمبيوتر مثالًا جيدًا للتعاون في مجال مكافحة هذه الجرائم؛ حيث تم صياغة هذا الميثاق عام 2001، وأسس لقواعد وثيقة من التعاون بين دول الاتحاد الأوروبي في مجال الاختصاص المشترك، وقد دخل هذا الميثاق حيز التنفيذ عام 2004، وتمت المصادقة عليه عام 2010 من قبل 33 دولة من بينهم الولايات المتحدة، وقد اتفقت هذه الدول استنادًا لهذا الميثاق على ثلاثة مبادئ رئيسة: أولها: ضرورة الاتفاق على الأفعال المجرمة في التشريعات الوطنية، وثانيها: تأسيس آليات وإجراءات مشتركة للتحقيق وجمع الأدلة في جرائم الكمبيوتر، وثالثها: تعزيز التعاون المشترك في مجال تسليم المتهمين والمجرمين في هذه الجرائم.[12]

لقد شكل هذا الميثاق خطوة من الخطوات الواسعة في مجال التغلب على موضوع الاختصاص في الجرائم الإلكترونية، ولكن المعوقات ما زالت موجودة، فليس جميع دول العالم أطرافًا في هذا الميثاق من ناحية، كما وجدنا أن هناك العديد من الدول كان لها تحفظات على الميثاق، خاصة في موضوع الاختصاص، مما يجعلها في حل من هذا الالتزام من ناحية أخرى.[13]

نظرًا لهذه المَزِيَّة الدولية لهذه الطائفة من الجرائم، كان لا بد للتشريعات الوطنية أن تأخذها في الحسبان في سبيل ملاحقة مرتكبيها. من هذا المنطلق ستقوم الدراسة بتناول الاختصاص القضائي لجرائم اختراق المواقع الإلكترونية في كل من التشريعات الجزائية الأردنية والقطرية وكذلك الاختصاص القضائي في التشريعات الإنجليزية وبعد ذلك اقتراح الآليات والحلول.

مبررات اختيار الموضوع

تهدد الجرائم الإلكترونية أمن المنظومة العالمية بالكامل، ولا يقتصر تأثيرها على دولة بعينها، أو منطقة محددة. كان من الضروري إيجاد آليات قانونية وتشريعية للحفاظ على الأمن العالمي، سواء من خلال التشريعات الوطنية أم من خلال الاتفاقيات الدولية. لقلة الدراسات البحثية التي أجريت حول هذا الموضوع في الفقه العربي، وقلة من قاموا بالخوض فيه، اهتمت الدراسة بسبر أغواره وتناوله من كافة زواياه، ووضع المقترحات القانونية والتشريعية اللازمة للتغلب عليه. وكذا الفضاء الافتراضي، ومكان وقوع الجريمة كذلك، بالإضافة إلى أن الفاعلين قد يكونون أكثر من واحد وكل منهم في بلد مختلف وموطن مختلف، لذلك فإن عملية ملاحقتهم تُشكل دربًا شائكًا وعرًا ينتابه الكثير من الصعوبة والغموض واللامنطقية أحيانًا، فأنت في اللامكان وفي كل مكان في آن معا، كما أنك في اللازمان وفي كل زمان كذلك.

---

11. Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, Minnesota Law Review, Vol. 94, Issue 5, & 1561-1587. 2010.

12. ترجع أصول هذا الميثاق لعام 1996، عندما قررت اللجنة الأوروبية للجرائم الإلكترونية (European Committee of Crime Problems CDPC) ضرورة تشكيل لجنة خبراء لوضع مسودة للجرائم الإلكترونية، وكان من أبرز النقاط التي أشارت إليها اللجنة أن طبيعة الجرائم الإلكترونية العابرة للحدود تشكّل تحديًا كبيرًا لسلطات تنفيذ القانون الوطنية، وأن هذا الأمر بحاجة لتعاون بين أعضاء المجموعة الأوروبية، ولا يكون ذلك إلا بوضع اتفاقية قانونية ملزمة لهذه الدول لمحاربة هذه الظاهرة (phenomena)، على حد وصف اللجنة، واستنادًا لهذا الرأي الاستشاري فقد قامت لجنة الوزراء عام 1997 بتشكيل لجنة بهذا الخصوص، وكانت المهمة المكلفة بها هذه اللجنة بالتحديد، أن تضع مسودة اتفاقية ملزمة، وأن تنهي عملها بالسرعة القصوى. انظر في ذلك تفصيلًا:
Michael A. Vatis, *The Council of Europe Convention on Cybercrime*, the national Academic Press. Washington, D. C. 2010,& 207.

13. للاطلاع على كافة السلبيات التي وجهت للميثاق الأوروبي لجرائم الكمبيوتر:
Miriam F. Miquelon-Weismann, The Convention on Cybercrime: *A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?* 23 J. Marshall J. Computer & Info. L. 329, 2005 & 329-361.

مبررات اختيار دول المقارنة

ستقوم الدراسة بتناول النصوص التشريعية في كل من الأردن وقطر وإنجلترا للوقوف على مدى كفاية النصوص المستخدمة في هذه الدول لمواجهة مثل هذه الأخطار، حيث صدر في الأردن قانون حديث لمكافحة جرائم نظم المعلومات عام 2015، ومن قبّله صدر في قطر قانون الجرائم الإلكترونية عام 2014. هما قانونان حديثان من المفروض أنهما أخذا هذا الأمر بعين الاعتبار. ستتم مقارنة هذه التشريعات ببعضها، كما ستتم مقارنتها مع قانون إساءة استخدام الحاسوب الإنجليزي لعام 1995 (Computer Misuse Act) وما طرأ عليه من تعديلات لاحقة. تم اختيار هذا القانون لإجراء المقارنة لسببين؛ أولهما: اعتبار هذا القانون قانونًا نموذجيًا من قبل الاتحاد الأوروبي ومنظمة الأمم المتحدة، وحث الدول على الاستعانة به عند وضع التشريعات الخاصة بها[14]، ثانيهما: زخم التطبيقات القضائية الإنجليزية على هذا القانون والتي سيتم الاستئناس بها في الدراسة، بالإضافة إلى عدد كبير من التعديلات التي تمت عليه، وفقًا لما سيتم تناوله في الدراسة.

مشكلة الدراسة

تقوم المشكلة الرئيسة التي تسعى الدراسة لحلها ومعرفة الوسائل والطرق اللازمة للتعامل معها، من منطلق واقع عملي نعيشه كل يوم، يزداد خطره وآثاره الفتاكة يومًا بعد يوم، ويتمثل بموجة الجرائم الإلكترونية والاختراقات التي تتم في جميع أنحاء العالم، ومشكلة وجود أو عدم وجود النصوص التي تكفل عدم إفلات مرتكبي هذه الجرائم من العقاب بدعوى عدم وجود السلطان القانوني اللازم لمتابعتهم. القانون والجريمة في سباق محموم، على القانون أن يمتلك البصر والبصيرة واستشراف المستقبل دائما ليكون قادرًا على الفوز في هذا المضمار، لا أن يكون خاسرًا ومتأخرًا؛ ما قد ينجم عنه نتائج وخيمة.

إلا أن المشكلة أكبر من مجرد وجود التشريعات التي تُجرم مثل هذه الأفعال، فقد تكون النصوص التجريمية موجودة، ولكنها لا تطال مرتكبي هذه الجرائم، وقد يرجع ذلك لعدم وجود النصوص التي تحدد قواعد الاختصاص بشكل دقيق، أو لعدم رغبة الدول الأخرى التي يوجد مرتكبو الجرائم على إقليمها بمعاقبتهم وملاحقتهم، لأي سبب كان، أو لتعنت الدول بموضوع تسليم مواطنيها أو المقيمين على أرضها. كل ذلك يقودنا للبحث عن قواعد اختصاص تمتد لتنال من هؤلاء المجرمين، ولا تجعل لها مأوى ولا ملجأ، خاصة أن الموضوع أصبح يتعلق بأمن عالمي جماعي، ولا يتعلق بالأمن الوطني فحسب.

يشكل هذا الموضوع مشكلة تدور ثناياها في نفس الباحث، سعيًا منه للحصول على الإجابات والحلول التشريعية الموجودة فعلًا وتقييمها ووزنها، وبيان مثالبها ومحاسنها، ومن ثم تقديم الحلول والمقترحات، علها تكون إضافة علمية من ناحية ويدًا ولَبِنَةً يتم البناء عليها من ناحية أخرى.

فرضيات الدراسة

هناك فرضية رئيسة تسعى الدراسة لاختبارها تتمثل بوجود تشريعات وطنية ودولية كافية، تمتد باختصاصها لتطال مرتكبي الجرائم الإلكترونية أينما كانوا وحيثما وجدوا.

أما الفرضيات المنبثقة فهي كما يلي:

تم تشريع قانون جرائم الكترونية أردني جديد، وبالتالي فهو يساير المستجدات المعاصرة، ويضع مشكلة الاختصاص في الحسبان، ويورد لها النصوص التشريعية الكفيلة بالتغلب عليها.

تم وضع قانون شامل للجرائم الإلكترونية في قطر، من المؤكد أن به من الحلول التشريعية لموضوع الاختصاص ما يسد كافة الثغرات، خاصة أنه استفاد كثيرًا من اتفاقية بودابست لمكافحة جرائم الحاسوب.

يحتوي قانون جرائم إساءة استخدام الحاسوب الإنجليزي على تفصيلات كثيرة تتعلق بموضوع الاختصاص، وذلك بعد عدد

14. The UK law was recently amended, in accordance with the European Convention on cyber-crime, by The Police and Justice Act 2006 Chapter 48, which came into force on October 1, 2008.

كبير من التعديلات التي تمت عليه، ومن الممكن أن تكون هذه التعديلات نموذجًا قانونيًا يُستفاد منه.

محددات الدراسة

حتى تقوم الدراسة بالوصول إلى أفضل النتائج؛ لا بد أن تضع لنفسها خارطة طريق واضحة المعالم لا تحيد عنها، بالتالي فإن هذه الدراسة سوف تقوم على المحددات التالية:

- سوف تركز الدراسة على موضوع الاختصاص الجغرافي في قانون الجرائم الإلكترونية.
- سوف يتم إجراء المقارنة بين تشريعات كل من الأردن وقطر وإنجلترا بشكل رئيس، مع التعرض أحيانًا للتشريعات الأخرى عند اللزوم.
- سوف يتم دراسة الأحكام القضائية في هذه الدول للوصول إلى النهج القضائي فيها للتعامل مع مشكلة الاختصاص.
- سوف تحاول الدراسة اقتراح الآليات والأدوات التشريعية اللازمة للتعامل مع هذا الطارئ.

منهجية الدراسة

تعتمد الدراسة، في سبيل وصولها لأفضل النتائج، على العديد من المناهج والأدوات الدراسية البحثية، حيث سيتم اللجوء للمنهج الوصفي لوصف واقع التشريعات والتطبيقات القضائية في دول المقارنة، ثم المنهج التحليلي لتحليل هذا الواقع، والوقوف على ما وراء النصوص وما خلف السطور، ثم المنهج المقارن للمقارنة بين هذه الأنظمة القانونية، وأخيرًا المنهج الكامل لوضع النتائج والتوصيات.

هيكل الدراسة

تتكون الدراسة من ثلاثة مباحث يتبعها خاتمة وكما يلي:

المبحث الأول: الجهود الدولية لحل مشكلة الاختصاص القضائي في الجرائم الإلكترونية.

المبحث الثاني: قواعد الاختصاص القضائي في التشريعات الوطنية ومدى شمولها للجرائم الإلكترونية.

المبحث الثالث: البعد الوطني والدولي لحل مشكلة الاختصاص القضائي للجرائم الإلكترونية، الواقع والمأمول.

المبحث الأول

الجهود الدولية لحل مشكلة الاختصاص القضائي في الجرائم الإلكترونية

سوف نتناول في هذا المبحث الجهود الدولية لحل مشكلة الاختصاص القضائي في الجرائم الإلكترونية، نتناول جهود المنظمة الدولية وجهود المنظمات الإقليمية، ثم نعرج على جهود المنظمات غير الحكومية.

أولًا: الجهود الدولية على مستوى الأمم المتحدة

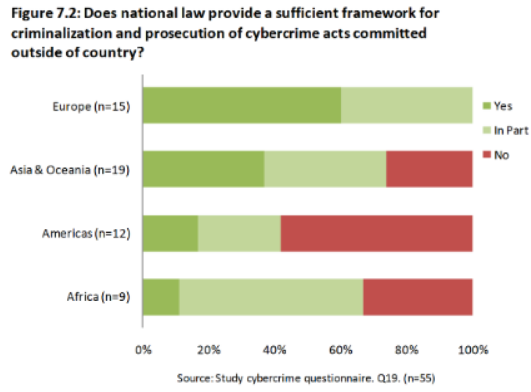
حقيقة الأمر أن هناك جهودًا كبيرة ومتنوعة تم بذلها من منظمة الأمم المتحدة وهيئاتها المختلفة؛ لمواجهة المستجدات الحديثة المتعلقة بالجرائم الإلكترونية. من ضمن هذه المواضيع موضوع الاختصاص، وطريقة امتداد الاختصاص الوطني خارج الدول؛ لضمان عدم إفلات مرتكبي هذا النوع من الجرائم من العقاب.

فقد لخص وزير خارجية الهند **للاتصالات** ونظم المعلومات خطر الجرائم الإلكترونية ومشكلة عبورها لحدود الدول، بمقولة شهيرة له في قمة الجرائم الإلكترونية (cybersecurity summit) التي عقدت في الهند عام 2012 بقوله: «لم يعد السؤال المطروح حول كيفية قيام الدول بحماية أمنها، بل أصبح السؤال عن كيفية قيام العالم بحماية نفسه».[15]

15. www.rebootrage.com.

قد شعر الجميع بخطورة هذه المشكلة حينها، **وتشكلت** فرق في معظم دول العالم لإيجاد الحلول لهذا الموضوع، الذي قد يشكل خطرًا داهمًا على جميع دول العالم إذا لم يتم وضع الحلول الناجعة له.

كان مكتب الأمم المتحدة لمكافحة المخدرات والجريمة (UNODC) أول المستجيبين لذلك، حيث تم تشكيل لجنة لإعداد دراسة شاملة لحل هذا الموضوع. سلمت اللجنة دراستها عام 2013 بعد إجراء العديد من الاستبانات، وتجميع البيانات من 69 دولة من مختلف القارات.[16]



تم خلال هذه الدراسة طرح سؤال على هذه الدول حول مدى رضاهم عن التشريعات الوطنية التي تنظم موضوع الاختصاص في الجرائم الإلكترونية، ومدى كفاية هذه التشريعات لملاحقة مرتكبي هذه الجرائم وضمان عدم إفلاتهم من العقاب، في حال تم ارتكابها من خارج إقليم الدولة.

توصلت الدراسة – وكما هو موضح في الشكل البياني جانبًا – أن حوالي ثلث الدول أبدت حاجتها إلى مزيد من امتداد الاختصاص في تشريعاتها لتطال هؤلاء المجرمين كي تكون هذه التشريعات مُرضية (sufficient)، حوالي 40% منها أبدى رضىً جزئيًا حول تشريعاتهم (sufficient in part)، و25% أجابوا بأنها غير كافية أو مُرضية (not sufficient).

أجمعت هذه الدول على أن تشريعاتها غير كافية، وعَزَت ذلك إلى القصور في هذه التشريعات، وعدم وجود قواعد الاختصاص الكافية، أو غيابها كليًا في معرض التعامل مع الجرائم التي يتسبب بها مجرمون من خارج الدولة، خاصة أن مثل هذه الجرائم لا تقتصر ملاحقتها على التشريعات الموجودة في كل دولة بشكل مستقل، بل لا بد أن تتضمن تشريعات الدول المتأثرة بالجريمة جميعها من القواعد؛ ما يسد أي ثغرة تتعلق بالملاحقة، وهذا يشكل تحديًا كبيرًا أمام التشريعات الوطنية كافة.

على الصعيد الدولي، اقترح الاتحاد العالمي للاتصالات (The International Telecommunications Union) (ITU) في المؤتمر الدولي للتكنولوجيا والمعلومات الذي عُقد في شهر ديسمبر في دبي عام 2012 ضرورة إجراء تعديلات جوهرية على لوائح وتشريعات الاتحاد والتي تم اعتمادها بموجب اتفاقية دولية عام 1988.في هذا المؤتمر وافقت 89 دولة على إعطاء الاتحاد كافة الصلاحيات المتعلقة بتقنية المعلومات وبالمقابل فقد رفضت 55 دولة هذا الاقتراح. تم متابعة هذا الموضوع في المؤتمر التالي الذي عقد في بوسان، في كوريا الجنوبية في أكتوبر 2014، حيث أثار الاتحاد موضوع الفضاء الإلكتروني والإنترنت وضرورة وجود تنظيم دولي يحكم التشريعات الوطنية ويصبح مرجعًا لها، إلا أن الاتفاق على ذلك لم يتم، حيث أبدت ما يقارب 40 دولة رغبتها بالسيطرة على ما يستطيع الأفراد تصفحه، وكان ذلك إما لأسباب سياسية أو دينية، بل زاد على ذلك أن طالب عدد من الدول بالسماح لهم بحجب بعض مواقع التواصل الاجتماعي مثل فيس بوك (Facebook) وتويتر (Twitter) ويوتيوب (YouTube).[17]

16. *Comprehensive study on Cybercrime*, UNODC, Vienna, February 2013, & 190.

17. يمكن الاطلاع على كافة هذه الوثائق والتعليمات على موقع الاتحاد العالمي للاتصالات على الرابط التالي: www.itu.int/en/Pages/.

ثانيًا: الجهود الدولية على مستوى المنظمات الإقليمية

تنبّه كل من الاتحاد الأوروبي والدول الأوروبية والولايات المتحدة الأمريكية لهذا الموضوع، وكان من أهم توصيات القمة الأوروبية الأمريكية لتكنولوجيا المعلومات التي عُقدت عام 2010 تشكيل فريق عملٍ مشتركٍ (A Working Group on Cybersecurity and Cybercrime)، ومن أهم ما جاء به ضرورة اعتماد اتفاقية بودابست كأساس لهذه الدول في وضع تشريعاتها الداخلية، والاتفاق على التعاون في التحقيق وتسليم المجرمين. لم تقم كل من روسيا والصين باعتماد هذه الاتفاقية، وكان رأيهما حيال ذلك، ضرورة وجود اتفاقية دولية تحت مظلة الأمم المتحدة، وأكدت روسيا هذا الأمر مرة أخرى عام 2013 في القمة العالمية لمكافحة الجرائم الإلكترونية.[18]

قامت دول الكومونولث عام 2011 بتأسيس فريق عمل مشترك لمكافحة الجرائم الإلكترونية، أنهى هذا الفريق عمله في شهر مايو 2013 وسلم تقريره في اجتماع وزراء القانون في هذه الدول عام 2014.[19] تمت تلاوة التقرير في ذلك الاجتماع وكان يتألف من أجزاء ثلاثة؛ الجزء الأول: تناول طبيعة الجريمة الإلكترونية والتحديات التي تحملها في طياتها، الجزء الثاني: يركز على موضوع التعاون بين الدول الأعضاء في مجال مكافحة الجرائم الإلكترونية، أما الجزءُ الثالث: يتناول موضوع التدريب ووضع استراتيجية تدريب متكاملة لتنفيذها من قبل جميع الدول الأعضاء والهيئات الوطنية المنخرطة في هذا المضمار. صادق جميع الوزراء على مخرجات فريق العمل.[20]

ثالثًا: الجهود الدولية على مستوى المنظمات غير الحكومية

يُعتبر معهد الشرق والغرب (East West Institute) (EWI)، الذي تأسس عام 2010، من أكثر المنظمات غير الحكومية نشاطًا في مضمار الجرائم الإلكترونية. لقد أثار مشكلة الاختصاص والتحقيق والتعاون الدولي في معظم المؤتمرات العالمية لتقنية المعلومات، وهو يعكف حاليًا، وعلى لسان مديره القاضي النرويجي (Stein Schjolberg) على إعداد مسودات لاتفاقية دولية شاملة للجرائم الإلكترونية؛ تُقدِّم حلًا لكل ما يثيره هذا الموضوع من مشاكل ومعاضل قانونية وفنية.[21]

المبحث الثاني

قواعد الاختصاص القضائي في التشريعات الوطنية ومدى شمولها للجرائم الإلكترونية

نتناول في هذا المبحث قواعد الاختصاص في التشريعات القطرية والأردنية، وفي قانون إساءة استخدام الحاسوب الإنجليزي، للوقوف على كيفية تعامل هذه التشريعات مع موضوع الاختصاص في الجرائم الإلكترونية، ومدى شمول أحكامها لكافة جزئيات ومستجدات هذا النوع من الجرائم.

المطلب الأول

قواعد الاختصاص القضائي في التشريعات القطرية ومدى شمولها للجرائم الإلكترونية

لا يوجد في قانون الجرائم الإلكترونية القطري رقم 14 لسنة 2014 أية أحكام تتعلق بتنظيم الاختصاص في هذا النوع من الجرائم، لذلك كان لا بد من العودة للأحكام العامة الواردة في قانون العقوبات، وكأن القانون اعتبر أنه لا يوجد ما يميز هذه الجرائم عن الجرائم العادية في موضوع الاختصاص، وهو أمر مثار نقاش سوف نقف عليه، ونرى مدى صحته.

تناول قانون العقوبات القطري موضوع الاختصاص تحت عنوان سريان النص الجزائي من حيث المكان في الباب الثاني من الكتاب الأول في المواد 13 حتى 20. الرجوع إلى أحكام هذه المواد لرؤية مدى انطباقها على الجرائم الإلكترونية نجد أن

18. Stein Schjolberg, *History of Cybercrime*: 1976-2014, Volume 9, Cybercrime Research Institute GmbH, & 77, 2014.

19. عُقد هذا الاجتماع في جابورون (Gaborone)، بتسوانا (Botswana)، 5-8 مايو 2014.

20. للاطلاع على جميع وثائق هذا المؤتمر يمكن زيارة موقع منظمة الكومونولث على هذا الرابط: www.thecommonwealth.org.

21. للاطلاع على مجهودات المعهد يمكن زيارة موقعه على الرابط التالي: www.eastwest.ngo.

القانون اعتمد أربعة مبادئ رئيسة في موضوع الاختصاص القضائي. سنتناول ذلك بإيجاز وفقًا لمقتضيات الدراسة، ولمعرفة مدى كفاية أحكامها للتعامل مع الجرائم الإلكترونية وهي:[22]

أولًا: مبدأ الصلاحية الإقليمية يقوم هذا المبدأ على أساس أن القانون الوطني يسري على كافة الجرائم التي ترتكب في الإقليم[23]. ولتحديد مكان وقوع الجريمة؛ اختلف الفقه بين اتجاهات ثلاثة[24]؛ ذهب الاتجاه الأول إلى أن العبرة في تحديد مكان وقوع الجريمة تكمن بالمكان الذي وقع فيه السلوك، بِغَض النظر عن المكان الذي تحققت فيه النتيجة، أو الذي كان يفترض أن تتحقق فيه. ذهب الاتجاه الثاني إلى أن مكان وقوع الجريمة يتحدد بالمكان الذي تحققت فيه النتيجة، أو كان من المفترض تحققها فيه. بين هذا وذاك؛ رأى الاتجاه الثالث أن العبرة في ذلك تكمن بمكان حصول أي منهما؛ السلوك أو النتيجة. لكل مذهب من هذه المذاهب مبرراته وأسانيده التي تعززه وتدعمه.[25] أما قانون العقوبات القطري فقد ذهب مذهبًا مختلطًا، ودمج بين مذهب مكان السلوك الإجرامي، ومذهب مكان وقوع الجريمة.

خلاصة الأمر أننا لم نجد في هذا المبدأ ما يضع نصوصًا خاصة للجرائم الإلكترونية. توسع قانون العقوبات القطري في الاختصاص الإقليمي، حيث امتد بسلطانه القضائي ليشمل أية جريمة، سواء أوقعت بكاملها داخل حدود الدولة، أم وقع أي عنصر من عناصرها في إقليم الدولة، يستوي في ذلك، الفعل والنتيجة. ذهب القانون العقابي القطري لأبعد من ذلك حينما شمل باختصاصه المكاني الجرائم التي كان يُراد أن تقع نتيجتها داخل إقليم الدولة، وهذا توسع يثير العديد من التساؤلات، فهو يشمل نتائج لم تتحقق أصلًا، وقد تكون ما زالت في مرحلة الإعداد والتفكير التي لا يُحاسب عليها القانون، أو أن الجريمة ما زالت في مرحلة الشروع ولم تتحقق النتيجة لأي سبب كان؛ على الرغم من ذلك فهو مذهب محمود إذ أنه يضفي توسعًا احتياطيًا لسلطان قانون العقوبات لا ضير فيه.[26]

تطبيقًا لذلك، فإن قانون العقوبات القطري يسري على كل من يرتكب جريمة إلكترونية في الحالات التالية:

- إذا كان الموقع الإلكتروني المُخترَق قطريًا وتم فعل الاختراق في الإقليم القطري.
- إذا كان الموقع الإلكتروني المُخترَق غير قطري ولكن فعل الاختراق تم في قطر.
- إذا اشترك عدة أشخاص باختراق موقع إلكتروني، سواء أكان قطريًا أم غير قطري، مادام أحد المشتركين قام بالفعل على الإقليم القطري، ومهما كان نوع الاشتراك.
- قام شخص أو عدة أشخاص بارتكاب جريمة الشروع باختراق موقع إلكتروني قطري فإن قانون العقوبات القطري يسري عليهم، سواء أتم الفعل أم لم يتم.

ثانيًا: مبدأ الصلاحية الذاتية أو العينية

يعتبر هذا المبدأ امتدادًا لمبدأ إقليمية القانون الجزائي، يمتد تطبيق القانون الجزائي للدولة إلى خارج إقليمها في حال

22. انظر في ذلك تفصيلًا: أشرف توفيق شمس الدين، **شرح قانون العقوبات القطري**، (الطبعة الأولى، جامعة قطر، 2010، ص. 194 وما بعدها) القسم العام، النظرية العامة للجريمة والعقوبة.

23. وكان هذا واضحًا في المادة 13 من قانون العقوبات القطري.

24. موسى مسعود أرحومة، **الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية**، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 28-29/ 10/2009، ص. 17.

25. انظر تفصيلًا: كمال أنور محمد القاضي، **تطبيق قانون العقوبات من حيث المكان**، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 22 إبريل 1965، ص. 90 وما بعدها.

26. انظر في ذلك حكم محكمة التمييز القطرية رقم 402 لسنة 2014 قضائية بتاريخ 4 مايو 2015 وجاء فيها ما يلي: «ولما كان واقع الحال في الدعوى الماثلة أن الطاعن غير قطري قصد من الحصول على الشهادة الجامعية – موضوع التزوير – إيجاد فرصة عمل له داخل قطر؛ مما حدا به إلى تقديمها إلى قسم التصديقات بوزارة الخارجية القطرية لاعتمادها تحقيقًا لمقصده هذا وإن لم تتحقق نتيجة فعله داخل قطر؛ إلا أنه يُؤْذِن بامتداد ولاية القضاء القطري على واقعة التزوير المرتكبة خارج قطر، ما دام أن الطاعن كان يريد أن تتحقق نتيجة فعله داخلها».

ارتكاب جرائم معينة بالذات تمس مصالحها الأساسية، وفقا لقانونها الداخلي، أيا كانت جنسية مرتكبها ومكان ارتكابها.[27] هذه المجموعة من الجرائم التي اختارها المشرع القطري واعتبرها من الجرائم ذات الأثر الكبير على أمن الدولة وسلامتها ومصالحها العليا – وردت على سبيل الحصر – فلا يجوز التوسع فيها ولا القياس عليها. كما يُلاحَظ أن المشرع اعتبر تجريمها وطنيًا كافيًا لملاحقة كل من يساهم فيها، سواء أكانت المساهمة أصلية أم تبعية، دون النظر لمحل التجريم في الدول الأخرى التي وقعت فيها الجريمة، ودون النظر كذلك لجنسية مرتكبها.

بالاطلاع على هذه الجرائم فإننا لا نجد من بينها الجرائم الإلكترونية، وبالتالي فإن هذه الجرائم لا تلاحق سندًا لمبدأ الصلاحية الذاتية أو العينية. حتى لو تصورنا أنه تم ارتكاب إحدى هذه الجرائم عن طريق اختراق موقع إلكتروني، فارتكبت جريمة من جرائم أمن الدولة مثلًا عن طريق اختراق موقع إلكتروني فإن هذا الاختراق يصبح عنصرًا من عناصر الجريمة الأصلية ولا يعتبر جريمة مستقلة بذاته، ذلك أن جريمة أمن الدولة ما كانت لتتم لولا هذا الاختراق الذي وقع لذلك الموقع الإلكتروني.

ما تراه الدراسة أن على المشرع في قطر إعادة النظر بهذه المادة لشمول الجرائم الإلكترونية المهمة والحساسة في الدولة، سواء أكانت تلك المواقع تتعلق بمصالح الدولة العليا السياسية أم الاقتصادية، حيث أن مثل هذه الجرائم لا تقل أهمية عن الجرائم التي وردت في المادتين السابقتين، والأمثلة الكثيرة التي تم ذكرها سابقًا في هذه الدراسة دليل على ذلك.

ثالثًا: مبدأ الصلاحية الشخصية

يقوم هذا المبدأ على أساس رابطة الجنسية التي تربط الفرد بدولته أينما وجد، مبررًا ذلك بأن مصلحة الدولة وحسن سمعتها يقتضيان ألا يرتكب أفرادها جرائم خطيرة في الخارج؛ إذ إن مثل هذا الأمر يسيء لمركزها بين الدول، فلولا هذا المبدأ لتعذر معاقبة من استطاع الهرب والعودة إلى وطنه بعد أن قارف الجريمة.

تم النص على هذا المبدأ في المادة 16 من قانون العقوبات القطري، التي اشترطت أن يكون الفعل معاقبًا عليه بمقتضى قانون البلد الذي أرتكب فيه، في حين لم يشترط قانون العقوبات الأردني هذا الشرط، واكتفى بأن الفعل معاقب عليه وفقًا لأحكامه. أي أن القانون الأردني يلاحق مواطنه في أي مكان وجد خارج إقليم الدولة، كما سنرى في المطلب الثاني من هذا المبحث.

تطبيقًا لشمول هذا المبدأ الجريمة الإلكترونية، فإننا نجد أن هذه الجرائم جميعها من نوع الجناية أو الجنحة، وبالتالي فإن مرتكبها؛ إذا كان يحمل جنسية الدولة، سيعاقب على هذا الفعل إذا رجع لدولته.

رابعًا: مبدأ الصلاحية العالمية الشاملة

يهيئ هذا المبدأ لأحكام قانون العقوبات نطاقًا واسعًا يشمل العالم بأكمله، وقد أستند الشارع في إقراره لذلك إلى فكرة التضامن الدولي في مكافحة الإجرام في الحالات التي لا يحاكم فيها المجرم أمام قاضي الاختصاص الطبيعي. في الواقع أن التأكيد على هذا المبدأ أصبح ضرورة قصوى اقتضاها استئصال آفة الإجرام الذي استفحل بعد أن ضربت البشرية بسهم وافر من التقدم والحضارة، وبعد أن مكنت سهولة المواصلات من في نفوسهم مرض، من تشكيل عصابات دولية تتجاوز جرائمهم نطاقًا دوليًا واحدًا. يتعين على هذه الدول أن تتعاون فيما بينها وأن تنهض بمسؤولياتها، فتضطلع كل دولة بمعاقبة الجاني الأجنبي الذي يقبض عليه على أراضيها؛ نيابة عن الدولة التي وقعت الجريمة في إقليمها إن تعذرت

27. انظر في ذلك: إبراهيم بشارة عواد السويلمين، **جريمة الاحتيال عبر شبكة المعلومات الدولية**، دراسة مقارنة بين القانون الأردني والقانون المصري، رسالة دكتوراه، جامعة عمان العربية للدراسات العليا، 2010، ص. 111. عبد الأحد جمال الدين، وجميل الصغير، **المبادئ الرئيسية في القانون الجنائي**، القسم العام، دار النهضة العربية للنشر والتوزيع، القاهرة، 1999، ص. 193 .

مقاضاته أمام قضاء تلك الدولة. هو إذًا اختصاص احتياطي أو ثانوي لا يمارس إلا إذا تعذر أن يمارس حيال المجرم الاختصاص الإقليمي أو العيني أو الشخصي. لكل من هذه الاختصاصات الثلاثة حق الأفضلية، أما وقد تعذر ممارسة أي منها؛ فلا سبيل للحيلولة دون إفلات الجاني من العقاب إلا إخضاعه إلى قانون الدولة التي قبضت عليه استنادًا إلى مبدأ الصلاحية الشاملة.[28]

عليه، يخطئ من يظن أن أمن أي دولة وسلامتها هو بمعزل عن باقي دول العالم. العصر الحديث والتكنولوجيا الحديثة وما رافقهما من تطور وتسارع وتقريب للمسافات، حتى كادت تكون وهمية، سهلت على الجناة ارتكاب الجريمة في أي مكان من العالم؛ لذلك فإن مبدأ الصلاحية العالمية يأتي مكملًا لباقي المبادئ، كدور شديد الأهمية.

تم النص على هذا المبدأ في المادة 17 من قانون العقوبات القطري، وفقًا لذلك؛ فإن شروط ممارسة هذا الاختصاص تتلخص بما يلي: أن يكون الفاعل أجنبيًا، وأن تكون الجريمة من الجرائم المحددة في المادة السابقة، ولا يدخل ضمن ذلك بطبيعة الحال جرم اختراق المواقع الإلكترونية، وأخيرًا شرط التواجد في الدولة.

لم يشترط القانون القطري سوى التواجد على إقليم الدولة بأي صفة كانت، وكان موفقًا في ذلك. إذ إن مجرد وجود الجاني على أرض الدولة، يعطي الدولة السلطان والنفوذ ببسط صلاحياتها عليه، حتى ولو كان وجودًا عرضيًا أو سريعًا؛ كما أن شرط الإقامة لا يتفق وروح مبدأ الصلاحية العالمية والغاية المنشودة منه، فكيف يتم إطلاق سراح شخص متهم بجناية أو جنحة لمجرد عدم تحقق شرط الإقامة؟ مثل ما سلكته بعض التشريعات: التشريع الأردني مثلًا كما سنرى في المطلب اللاحق.

يشار هنا إلى أن المشرع القطري اقتصر على عدد معين من الجرائم التي ارتأى أنها تتعلق بالأمن العالمي، والتي أوردها – على سبيل الحصر – مما يعني عدم جواز القياس عليها ولا الاجتهاد فيها. حبذا لو تُرك هذا الموضوع للقضاء واكتفى المشرع بالنص على أسسٍ عامةٍ للتطبيق.

المطلب الثاني

قواعد الاختصاص القضائي في التشريعات الأردنية ومدى شمولها للجرائم الإلكترونية

استشعر المشرع الأردني خطورة العالم الافتراضي الذي تُرتكب فيه الجرائم الإلكترونية، واحتمالية إفلات المجرمين من العقاب. فانتقل من مرحلة الأحكام العامة الواردة في قانون العقوبات رقم 16 لسنة 1960، بإضافة فقرة رابعة للمادة الخامسة من قانون أصول المحاكمات الجزائية رقم 9 لسنة 2006[29]، وبعد ذلك وضع مادة كاملة نظّم بموجبها هذا الاختصاص في قانون الجرائم الإلكترونية رقم 27 لسنة 2015.

سندًا للأحكام العامة، فقد تناول قانون العقوبات الأردني أحكام الاختصاص القضائي في المواد 7 حتى 11 من قانون العقوبات تحت عنوان «الأحكام الجزائية من حيث المكان»، أما الفقرة الرابعة من المادة الخامسة من قانون أصول المحاكمات الجزائية فقد جاء فيها ما يلي: «يجوز إقامة دعوى الحق العام على المشتكى عليه أمام القضاء الأردني؛ إذا ارْتُكِبت الجريمة بوسائلَ إلكترونيةٍ خارج المملكة وترتبت آثارها فيها – كليًا أو جزئيًا – أو على أي من مواطنيها»، وجاء في المادة 17 من قانون الجرائم الإلكترونية ما نصه: «تُقام دعوى الحق العام والحق الشخصي على المشتكى عليه أمام المحاكم الأردنية إذا ارتُكِبت أي من الجرائم المنصوص عليها في هذا القانون؛ باستخدام أنظمة معلومات داخل المملكة أو

28. أسعد محمد أحمد الغرايبة، **تنازع الاختصاص في المسائل الجزائية**، دراسة مقارنة، رسالة دكتوراه، جامعة عمان العربية للدراسات العليا، 2012، ص. 61.

29. تم إضافة هذه الفقرة بموجب التعديل الذي تم على قانون أُصول المحاكمات الجزائية بتاريخ 16مارس 2006 بواسطة المادة الثانية من قانون رقم 15 لسنة 2006؛ بشأن القانون المعدل لقانون أصول المحاكمات الجزائية.

ألحقت أضرارًا بأي من مصالحها أو بأحد المقيمين فيها أو ترتبت آثار الجريمة فيها، – كليًا أو جزئيًا – أو ارتكبت من أحد الأشخاص المقيمين فيها».

من ناحية الصياغة التشريعية فإن الدراسة ترى أن المشرع الأردني استخدم في المادة الخامسة تعبير «الوسائل الإلكترونية»، وكان ذلك عام 2006، وبعد أن صدر قانون جرائم أنظمة المعلومات رقم 30 لسنة 2010 استعمل تسمية «أنظمة المعلومات»، ثم عاد عام 2015 واستعمل مصطلح "الجرائم الإلكترونية" وفقًا لقانون عام 2015، ولكنه وفي المادة 17 من القانون ذاته؛ عاد وأطلق عليها تسمية «أنظمة المعلومات»، مما يشكل نوعًا من التخبط لا بد من إزالته بهدف توحيد المسميات والمفاهيم.[30] سوف نتناول هذا المطلب في فرعين؛ نخصص الفرع الأول للأحكام العامة للاختصاص في الجرائم الإلكترونية في الأردن ومدى انطباقها على الجرائم الإلكترونية، ونخصص الفرع الثاني لأحكام الاختصاص الخاصة بالجرائم الإلكترونية في التشريعات الأردنية.

الفرع الأول: الأحكام العامة للاختصاص في التشريعات الأردنية ومدى انطباقها على الجرائم الإلكترونية

سوف نتناول بإيجاز، وفقًا لأغراض الدراسة، الأحكام العامة للاختصاص في قانون العقوبات الأردني، ومدى انطباق هذه الأحكام على الجرائم الإلكترونية، حيث إن قانون العقوبات الأردني حدد أربعة مبادئ للاختصاص كما يلي:

1. **الصلاحية الإقليمية**: الربط بين الاختصاص ومكان ارتكاب الجريمة[31]؛ امتد سلطان الدولة القضائي ليشمل أية جريمة تُرتكب على الإقليم الأردني، سواء أوقعت بكاملها داخل حدود الدولة، أم وقع أي عنصر من عناصرها في إقليمها، سواء الفعل أم النتيجة[32]،لكن المشرع الأردني لا يعتبر الجريمة في الإقليم الأردني إلا إذا وقعت النتيجة فعلًا، أما إذا لم تقع لأي سبب فلا تعتبر واقعة فيه حتى وإن تبين بأن الجاني توقع حصولها فيه، نعني بذلك حالة الشروع التي يرتكب الجاني فيها فعله خارج الإقليم، ويتوقع وقوع النتيجة الجرمية في الإقليم إلا أنها لم تتحقق؛ أي أن المشرع الأردني يعتبر قانون العقوبات واجب التطبيق إذا أُرتكب في الإقليم الأردني أحد العناصر التي تؤلف الركن المادي للجريمة، سواء أكان النشاط الجرمي أم النتيجة أم علاقة السببية بينهما[33]، وسواء أوقعت النتيجة والضرر أم كانت الجريمة شكلية وكان هناك خطر

30. أطلق عليها المشرع السعودي «الجرائم المعلوماتية»، والمشرع القطري «الجرائم الإلكترونية»، وهناك من أطلق عليها «جرائم تقنية المعلومات» كما فعل القانون العماني، والقانون الإماراتي. أما على المستوى الدولي فقد أطلق عليها المشرع البلجيكي «جرائم الكمبيوتر»، وكذلك فعل المشرع الإنجليزي، والمشرع الياباني، والمشرع الفرنسي، والعديد من الولايات في الولايات المتحدة الأمريكية. أما المشرع البلغاري فأطلق عليها «جرائم العالم الافتراضي»، وكذلك فعل المشرع الكندي، والمشرع الألماني، والمشرع الهنغاري، والمشرع الإيطالي. أما المشرع الدنماركي فأطلق عليها «جرائم تكنولوجيا المعلومات»، وكذلك فعل المشرع الهندي. انظر في ذلك: أنور محمد صدقي مساعدة، **اضاءات وتأملات في قانون الجرائم الإلكترونية القطري الجديد الصادر بالقانون رقم 14 لسنة 2014**، العدد الثاني مجلة مركز الدراسات القانونية والقضائية، وزارة العدل، قطر (السنة الثامنة 2016)، ص. 305؛ أنور محمد صدقي مساعدة، **مدى كفاية أحكام التجريم الإلكتروني في قانون الجرائم الإلكترونية الأردني الجديد رقم 27 لسنة 2015**، العدد 74، السنة 32، رجب 1439 هـ، إبريل 2018، مجلة الشريعة والقانون، جامعة الإمارات، الإمارات العربية المتحدة ص. 455.
New German Laws on Cybercrime: www.securityfocus.com. The World Information Technology and Services Alliance: www.witsa.org. National Belgium Information Technology Center: www.nitc.gov. National English Information Technology Center: www.nitc.gov.np. Science links japan website: http://sciencelinks.jp/j-east. Website of Athabasca University: www.athabascau.ca/policy/computingservices. James M. Thomas, *The Computer Fraud and Abuse Act: A Powerful Weapon vs. Unfair Competitors and Disgruntled Employees*, In-House Defense Quarterly, Chicago, 2007, &1.

31. وكان ذلك في المادة السابعة من قانون العقوبات الأردني.

32. انظر تفصيلًا: كامل السعيد، **شرح الأحكام العامة في قانون العقوبات الأردني**، دراسة مقارنة، المركز العربي للخدمات الطلابية، عمان، 1998، ص. 100-101. نظام المجالي، شرح قانون العقوبات، القسم العام، دار الثقافة، عمان، 2009، ص. 114.

33. انظر في ذلك حكم محكمة التمييز الأردنية بهيئتها الخماسية رقم 2000/258، تاريخ 2000/4/19 إذ جاء فيه ما يلي: «حيث إن جرم التصدير والاستيراد للمادة المخدرة التي يحاكم المميِّز وآخرون عليها؛ هو من الجرائم غير المتجزئة، وحيث إن المميز أُلقي القبض عليه في الأردن وضبط معه مبلغ عشرة آلاف دولار ثمن المادة المخدرة التي ضبطت في الأردن فيكون ما تم على الأرض الأردنية أحد العناصر التي تمت عليها والتي تؤلف الجريمة. وعليه تكون المحاكم الأردنية صاحبة صلاحية إقليمية بنظر الجرم المسند للمميز».

من وقوع الضرر[34]، وذلك على خلاف المقرر في القانون القطري، وبعض التشريعات العربية الأخرى التي تمتد بسلطانها لتشمل جرائم الشروع التي يتم بها الفعل خارج الإقليم، ولا تتحقق النتيجة داخله.[35]

2. **الصلاحية الذاتية أو العينية:** تبنّى المشرع الأردني هذا المبدأ في المادة التاسعة من قانون العقوبات الأردني، وبالاطلاع على هذه الجرائم فإننا لا نجد من بينها الجرائم الإلكترونية؛ بالتالي فإن هذه الجرائم لا تُلاحَق، سندًا لمبدأ الصلاحية الذاتية أو العينية.

3. **الصلاحية الشخصية:** تم النص على هذا المبدأ في المادة العاشرة من قانون العقوبات الأردني، من الملاحظ أن قانون العقوبات الأردني لم يشترط ازدواجية التجريم – كما هو الحال في القانون القطري – بل اكتفى بأن يؤلف الفعل جريمة وفقًا لأحكامه. بالتالي فإن قانون العقوبات الأردني كان أكثر شمولًا حين امتد بالاختصاص لكافة الأفعال المُجَرَّمة بموجبه، ذلك أنه قد يحدث أن تكون هناك أفعال غير مُجَرَّمة في تشريعات أخرى وبالتالي فإن مقترفها سينجو من العقاب وفقًا لتلك الأحكام، ولكنه لن ينجو بفعلته وفقًا لقانون العقوبات الأردني، وسيلاحق على هذه الفعلة حتى لو تم محاكمته غيابيًا.

الجرائم الإلكترونية، وفقًا لقانونها في الأردن، من نوع الجناية أو الجنحة، وبالتالي فإن مرتكبها إذا كان ممن يحمل الجنسية الأردنية سيعاقب على هذا الفعل حين عودته.[36]

4. **الصلاحية العالمية الشاملة:** تم النص على هذا المبدأ في الفقرة الرابعة من المادة العاشرة. سندًا لهذه المادة فإن شروط ممارسة هذا الاختصاص تتلخص في ما يلي؛ أن يكون الجاني أجنبيًا، أن يكون الفعل من نوع الجناية أو الجنحة أيًا كان طبيعة هذا الفعل، ويدخل ضمن ذلك بطبيعة الحال جرم اختراق المواقع الإلكترونية؛ شرط الإقامة؛ أي أن يكون الجاني مقيمًا في الأردن، والإقامة بطبيعة الحال تختلف عن مجرد الدخول، أو التواجد أو المرور، وألا يكون هناك طلب لتسليم هذا الجاني أو تم قبوله.[37]

من الملاحظ أن القانون الأردني اشترط شرط الإقامة في الدولة على عكس القانون القطري الذي لم يشترط سوى التواجد على إقليم الدولة بأي صفة كانت. ما نراه أن المشرع القطري كان أكثر توفيقًا، إذ إن مجرد وجود الجاني على أرض الدولة، يعطي الدولة السلطان والنفوذ ببسط صلاحياتها عليه، ولو كان وجودًا عرضيًا أو سريعًا، كما أن شرط الإقامة لا يتفق وروح مبدأ الصلاحية العالمية والغاية المنشودة منه. إذ كيف يتم إطلاق سراح شخص متهم بجناية أو جنحة لمجرد عدم تحقق شرط الإقامة في الدولة، وهو ما جرت عليه أحكام محكمة التمييز الأردنية تطبيقًا لهذا النص.[38]

---

34. انظر في ذلك حكم محكمة التمييز الأردنية: قرار تمييز جزاء رقم 83/89 صفحة 1301 لسنة 1983 ورقم 85/69 صفحة 1270 سنة 1985 ورقم 80/152 لسنة 1981 رقم 152 لسنة 1988 وجاء فيه ما يلي: «في حال كون السند الرسمي المزور باطلًا فإن ذلك ليس مانعًا من معاقبة مقترف التزوير ما دام أن التزوير في الأسناد الرسمية قد تسبب في ضرر فعلي أو من المحتمل أن يتسبب بضرر».

35. انظر تفصيلًا: السعيد، مرجع سابق، ص. 100-101. نظام المجالي، مرجع سابق، ص. 114-115.

36. انظر في ذلك حكم محكمة التمييز الأردنية: الأحكام الجزائية، الطعن رقم 165 لسنة 2001 قضائية، ص. 2042، وجاء فيه ما يلي: «حيث إن الجريمة موضوع الدعوى هي جناية ارتكبت من أردني في الخارج وتعلقت بأمن الدولة الأردنية فإن محاكمته وفقًا لقانون العقوبات لا تخالف القانون».

37. انظر تطبيقًا لذلك حكم محكمة التمييز الأردنية: محكمة التمييز، الأحكام الجزائية، الطعن رقم 1427، لسنة 2007 قضائية وجاء فيه ما يلي: «يسري القانون الأردني على الأجانب المقيمين في المملكة والذين وقعت منهم جريمة التزوير في أوراق رسمية خارج المملكة ولم يطلب استردادهم، وذلك عملًا بالفقرة الرابعة من المادة العاشرة من قانون العقوبات لسنة 1960».

38. انظر تطبيقًا لذلك حكم محكمة التمييز الأردنية: الأحكام الجزائية، الطعن رقم 806 لسنة 1999 قضائية، بتاريخ 15 أبريل 2000 وجاء فيه ما يلي: «حيث يتبين من أوراق هذه القضية أن الجريمتين المسندتين للمتهم المميز قد ارتكبتا خارج المملكة، وأن المتهم المميز هو سوري الجنسية وهو غير مقيم في الأردن وقد قبض عليه في الأراضي الأردنية أثناء دخوله من الأراضي السعودية متوجهًا إلى بلده سورية فإن ما ينبني على ذلك كله؛ أن قانون العقوبات الأردني لا يسري على المتهم وبالتالي فإن المحاكم الأردنية غير مختصة بمحاكمته».

الفرع الثاني: قواعد الاختصاص الخاصة بالجرائم الإلكترونية في التشريعات الأردنية

توصلت الدراسة إلى أن النصوص التي نظمت موضوع الاختصاص في الجرائم الإلكترونية في الأردن اعتمدت مجموعة من المعايير وهي كما يلي:

أولًا: معيار الوسيلة أي وسيلة ارتكاب الجريمة، بأن أُفْرِدَ للجرائم الإلكترونية تنظيمٌ خاصٌّ بها إذا ما تمت بهذه الطريقة[39] وذلك في الحالات التالية:

1. **المادة 4/5 من قانون أصول المحاكمات الجزائية** لم تضف هذه المادة أي جديد لمفهوم الاختصاص في الجرائم الإلكترونية؛ حيث يمتد بموجبها السلطان المكاني للقانون إلى خارج حدود الإقليم، ويُطبق على الجرائم التي تتم خارج الإقليم الأردني، ولكن نتائجها وآثارها ترتبت داخله – سواء كليًا أو جزئيًا – هذا ليس بالأمر الجديد، إذ إن هذا موجود أصلًا بموجب مبدأ الصلاحية الإقليمية؛ سندًا للمادة السابعة السالفة الذكر، كل ما أضافته هذه المادة لمبدأ الصلاحية الإقليمية هو وسيلة ارتكاب الجريمة، في حين أنه من المسلمات أن قواعد الاختصاص لا تتأثر بوسيلة ارتكاب الجريمة، بل تتحدد بالتكييف القانوني للجريمة، أيًا كانت الوسيلة التي تمت بها؛ ولذلك فإن هذا التعديل، وحسب رأي الدراسة، لم يأتِ بأي جديد.
1. **المادة 17 من قانون الجرائم الإلكترونية:** امتد هذا القانون بالاختصاص، بشرط مفترض مفاده أن ارتكاب الجريمة يكون بوسيلة إلكترونية. جاءت هذه المادة بنصوص واسعة فضفاضة غير دقيقة، لا تتفق والسياسة التشريعية؛ خاصة في التشريعات الجزائية. بيان ذلك ما يلي:

أ- **«إذا ارتكبت الجريمة باستخدام أنظمة معلومات داخل المملكة»** حيث إن هذه الفقرة لم تبين وقوع النتيجة ومكان وقوعها، وفي تفسيرنا لذلك؛ فإن الدراسة ترى أن المشرع يَفترض أن مجرد وقوع الفعل داخل المملكة يكون كافيًا لتحريك دعوى الحق العام أمام محاكمها، سواء أتحققت النتيجة داخلها أم خارجها أم لم تتحقق البتة، وبقيت في مرحلة الشروع

ب- إذا **«ألحقت أضرارا بأي من مصالحها»** لم تحدد هذه الفقرة مكان هذه المصالح، أهو داخل المملكة أم خارجها، كما لم تحدد المقصود بالمصالح، وفي تفسيرنا لهذه الفقرة؛ فإننا نرى أن المشرع يقصد بذلك المصالح الأردنية خارج حدود المملكة، إذ لو قصد بذلك تلك المصالح الموجودة داخل حدودها لاكتفى بالشطر الأول من هذه الفقرة دون زيادة، هذا من ناحية؛ أما من الناحية الأخرى، فإن مفهوم المصالح مفهوم واسع فضفاض، وقد تعني الأماكن السيادية الأردنية من مبان وسفارات وهيئات، أو أنها المصالح السيادية الموضوعية، من مصالح اقتصادية وسياسية وغيرها، وفي ذلك توسع لا بد من ضبطه. وفي محاولة الدراسة الوقوف على المقصود بعبارة «مصالح» بغية ضبطها، وكون التشريعات تُشكل وحدة واحدة لا تتجزأ، وبالرجوع لأحكام قانون العقوبات الأردني؛ وجدنا أن هذه العبارة استخدمت للدلالة على المصالح العسكرية كما في الفقرة (ب) من المادة السابعة[40]، كما استخدمت في جرائم المتعهدين استخدامًا عامًا لتدل على كل ما يتعلق بالخدمات والمرافق الرئيسة والهامة في حياة المواطنين في الفقرة الأولى من المادة (133)[41]، واستخدمت في جرائم إساءة استعمال السلطة والإخلال بواجبات الوظيفة لتدل على كل ما يتعلق بمؤسسات الدولة المختلفة في الفقرة الثانية من المادة (183)[42]، واسْتُخدمت أخيرًا استخدامًا يتعلق بالحقوق الشخصية للأفراد ومصالحهم الخاصة، كما هو الحال في المادة (266)[43]،

39. عرف قانون الجرائم الإلكترونية الأردني «نظم المعلومات» في المادة الأولى منه، وجاء فيها ما يلي: «نظام المعلومات: مجموعة البرامج والأدوات المعدة لإنشاء البيانات أو المعلومات الكترونيا، أو إرسالها أو تسلمها أو معالجتها أو تخزينها أو إدارتها أو عرضها بالوسائل الإلكترونية».
40. جاء فيها: «إذا كانت الجريمة المقترفة تنال من سلامة الجيش أو من مصالحه».
41. جاء فيها: «أو تقديم خدمات تتعلق بالدفاع الوطني ومصالح الدولة العامة أو تموين الآهلين فيها».
42. جاء فيها: «إذا لحق ضرر بمصالح الدولة».
43. جاء فيها: «أو تلحق الضرر بمصالح أحد الناس».

وهذا كله للدلالة على شمول هذه المفردة لتتسع اتساعًا كبيرًا أحيانًا وتحمل في طياتها كل ما يتعلق بالدولة أحيانًا، وتضيق جدًا أحيانًا أخرى لتنحصر بمصالح الأفراد الخاصة؛ مما يعني تعذر ضبطها.

ج. «إذا ترتبت آثار الجريمة فيها كُليًا أو جزئيًا» قد يتبادر للذهن، لأول وهلة؛ أن هذه الفقرة تتناول النتيجة المترتبة على الجريمة، ولكن الحقيقة غير ذلك؛ فالنتيجة الجرمية تختلف عن آثار الجريمة، ولو أراد المشرع النتيجة لاستعمل العبارات التي وردت في المادة السابعة من قانون العقوبات عن عناصر الجريمة، ومن ناحية أخرى فإن نتيجة الجريمة قد تم تضمينها في الجزء الأول من هذه المادة، وبالتالي فإن المشرع يكرر نفسه وهذا من غير المتوقع، ومن هنا فإن هذه الحالة تركز على آثار الجريمة، والأثار – بطبيعة الحال – تختلف عن النتيجة الجرمية، فالنتيجة هي التغيير الذي يحصل في العالم الخارجي المحيط بشخص الفاعل بتأثير الفعل الذي ارتكبه، والتغيير النتيجة، والذي يعنى به قانون العقوبات ليس أي تغيير يحدث في العالم الخارجي كأثر للسلوك الجنائي، وإنما هو بالذات ذلك التغيير الذي يجعله قانون العقوبات محلًا للتجريم، فنتيجة جريمة القتل هي الوفاة، أما يترتب عليها من نتائج أخرى من أضرار مادية وأدبية فليس مما تُعنى به نصوص القتل، أما آثار الجريمة فهي التكلفة التي يتكبّدها الفرد والمجتمع من انتشار الجريمة، فالتكلفة ليست مادية فحسب، وإنما هي مجموعة من الآثار السلبية المدمرة على النواحي الإنسانية والاجتماعية لكافة فئات المجتمع.[44] وإذا أخذنا بهذا المفهوم فإن أي جريمة إلكترونية تحدث في أي مكان في العالم لا بد وأن تؤثر بشكل أو بآخر على الشبكة المعلوماتية، أو على اقتصاد البنوك أو المؤسسات أو التجارة الإلكترونية أو وسائل الإعلام أو الأسواق المالية أو سعر صرف العملات، وبالتالي فإن القانون الأردني يمتد باختصاصه ليطالها جميعها وفقًا لهذا المفهوم المتسع بشكل لا حدود له.

ثانيًا: المعيار الشخصي: اعتمد المشرع الأردني على معيار شخصي في بعض الحالات، وهو يختلف عن مبدأ الصلاحية الشخصية التي تُركز على الفاعل، بل ركز هنا على شخصية المجني عليه، وأحيانًا شخص الجاني وفقًا للحالات التالية:

1. **«إذا ارتكبت الجريمة على أي من مواطني الدولة»:** وذلك سندًا للمادة الخامسة من قانون أصول المحاكمات الجزائية، أي أن القانون الأردني يضفي حماية جزائية على كل مواطن أردني ارتكبت بحقه جريمة إلكترونية، أيًا كان مكان ارتكاب الجريمة، وأيًا كان مكان تواجد المواطن الأردني، وفي هذا توسع قد يكون القصد منه حماية المواطن من أي اعتداء إلكتروني في كل مكان على وجه البسيطة، الأمر الذي قد يضفي لمسة جمال ورعاية من الناحية النظرية، غير أنه قد يكون صعب التطبيق من الناحية العملية، وكان الأجدر بالقانون أن يضع المزيد من التفصيل في هذا المجال ليبين محدداته وضوابطه.
2. **«إذا ألحقت أضرارًا بأحد المقيمين فيها»:** سندًا للمادة 17 من قانون الجرائم الإلكترونية، وبطبيعة الحال فإن المجني عليه غير المضرور، فالأصل أن يكون المجني عليه هو الشخص المتضرر، إلا أنه ليس بالضرورة أن يتحد شخص المجني عليه بشخص المتضرر بصورة دائمة[45]، وليس من المتصور أو المنطق أن يضفي القانون الأردني سلطانه على كل مضرور من جريمة، أينما وقعت، لمجرد أن المضرور موجود على أراضيها.
3. **«إذا ارتكبت من أحد الأشخاص المقيمين فيها»:** وفي تفسير هذا النص ما قد يحمل نتائج غريبة، فمن المتصور أن يضفي القانون الأردني سلطانه على الجرائم المرتكبة من مقيم على أراضيها، وهذا سندًا لمبدأ الصلاحية الإقليمية وتم تكراره في أكثر من موضع، وعند البحث في كلمة مقيم؛ وجدنا في التشريعات ما يعطيها معنى «الشخص الذي يحمل إذنًا

44. انظر تفصيلًا في ذلك معظم مؤلفات علم الإجرام والعقاب، والتي تتناول آثار الجريمة على المجتمعات من مختلف الأوجه والصعد. من ذلك: أحمد عوض بلال، **علم الإجرام**، (دار الثقافة العربية للنشر والتوزيع، القاهرة، 1995).

45. فالمجني عليه مثلًا في جريمة القتل من تم إزهاق روحه، ولكن المتضررين من ذلك كثر، مثل زوجته وأبنائه، والمجني عليه في جريمة إساءة الائتمان هو المودع، أما المضرور فهو المالك، والأمثلة على ذلك كثيرة. انظر تفصيلًا: عبود السراج، **شرح قانون العقوبات القسم العام**، (جامعة دمشق، دمشق، 2007، ص. 230 وما بعدها).

رسميًا بالإقامة في المملكة»[46]، ووجدنا في التطبيقات القضائية ما يعطيها معنى «مقيم في المملكة الأردنية الهاشمية أي له موطن قانوني في الإقليم الأردني»[47]، وتفسير ذلك أن هذا الشخص يطبق عليه القانون الأردني في أي مكان يرتكب فيه جريمة إلكترونية، سواء أتم ذلك في الإقليم الأردني أم خارجه.

المطلب الثالث

ضوابط الاختصاص القضائي في قانون إساءة استخدام الحاسوب الإنجليزي ومحدداته

ظهرت مشكلة الاختصاص في القانون الإنجليزي إلى حيز الوجود عام 1985، عندما قام أحد الأشخاص بإرسال برقية من لندن يعتزم من خلالها تحويل أموال – بشكل غير قانوني – من نيويورك إلى حسابه في جنيف، ولكن العملية لم تتم، حيث تم عرض القضية على محكمة (Crown Court) وتم إدانته؛ إلا أنه عندما نظرت محكمة الاستئناف في القضية قررت عدم اختصاص المحاكم الإنجليزية بها؛ لعدم وجود النص، وتوصلت إلى استنتاج مفاده؛ «أنه وفي حال كانت المحاولة ناجحة، فإن السرقة سوف تكون في نيويورك وبالتالي فإنه لن يكون للمحاكم الإنجليزية أي اختصاص لملاحقة الجاني».[48]
من هنا ثار النقاش في الفقه الإنجليزي حول هذا الموضوع، ذلك أن الاختصاص الوطني على درجة عالية من الأهمية لاستهداف مرتكبي جرائم القرصنة والاختراق، خاصة أن الطريقة المتبعة لارتكاب هذا النوع من الجرائم يجعل القواعد المعمول بها حاليًا في التشريعات الإنجليزية غير قابلة للتطبيق. الأفعال قد تكون مُجرمة في دولة وغير مُجرمة في دولة أخرى بالرغم من أن تأثيرها يطال الدولتين، وتنازع الاختصاص قد يكون سلبيًا عندما لا يطال اختصاص الدولتين أيًّا من الأفعال المرتكبة، كما قد يكون إيجابيًا عندما تدعي أكثر من دولة اختصاصها في الوقت ذاته. من هنا احتدمت الآراء في الفقه الإنجليزي حول أي من المعايير تُعتمد في موضوع الاختصاص الوطني: هل هو معيار مكان ارتكاب الفعل، أم أنه مكان إقامة الفاعل، أم أنه مكان وقوع النتيجة، أم جنسية مالك الكمبيوتر الذي تم اختراقه، أم كل هذه المعايير مجتمعة.

نتيجة لهذا النقاش، احتوى «قانون إساءة استخدام الحاسوب» على قواعد معقدة لتنظيم الاختصاص القضائي، وتسليم المجرمين في هذا النوع من الجرائم وذلك في فقراته من 4 حتى 9، حيث نص القانون على أن كل ما يتطلبه القضاء الإنجليزي لإسباغ ولايته على هذه الجرائم هو وجود (Significant Link) «رابط هام» مع الإقليم الإنجليزي إنجلترا، ويلز، اسكتلندا أو إيرلندا الشمالية، فإما أن يكون الفعل ارتكب في إنجلترا بهدف اختراق كمبيوتر خارج الوطن، أو ارتكب خارج الوطن بهدف اختراق كمبيوتر في إنجلترا. على سبيل المثال؛ يحاول شخص من داخل إنجلترا القيام بعملية اختراق كمبيوتر في السويد، أو يحاول شخص في إيطاليا اختراق كمبيوتر يقع في لندن، بشرط ازدواجية التجريم؛ أي أن الفعل الذي تم ارتكابه من إنجلترا أو على إنجلترا يُشكل جريمة في كلتا الدولتين. بطبيعة الحال فإن هذا الأمر لا يُشكل أي عائق كون جرائم الاختراق والاحتيال الإلكتروني مُجرمة في معظم الدول.[49]

سوف نقسم هذا المطلب لفرعين، نتناول في الأول قواعد الاختصاص في قانون إساءة استخدام الحاسوب البريطاني، ونخصص الثاني للآراء الفقهية المختلفة التي بدأت تنادي بالعودة عن هذا الاختصاص، واستعادة القوانين سلطانها على الإقليم الوطني، على حد رأيهم.

الفرع الأول: قواعد الاختصاص في قانون إساءة استخدام الحاسوب البريطاني

صاغ القانون مجموعة من الأسس والتي حدد بموجبها اختصاص القضاء الإنجليزي بنظر هذا النوع من الجرائم. هذه

46. انظر في ذلك قانون الإقامة وشؤون الأجانب الأردني رقم 24 لسنة 1973 وغيره العديد من القوانين.
47. حكم محكمة التمييز الأردنية: الأحكام الجزائية، الطعن رقم، 806 لسنة 1999 قضائية، بتاريخ 15 أبريل 2000.
48. For more details see: Russel Smith, Peter Grabosky and George Urbas, *Cyber Criminals on Trial*, Cambridge University Press, Cambridge, 2004, & 59.
49. Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, Sapna Tyagi, *Cybercrime, Digital Forensics and Jurisdiction*, Springer International Publishing Switzerland, 2015, & 33.

الأسس قامت بناء على ما تم تسميته «الرابط الهام» (Significant Link) بإقليم الدولة، فإذا ما وجد هذا الرابط بالإقليم فإن القضاء الإنجليزي يكون مختصًا بالنظر في الجريمة. حددت المادة الخامسة من القانون حالات توافر «الرابط الهام» وفقًا لما يلي:

1. **الجرائم المرتكبة خارج الإقليم:** عندما يكون المتهم في بلد خارج المملكة المتحدة وقت ارتكاب الفعل الذي يُشكل الجرم، يتوفر «رابط هام» بالولاية القضائية الوطنية إذا:

أ. كان المتهم من مواطني المملكة المتحدة في ذلك الوقت.

ب. كان الفعل يشكل جريمة بموجب قانون البلد الذي وقعت فيه.

أي أن القانون اشترط توافر هذين الشرطين مجتمعين، أي أن يكون المتهم بريطاني الجنسية، مع ازدواجية التجريم. هذا بطبيعة الحال ما ينسجم ومذهب الصلاحية الشخصية، الذي يلاحق المواطن الذي يرتكب جناية أو جنحة خارج الدولة، إذا لم يتم معاقبته في تلك الدولة. غير أن هذا النص يتعلق بقانون إساءة استخدام الحاسوب والجرائم التي تم النص عليها بموجبه.

قد تم تعديل هذه المادة عام 2015[50] بإضافة فقرة تفسيرية لها؛ حيث عَرَّف التعديل كلمة «البلد» (Country) الذي يقيم فيه المتهم بالإقليم، بطبيعة الحال فإن الإقليم يتضمن المساحة الجغرافية التي يطبق عليها القانون، سواء أكانت إقليمًا بريًا أم جويًا أم مياهًا إقليمية. كما تم بيان المعنى المُتَضَمَّن في عبارة «مواطن المملكة المتحدة» (United Kingdom Citizen) بأنه كل من يحمل الجنسية بموجب قانون الجنسية البريطاني لعام 1981، سواء أكان مقيمًا في بريطانيا، أم خارجها.

2. **الجرائم المرتبطة بالإقليم:** نص قانون إساءة استخدام الحاسوب على وجود «رابط هام» في حال ارتبطت الجريمة بالإقليم البريطاني بهذا الرابط، سواء من ناحية الفاعل أم من ناحية محل الجريمة؛ بناء عليه فقد اعتبر القانون هذا الرابط موجودًا في الحالات التالية:

أ. إذا كان الفاعل موجودًا في البلد الذي تم به فعل الاختراق الذي وقع على كمبيوتر أو نظام معلوماتي في المملكة المتحدة؛ أي أن الفعل وقع على الإقليم الوطني بواسطة شخص موجود خارج إقليم الوطن، نلاحظ هنا أن المشرع اشترط تمام الفعل لإجراء الملاحقة، ولم يتطرق للشروع بذلك.

ب. إذا كان الكمبيوتر أو النظام المعلوماتي الذي تم اختراقه أو محاولة اختراقه موجودًا خارج إقليم المملكة المتحدة من قبل شخص موجود داخلها؛ في هذه الحالة بسط المشرع الإنجليزي سلطانه سواء أتم الفعل أم اقتصر على حالة الشروع به.

ج.إذا كان الكمبيوتر أو النظام المعلوماتي الذي تم اختراقه أو محاولة اختراقه أو تسهيل عملية اختراقه موجودًا خارج إقليم المملكة المتحدة من قبل شخص موجود داخلها؛ وفي هذه الحالة فإن المشرع الإنجليزي يمتد بسلطانه للاشتراك بالفعل، فلم يقتصر ذلك على الفاعل الأصلي؛ بل امتد به للشريك الذي يقتصر دوره على تسهيل عملية الاشتراك.[51]

نلاحظ في هذه النصوص أن الرابط الذي استخدمه المشرع الإنجليزي يستند إلى مبدأ الصلاحية الإقليمية، فيعتبر أن الجريمة مرتكبة في الإقليم الوطني إذا تم أي عنصر من عناصرها داخل الإقليم، سواءً ارتُكِبَت بالكامل، أم توقفت عند مرحلة الشروع، وسواء أكانت المساهمة أصلية أم تبعية؛ أما في حالة الجرائم المرتكبة من قبل أشخاص خارج الإقليم وكان محلها موجودًا في الإقليم فقد اكتفى المشرع ببسط سلطانه في حال اكتملت عناصر الجريمة ولم يشمل الشروع بها.

الفرع الثاني: ظهور تيار حديث في إنجلترا تحت مسمى «استعادة السيطرة على قوانين المملكة المتحدة»

ثار نقاش وجدل كبير في حزب المحافظين في الآونة الأخيرة حول ضرورة استعادة إنجلترا سيطرتها على قوانينها ثانية.

50. تم إضافة الفقرة 5 (1A) و (B1) بتاريخ 5 مارس 2015 بموجب الفقرة التاسعة من قانون الجرائم الخطرة لعام 2015 (Serious Crime Act 2015).

51. تم إضافة هذه الفقرة بموجب التعديل الذي تم بقانون الشرطة والعدالة الجنائية لعام 2006 (Police and Justice Act 2006) والجدير ذكره؛ أن تعديلين دخلا على هذه الفقرة: الأول بتاريخ 1 أكتوبر 2007 والثاني بتاريخ 1 أكتوبر 2008.

وجدت هذه النداءات آذانًا مصغية من قبل الحكومة في معظم القوانين باستثناء قانون واحد؛ هو قانون إساءة استخدام الحاسوب (Computer Misuse Act)، النقاش الذي أثاره الحزب هو أن المملكة المتحدة ما زالت تولي اهتمامًا كبيرًا لمصالح الدول الأخرى، في حين أن جرائم كبيرة قد ترتكب على الأراضي البريطانية.[52]

بالعودة إلى الجذور التاريخية لقواعد الاختصاص في هذا القانون، نجد أن هذا الموضوع أُثير في العام 1990 من قبل اللجنة التي صاغت القانون. كانت هناك دعوة من قبل (Tam Dalyell) لمحاكمة من يرتكب جريمة استنادًا لهذا القانون في المملكة المتحدة ما دام الشخص موجودًا فيها والفعل تم فيها، حتى لو كانت أجهزة الحاسوب المستهدفة خارج المملكة المتحدة؛ إلا أنه لم يؤخذ برأيه في ذلك الحين، وتوالت التعديلات في القانون حتى تغيرت وجهة النظر هذه بالعديد من التعديلات والأسس المعقدة والمتداخلة.[53]

يمكن ملاحظة ذلك في المعايير التي تم اعتمادها لتحديد الاختصاص في قانون إساءة استخدام الحاسوب، حتى إن معظم الفقه الإنجليزي أطلق عليها المعايير المعقدة (Complex Elements)، كما بينا سابقًا. بدأت سهام النقد لهذه المعايير تتصاعد حتى ظهرت بكل قوتها عام 2016 بعد قضية «US v Lauri Love»[54] حيث ظهر ما يسمى بتيار (taking back control of UK laws) أي لنستعيد سيطرتنا على قوانينا.

حقيقة الأمر أن هذه الانتقادات بدأت منذ عام 1996 في قضية شاهال (Chahal v. The UK). ازدادت حدتها عام 2012 في قضية عثمان الملقب بأبي قتادة (Othman (Abu Qatada) v. UK)، عندما بدأ مسؤولون وقضاة من إنجلترا ينتقدون السيطرة والسيادة التي تمتد بها المحكمة على سلطان القوانين الإنجليزية.[55]

تفاصيل القضية أن «شاهال» من أصول هندية، هاجر إلى بريطانيا بشكل غير مشروع، ثم ما لبث أن صحح وضعه القانوني استنادًا إلى قوانين اللجوء، حيث إنه من قادة طائفة السيخ الهندية. قام بعد ذلك بتزعم تيار سيخي متطرف في إنجلترا، واتهم عدة مرات بقضايا إرهابية غير أنها لم تثبت عليه؛ بناء عليه قرر القضاء الإنجليزي ترحيله إلى الهند، طعن أنه سيتعرض للاضطهاد أذا تم ذلك؛ فقام بتقديم شكوى للمحكمة الأوروبية، صدر قرار المحكمة وقضى بإلغاء قرار القضاء الإنجليزي، واعتباره أن هذا القرار مخالف للمادة الثالثة من الميثاق الأوروبي لحقوق الإنسان.[56] أما في قضية أبي قتادة فقد تم طلب استرداده من قبل الأردن؛ لاتهامه بالعديد من قضايا الإرهاب، صدر قرار القضاء الإنجليزي وقضى بترحيله، لكن وبعد طعنه بهذا الحكم أمام المحكمة الأوروبية تم إلغاء القرار للسبب ذاته أعلاه.[57]

تمت إثارة موضوع الاختصاص مرة أخرى في قضية السيد لوري عام 2016، ولأهمية هذه القضية وبسبب الأبعاد الكبيرة التي أخذتها سياسيًا وقانونيا، فقد آثرت الدراسة تناولها بشيء من التفصيل ومن مصادر ومراجع مختلفة.

إذ إن Lauri Love يبلغ من العمر 31 عامًا، ومصابٌ بداء التوحد. تمكن هذا الشاب من اختراق العديد من المواقع

52. Amberhawk Training, "Should Computer Misuse Act offences committed in UK be prosecuted in UK? Take back control... that's the plan, right?", *The Register*, a leading global online tech publication, 4 October 2016. Last visited: June 24, 2017. www.theregister.co.uk.
53. Janet (UK), *All-Party Internet Group enquiry into the Computer Misuse Act*, 2004. See link: community.jisc.ac.uk.
54. USA v Lauri Love, *Judge N Tempia In the Westminster Magistrates' Court*, September 16, 2016. For full details see: www.judiciary.gov.uk.
55. كان من أبرز هؤلاء المنتقدين: رئيس الوزراء ديفيد كاميرون (David Cameron)، والأمين العام للقضاء كريس جريلنغ (Chris Grayling)، بالإضافة إلى تيريزا ماي (Theresa May) والعديد من كبار القضاة. انظر في ذلك:
Kessler, Reuters, "Why are the Conservatives against the European court of human rights?", *The Guardian*, 17 July 2014. www.theguardian.com.
56. Chahal v. The UK, (22414/93) [1996] ECHR 54 15 November 1996. www.hrcr.org.
57. Othman (Abu Qatada) v UK (2012) 55 EHRR 1, 189. Law Teacher, The Law Essay Professionals, www.lawteacher.net.

الإلكترونية التابعة لمختلف الوكالات الحكومية الأمريكية مثل الجيش، ناسا، مجلس الاحتياطي الاتحادي ووكالة حماية البيئة. في عام 2013 تم اعتقال السيد لوري من قبل السلطات البريطانية استنادًا إلى قانون إساءة استخدام الحاسوب.

تم النظر في طلب التسليم من قبل المحكمة (Crown Court)، وضمّن الادعاء العام بيناته أن الجرائم المرتكبة من قبيل الجرائم الخطيرة (Serious Crimes) والتي يجوز التسليم فيها سندًا لأحكام قانون إساءة استخدام الحاسوب، ودليل على ذلك بسابقتين؛ أولاهما قضية (R v Adam) في محكمة كينغستون كراون (Kingston Crown Court) في 12 سبتمبر 2016، حين قام أحد القراصنة بالوصول إلى موقع شركة سبائك ذهب للحصول على أسماء وعناوين وأرقام عائدة للعملاء؛ وذلك لتمكين الشركات الزميلة من اعتراض عمليات تسليم الذهب. حكم عليه بالسجن لمدة خمس سنوات وأربعة أشهر.[58] وقضية "R v Nazariy Markuta" في محكمة تاج سوثوارك (Southwark Crown Court) في 22 سبتمبر 2016، حين تمكن عضو في مجموعة قرصنة من الحصول على 300 كيلوبايت من أسماء المستخدمين وكلمات السر من موقع ياهو وعرضها للبيع، وقد حكم عليه بالسجن لمدة عامين.[59]

رد الدفاع بأن السيد لوري سيواجه حكمًا بالسجن لمدة 99 عامًا إذا تم تسليمه للولايات المتحدة، أي أنه يساوي ما بين جريمة القرصنة وجرائم القتل والاغتصاب، وهو أمر غير قابل للتصديق ولا يقبله العقل. في سبيل منع تسليم المتهم؛ بنى محامي الدفاع بيناته على محاور ثلاثة، أولها: أن المتهم سيواجه عقوبة بالسجن في الولايات المتحدة وليس في المملكة المتحدة على بعد آلاف الأميال، وهذا يعني أن جزءًا كبيرًا من التحقيق وجمع الأدلة لم تشارك به سلطات التحقيق البريطانية؛ كونه وقع في الأراضي الأمريكية حيث تقع المواقع الإلكترونية التي تم الاعتداء عليها؛ ثانيها: أن السيد لوري يعاني من أمراض عديدة منها؛ متلازمة أسبرجر وطيف التوحد والاكتئاب والأكزيما والربو، ولن يجد العناية الخاصة به كمريض في السجون الأمريكية، وهذا أمر يضر بصحته؛ وثالثها: أن هناك جزءًا كبيرًا من القضية ساهمت به المواقع الإلكترونية ذاتها التي تم الاعتداء عليها؛ كونها فشلت في الحفاظ على أمن وسلامة مستخدميها، ولو حدث هذا في إنجلترا لتم إيقاع غرامة كبيرة على هذه المواقع؛ جراء فشلها في حماية مواقعها بالطرق الصحيحة. من الأمثلة التي ساقها الدفاع على ذلك:

- تم تغريم شركة (Staysure.co.uk Limited)، وهي شركة تأمين للإجازات التي يتم حجزها عبر الإنترنت، مبلغ £175,000 بسبب إخفاقها في تأمين سجلات العملاء، مما تسبب بالحصول على معلومات حول 100.000 بطاقة ائتمان سارية المفعول، ومعلومات طبية، وأرقام سرية لبطاقات ائتمان تتعلق بالعملاء بالرغم من أن قواعد الأمان تفرض عدم تخزين مثل هذه المعلومات.[60]
- تم تغريم شركة (Worldview Limited)، وهو موقع لحجز الفنادق على الإنترنت، مبلغًا قدره £7.500، تم تخفيضه من أصل الغرامة البالغة £75،000 حيث كانت الشركة في حالة عسر مالي، بعد فشلها في إجراءات الحماية لمجموعة من نقاط الضعف على موقع الشركة مما أدى إلى حصول المخترقين على تفاصيل بطاقات الدفع الإلكتروني لعدد من العملاء بلغ عددهم 3.814 زبونًا.[61]

بالرغم من كل هذه المعطيات إلا أن حكم القاضي كان كالتالي: «بإجراء عملية المقاربة والموازنة بين حقوق السيد لوري، فإن المحكمة تجد بأن حقوقه لم يتم انتهاكها، وأن السيد لوري متهم بارتكاب العديد من الجرائم الخطرة المتعلقة باختراق مواقع إلكترونية خلال الفترة من أكتوبر 2012 ولغاية أكتوبر 2013، وتتفهم المحكمة بأن السيد لوري يعاني من مشاكل نفسية

58. What lies beneath the extradition of hacker Gary McKinnon to the USA, Amberhawk Training Limited. www.amberhawk.typepad.com.
59. Untargeted, bulk, indiscriminate data retention is unlawful and creates risks to adequacy determination post. Brexit, Amberhawk Training Limited, www.amberhawk.typepad.com.
60. £175,000 fine for data breach, Article posted Thursday 5 March 2015, last visited 24 June 2017. www.cookeandmason.com/news.
61. UK hotel booking website fined after theft of payment card data, article posted on 25 October 2014, last visited 24 June 2017. www.pcibooking.net/blog.

وجسدية؛ إلا أنها تجد أن العناية الصحية الكافية ستقدم له خلال فترة محاكمته أو الحكم عليه في السجون الأمريكية، وأن كافة احتياجاته سوف يتم تلبيتها من قبل السلطات الأمريكية، وعليه فإن المحكمة مطمئنةٌ لكافة ظروف التسليم وبأن كافة حقوق السيد لوري سيتم ضمانها، ولذلك فإنها توافق على التسليم».

واجه هذا الحكم انتقادات حادة من كافة الأطياف القانونية والسياسية، وتعالت الأصوات بضرورة عدم تسليمه، وضرورة إعادة النظر بكافة أسس التسليم وقواعد الاختصاص بقانون إساءة استخدام الحاسوب، ولا يزال هذا النقاش والجدال الفقهي محتدمًا لغاية الآن.[62]

المبحث الثالث

البعد الوطني والدولي لحل مشكلة الاختصاص القضائي للجرائم الإلكترونية

الواقع والمأمول

سوف نتناول في هذا المبحث الإصلاحات الوطنية التي تقترحها الدراسة على التشريعات الوطنية، وذلك في المطلب الأول، والإصلاحات على المستوى الدولي، نحو محكمة دولية للجرائم الإلكترونية، وذلك في المطلب الثاني.

المطلب الأول

الإصلاحات التشريعية الوطنية

اعتمدت التشريعات الأردنية على الأحكام العامة الواردة في قانون العقوبات حتى عام 2006، وهو العام الذي شهد أول تعديل يتعلق بموضوع الاختصاص في الجرائم الإلكترونية وفقًا لقانون أصول المحاكمات الجزائية؛ حيث يُفترض أنه شكل إضافة لهذا الموضوع. ومن ثم رأى التنظيم النهائي لهذا الموضوع النور بموجب المادة 17 من قانون الجرائم الإلكترونية عام 2017، مما يعطي الانطباع أن التجارب المختلفة في التشريعات الأردنية، والاستفادة من خبرات الدول كان ولا بد أن تترك أثرها على القانون، خاصة وأنه صدر عام 2015، أي بعد تجارب طويلة جدًا للعديد من الدول في العالم، والتي من المفروض أنها أُخِذت بعين الاعتبار.

لكن الواقع ينبئنا بعكس ذلك، فالتعديل الذي حصل عام 2006 كان موفقًا بجزء منه، وغير منضبط في الجزء الآخر، أما قانون عام 2015 فقد استحدث مادة بها من العيوب والنقد الشيء الكثير، وبها من الغموض شيء أكثر، كما أنها واسعة فضفاضة بشكل لا مثيل له، مما يثير الكثير من الإشكالات أمام تطبيقها. رغم عدم عثور الدراسة على أي تطبيق لها لغاية الآن، وترك موضوع الاختصاص للأحكام العامة أفضل من قواعد غير محددة ولا منضبطة.

تقترح الدراسة على المشرعين الأردني والقطري أحد خيارين، أولهما: إجراء التعديل على الأحكام العامة في قانون العقوبات وفقًا لما يلي:

- التعديل على مبدأ الصلاحية الإقليمية لشمول جرائم الشروع بالجرائم الإلكترونية، كما فعل القانون القطري، ذلك أن قانون الجرائم الإلكترونية الأردني لا يعاقب على الشروع في هذه الجرائم، إلا إذا كانت من نوع الجناية وفقًا للأحكام العامة، وبالتالي شمولها في الاختصاص الإقليمي، إذا ما أراد الفاعلون إيقاع النتيجة على الإقليم الأردني.
- التعديل بإضافة الجرائم الإلكترونية لمبدأ الصلاحية الذاتية، أي اعتبارها من ضمن الجرائم التي تتعلق بأمن الدولة ومصالحها العليا، وبالتالي فإن قانون العقوبات في البلدين، الأردن وقطر، يسري عليها إذا تم ارتكابها خارج الإقليم، هذا يعني عدم التوسع لشمول كافة الجرائم الإلكترونية في الخارج، إنما الجرائم الخطيرة فقط، وفقًا لضابط تعلقها بأمن الدولة ومصالحها العليا.

62. For more details see: Mark Goldberg, *From Latvia, without love: EU-US cybercrime extradition in the global rights conversation*, European Legal Studies Center, Columbia University, Columbia Journal of European Law, Spring, 2015, 21 Colum. J. Eur. L. 329. Duncan Campbell, "Lauri Love wouldn't get justice in the US. UK courts must try his hacking case", The Guardian, January 9, 2017.

- التعديل على مبدأ الصلاحية العالمية؛ للنص على سيادة السلطان التشريعي في الأردن وقطر على كل من يقبض عليه في الإقليم الأردني أو القطري، وكان قد ارتكب جريمة إلكترونية خارجه، وألا يقتصر هذا الموضوع على المقيم فقط.

ثانيهما: هو أن يتبنى قانون الجرائم الإلكترونية ما جاء في العديد من الاتفاقيات الدولية، مثل اتفاقية الجريمة المنظمة عبر الوطنية UNTOC))، واتفاقية الأمم المتحدة لمكافحة الفساد (UNCAC) وغيرها العديد من الاتفاقيات الدولية والعربية من مثل القانون العربي الاسترشادي لمكافحة الفساد، والقانون العربي الاسترشادي لمكافحة جرائم الاتجار بالبشر[63]، التي جاءت في النصوص ذاتها، حين تناولت الجرائم عبر الوطنية.

تناولت اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية[64] هذا الموضوع معتبرةً الجريمة ذات طابع عبر وطني، في إحدى الحالات التالية[65]: إذا ارتُكبت في أكثر من دولة واحدة، أو إذا ارتُكبت في دولة واحدة ولكن جرى جانب كبير من الإعداد أو التخطيط لها أو توجيهها أو الإشراف عليها في دولة أخرى، أو إذا ارتُكبت في دولة واحدة، ولكن ضلعت في ارتكابها جماعة إجرامية منظمة تمارس أنشطة إجرامية في أكثر من دولة واحدة.

ذلك أن هذه العناصر تشمل كافة الصور التي يمكن من خلالها للجريمة أن تتجاوز الحدود، بالإضافة أن كلا البلدين، الأردن وقطر، قاما بالتصديق على معظم هذه الاتفاقيات بالتالي فإنهما – بطبيعة الحال – ملتزمتان بها[66]؛ هذا بالإضافة إلى أنه تم استعمال هذه المعايير في أكثر من قانون، سواء في الأردن أو قطر.[67]

المطلب الثاني

الإصلاح على المستوى الدولي

«نحو محكمة جنائية دولية للجرائم الإلكترونية»

لا بد للمجتمع الدولي من الاعتراف بأمرين؛ أولهما أن أمن هذا المجتمع وحدة واحدة لا تتجزأ، وأن المجرمين لا يحترمون الحدود الجغرافية والسياسية ولا يلقون لها بالًا، وثانيهما ضرورة وجود هيئة دولية ممثلة بتنظيم دولي «محكمة دولية» لمواجهة مثل هذه الجرائم، ذلك أن الواقع ينبئنا أن عددًا كبيرًا من جرائم الإنترنت الدولية التي ترتكب لا يتم متابعتها قضائيا، أو تتعذر هذه المتابعة.

وبناء عليه – وفي سبيل بيان رؤية الدراسة لإنشاء محكمة دولية للجرائم الإلكترونية – سوف نبين فيما إذا وجدت سوابق قضائية دولية، بإيجاد محاكم دولية، لجرائم معينة؛ يستشعر الجميع خطورتها من ناحية، ومبررات عدم اختصاص المحكمة الجنائية الدولية بالجرائم الإلكترونية، ومن ثم ننتقل للتوصية الرئيسة لهذه الدراسة.

أولًا: السوابق القضائية الدولية

في إطار بحثنا عن سوابقَ عملية لمحاكم في تاريخ الأمم المتحدة، فقد وجدت الدراسة تطبيقًا مثيلًا لذلك؛ يتمثل باتفاقية الأمم المتحدة لقانون البحار 1982، والتي أصبح يطلق عليها فيما بعد «اتفاقية قانون البحار»، والتي تحوي فصولًا متعددة، من بينها تنظيم موضوع القرصنة في أعالي البحار، وإنشاء محكمة خاصة لذلك، حيث شعر الجميع بأن هناك منطقة في العالم لا تخضع لسلطان أي دولة، وهي منطقة أعالي البحار، وأن هناك من يستغل هذه المنطقة لارتكاب أعمال القرصنة،

63. انظر القوانين العربية النموذجية الاسترشادية على موقع جامعة الدول العربية. www.lasportal.org

64. اعتُمدت وعُرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 25 الدورة الخامسة والخمسون المؤرخ في 15 نوفمبر2000.

65. لمزيد من التفصيل انظر: أمير فرج يوسف، **الجريمة المنظمة عبر الوطنية**، (دار المطبوعات الجامعية، الإسكندرية، 2008، ص. 15 وما بعدها).

66. الاتفاقيات والمواثيق الدولية التي صادقت عليها المملكة الأردنية الهاشمية: www.ncihl.org.jo والاتفاقيات والمواثيق الدولية التي صادقت عليها دولة قطر: www.qatar.smetoolkit.org.

67. انظر مثالًا: المادة الأولى من قانون مكافحة الاتجار بالبشر القطري رقم 15 لسنة 2011، والمادة الثالثة من قانون منع الاتجار بالبشر الأردني رقم 9 لسنة 2009.

ومن هنا تنبه المجتمع الدولي لهذا الخطر، وأنه ما من سبيل لمكافحة القرصنة إلا بالتعاون الدولي بين جميع الدول، وهذا ما نصت عليه المادة 100 من الاتفاقية وجاء فيها ما يلي: «تتعاون جميع الدول إلى أقصى حد ممكن في قمع القرصنة في أعالي البحار أو في أي مكان خارج ولاية أية دولة».

1. تأليف المحكمة

تم إنشاء هذه المحكمة استنادًا للملحق السادس من اتفاقية قانون البحار، حيث تتألف من هيئة تتكون من 21 عضوًا مستقلًا، ويُراعى في التكوين تمثيل النظم القانونية الرئيسة في العالم والتوزيع الجغرافي العادل.

2. اختصاص المحكمة

تختص المحكمة بفرعين رئيسين: قضائي يتمثل بحل النزاعات وآخر استشاري. أما الاختصاص القضائي فيتمثل بما يلي: النظر بأي نزاع حول تفسير أو تطبيق اتفاقية الأمم المتحدة لقانون البحار، والنزاعات المتعلقة بقاع البحار، والنظر في الإجراءات التحفظية، والنظر في طلبات الإفراج السريع عن السفن وطواقمها.
وكما أن للمحكمة دورًا قضائيًا في حل المنازعات، لها أيضًا دورٌ استشاريٌّ سواء أكان ذلك يتعلق بالاتفاقية ذاتها أم سندًا لأي اتفاقية أخرى؛ كما تجب الإشارة إلى أن الفقرة الرابعة من المادة 288 من الاتفاقية، والمادة 58 من القانون الداخلي للمحكمة الدولية لقانون البحار؛ تقضيان بأن المحكمة هي صاحبة الولاية في تحديد الاختصاص الخاص بها في حالة نشوب خلاف حول ما إذا كانت المحكمة ذات اختصاص أم لا، ويكون ذلك بموجب قرار يصدر عنها.

ثانيًا: المحكمة الجنائية الدولية

للإجابة على التساؤل حول جواز قيام المحكمة الجنائية الدولية بنظر الجرائم الإلكترونية – ولقطع دابر الشك باليقين – لا بد من التطرق السريع لاختصاصاتها والنظر فيما إذا كانت تختص بهذا النوع من الجرائم أم لا.

انطلاقا من ديباجة نظام روما الأساسي للمحكمة الجنائية الدولية فإن اختصاص هذه المحكمة يتحدد في الجرائم الأشد خطورة والتي تثير قلق المجتمع الدولي بأسره، وقد جاءت المادة الخامسة من نظام روما الأساسي في فقرتها الأولى لتحديد هذه الجرائم بأنها كما يلي[68]: جريمة الإبادة الجماعية، والجرائم ضد الإنسانية، وجرائم الحرب، وجريمة العدوان.
لدى اطلاعنا على الاختصاص الموضوعي للمحكمة الجنائية، نصل لنتيجة مفادها أن الجرائم الإلكترونية غير مدرجة ضمن هذه الجرائم بشكل مباشر، بالرغم من أن بعض هذه الجرائم السالفة الذكر قد يتم ارتكابها بوسائل إلكترونية، وتبقى الجنائية الدولية بالنهاية محكمة غير مختصة بنظر هذا النوع من الجرائم.[69]

ثالثًا: المحكمة الدولية للجرائم الإلكترونية (International Cybercrimes' Court (ICC))

من الواضح أن هذا الخطر الداهم بات يهدد العالم أجمع، حيث أصبحنا نسمع كل يوم عن غزو جديد يطال العديد من دول العالم ويضرب أكثر المؤسسات الاقتصادية والسياسية أهمية، وقد أكدت هذه الهجمات أنها قادرة على النيل من أكثر الدول التي تعتقد أنها محصنة وأنها بمنأى عن هذا الخطر، وهذا كاف للرد على الدراسة الشاملة التي أجراها مكتب الأمم المتحدة لمكافحة المخدرات والجريمة عام 2013، والتي أشارت إلى أن معظم الاستبانات التي تم توزيعها على كافة الدول التي اشتركت بهذه الدراسة؛ أكدت أن دول العالم النامي وحدها من يعتقد بضعف قدرته على مقاومة هذه الهجمات، وأن معظم الدول الأوروبية وأمريكا يرون أنهم قادرون على مواجهتها والنيل منها[70]، وهذا مخالف للواقع الذي يُظهر أن

68. انظر في ذلك: عبد الفتاح بيومي حجازي، **قواعد أساسية في نظام محكمة الجزاء الدولية**، (دار الفكر الجامعي، الإسكندرية، 2006، ص. 22 وما بعدها).

69. Ellen S. Podgor, *Cybercrime: National, Transnational, or International?*, 50 Wayne L. Rev. 97, 2004, & 101.

70. *Comprehensive study on Cybercrime*, Op. cit. 2013, & 192.

معظم هذه الهجمات لا يطال سوى الدول المتقدمة والصناعية؛ الأمر الذي أجبر وزراء من الدول الصناعية السبع الكبرى على ضرورة الاجتماع للتباحث في مكافحة هذا الغزو، وكان ذلك في روما في العاشر من شهر يونيو الماضي 2017، حيث أثمر هذا الاجتماع عن اتفاق هذه الدول على توحيد الجهود في سبيل مكافحة تفاقم خطر الهجمات الإلكترونية الدولية.[71]

من هنا فقد توصلت الدراسة إلى نتيجة مفادها أن الإصلاحات التشريعية الوطنية أمر واجب؛ وعلى غاية من الأهمية، بهدف ألا يكون هناك أي منفذ لأي مجرم، وأن التعاون الدولي شديد الأهمية، وهذا التعاون لا بد أن يثمر – برأي الدراسة – عن صيغة دولية تُجمع عليها دول العالم عن طريق اتفاقية لإنشاء محكمة دولية خاصة؛ للجرائم الإلكترونية تتولى هذه المهمة ((International Cybercrimes' Court (ICC)، ورأينا إمكانية ذلك في المبحث السابق، حينما أجمعت الدول على ضرورة وجود محكمة للنيل من قراصنة البحار، الذين يستغلون مناطق لا سلطان عليها للدول لارتكاب جرائمهم، وما أشبه اليوم بالأمس، ذلك أن الفضاء الإلكتروني أكثر ما يشبه هذه المنطقة، وأن هذا الفضاء يتم استغلاله لارتكاب جرائم تهدد أمن العالم أجمع، ومن هنا نشأت أهمية وجود محكمة مماثلة لنظر مثل هذا النوع من الجرائم، التي يظن مرتكبوها أنهم بمأمن من أي اختصاص، وأن تنازع الاختصاص بين الدول من ناحية، وتعدد جهات التحقيق من ناحية أخرى سيؤمن لهم ملاذًا آمنًا للإفلات من أية عقوبة.

1. الأداة القانونية لإنشاء المحكمة الدولية للجرائم الإلكترونية ((International Cybercrimes' Court (ICC)

مما لا شك فيه أن الجرائم الإلكترونية أصبحت تهدد الأمن والسلم الدوليين، ذلك أن أكثر المنشآت العالمية أهمية وحساسية ليست ببعيدة عنها، والخوف الأكبر من تعرض المنشآت النووية لأي عملية اختراق، وعليه فإنه من الممكن إنشاء المحكمة بقرار من هيئة الأمم المتحدة، أو من مجلس الأمن استنادًا لنص المادة 39 من ميثاق الأمم المتحدة التي تنص على ما يلي: «يقرر مجلس الأمن ما إذا كان قد وقع تهديد للسلم أو إخلال به أو كان ما وقع عملًا من أعمال العدوان، ويقدم في ذلك توصياته أو يقرر ما يجب اتخاذه من التدابير طبقًا لأحكام المادتين 41 و42 لحفظ السلم والأمن الدوليين أو إعادته إلى نصابه".

في إطار بحثنا عن المقصود بمفهوم «السلم والأمن الدوليين» فقد وجدت الدراسة أن ميثاق الأمم المتحدة لم يحدد المقصود بذلك، وجدير بالذكر أن العديد من الباحثين أكدوا على أن الميثاق كان محقًا عندما لم يحدد هذا المفهوم، باعتبار أن السلم والأمن الدوليين يتطوران باستمرار تبعًا لتطور العلاقات الدولية، وأن الممارسة الدولية الميدانية أثبتت أن الأسباب الكامنة وراء هذا النص هي، تمكين مجلس الأمن من صلاحيات تقديرية واسعة في هذا الشأن بموجب المادة ٣٩ من الميثاق.[72]

في سبيل توضيح ذلك، فإنه لا بد من الإشارة إلى أن مفهوم الأمن والسلم الدوليين قد اتسع معناه لما يتجاوز التهديد العسكري، فهناك من يرى أن العديد من الأحداث التي وقعت في العالم غيرت هذا المفهوم تغييرًا كليًا، فمع سقوط الاتحاد السوفييتي وانهيار جدار برلين، التفت العالم إلى مخاطر أخرى – غير عسكرية – لا تقل في خطورتها وأهميتها عن النزاعات المسلحة، مما جعل مدلولي الأمن والسلم الدوليين يبدوان – في هذه المرحلة من تطور العلاقات الدولية – أكثر توسعًا وشمولًا، ومن الواضح أن تشابك العلاقات الدولية نتيجة لتزايد الاعتماد المتبادل وتشابك المصالح بين مختلف أشخاص القانون الدولي، جعل من مواجهة هذه المخاطر الآخذة في التطور أمرًا ملحًا؛ لما تفرضه من تحديات أمام جميع الدول في ظرفيّة لم تعد فيها الحدود الجغرافية والسياسية حصنًا منيعًا للاحتماء من تداعياتها؛ فهذه المخاطر تتطلب مقاربة عقلانية ومتطورة في إطار من التنسيق والتعاون الدوليين، خصوصا أن ما كان ينطبق على أشكال الحرب أصبح ينطبق أيضًا على أشكال السلام، وباعتمادنا قراءة متأنية لميثاق الأمم المتحدة، نجد أنه يتوخى تحقيق

71. **الهجوم الإلكتروني يستنفر الدول الكبرى**، شبكة الجزيرة الإعلامية، www.aljazeera.net. 13 يونيو2017، تاريخ آخر زيارة للموقع 21 يونيو 2019.

72. انظر في ذلك: تقرير الفريق الرفيع المستوى، المعنيّ بالتهديدات والتحديات والتغيير بشأن «عالم أكثر أمنا: مسؤوليتنا المشتركة» [565/59/A] ديسمبر2004. وانظر أيضًا: كوفي عنان، **مواجهة تحديات عالم متغير**، التقرير السنوي لأعمال المنظمة، منظمة الأمم المتحدة، 2006.

السلم والأمن الدوليين من خلال محاولة التأسيس لعلاقات دولية متوازنة، تحكمها مجموعة من الضوابط الصارمة والعلاقات الودية المتبادلة، وهو ما يندرج ضمن الإجراءات الوقائية التي اتبعها الميثاق، فهذا الأخير أكد في ديباجته على أن الأمم المتحدة تهدف إلى ترقية الأوضاع الاجتماعية والاقتصادية لشعوب العالم، بعدما اتضح لواضعي هذا الميثاق تلك العلاقات الجدلية والوثيقة بين تدهور الأحوال الاقتصادية والاجتماعية وبين تنامي الأزمات المختلفة في العالم، بالإضافة إلى أن الميثاق جاء بالعديد من المبادئ التي تدعو إلى إعداد مناخ دولي من التعاون والسلم.[73]

وينبغي لهذا القرار أن يشمل إنشاء جميع الأجهزة المتعلقة بالمحكمة الدولية للجرائم الإلكترونية، من هيئات تحقيق، ونيابة عامة، وقضاة، واختصاص زماني ومكاني، ذلك أن المعاهدة التأسيسية للأمم المتحدة تتمثل بميثاقها الذي ينطبق على جميع أعضائها، وبالتالي فإن قرار مجلس الأمن يشكل قرارًا ملزمًا لكافة الدول الأعضاء فيه.

أما الطريقة الأخرى لإنشاء هذه المحكمة فيمكن أن يكون عن طريق اتفاقية مستقلة تدعو لها الأمم المتحدة، أو يتم الدعوة لها بقرار ملزم من مجلس الأمن، ويلتزم بهذه الاتفاقية من يصادق عليها من الدول الأعضاء، ويُلزم الجميع بالتعاون معها، سواء أصادق على هذه الاتفاقية أم لا.

1. نظام النيابة العامة في المحكمة

لا بد أن يشتمل نظام تأسيس المحكمة على وجود جهاز متكامل ومستقل للنيابة العامة، يختص بالتحقيق وملاحقة مرتكبي الجرائم الإلكترونية الخطيرة والدولية، ويكون هذا الجهاز مستقلًا، وغير تابع لأية دولة أو منظمة، وتلتزم جميع الدول الأعضاء بالتعاون معه، وكذلك المنظمات الدولية المختصة بالتحقيق والملاحقة مثل جهاز الشرطة الدولية.[74]

2. قضاة المحكمة

يكون للمحكمة شخصية قانونية دولية، كما يكون لها الأهلية القانونية اللازمة لممارسة وظائفها وتحقيق مقاصدها، وللمحكمة أن تمارس وظائفها وسلطاتها، على النحو المنصوص عليه في النظام الأساسي لها على إقليم أية دولة طرف.
كما أنه من الممكن الاستئناس باختيار القضاة في المحكمة، بذات أسس وشروط اختيار قضاة المحكمة الجنائية الدولية، مع إضافة شرط الخبرة في مجال الجرائم الإلكترونية، كما أن للمحكمة أن تشكل من قضاتها هيئات بدائية وهيئات استئنافية[75].

3. اختصاص المحكمة

ترى الدراسة أن يكون اختصاص المحكمة الدولية للجرائم الإلكترونية مرتبطًا بشرطين: أولهما أن تكون هذه الجرائم من الجرائم الإلكترونية الخطيرة (Serious Cybercrimes) وفقًا للمعايير التي تحددها المحكمة، وثانيهما أن يكون لهذه الجرائم تأثير على الأمن والسلم الدوليين، ويتسع هذا المفهوم، كما تناولنا سابقًا؛ ليشمل الجوانب السياسية والاقتصادية والاجتماعية وغيرها من الجوانب التي ترتئيها المحكمة استنادًا لوثيقة تأسيسها.

---

73. ادريس لكريني، **مستقبل السلم والأمن الدوليين على ضوء التهديدات الدولية العابرة للحدود**، المجلة المغربية للسياسات العمومية، العدد/المجلد 20، المغرب، ص. 126 وما بعدها، (2016).

74. انظر المادة 15 من نظام روما الأساسي للمحكمة الجنائية الدولية المعتمد في روما في 17 يوليو 1998 وما طرأ عليه من تعديلات في مايو 1999.

75. انظر استئناسًا المواد 34-40 من نظام روما الأساسي للمحكمة الجنائية الدولية، كما يمكن الاستئناس بمبادئ بنجالور للسلوك القضائي (Bangalore Principles of Judicial Conduct) التي وضعت من قبل مكتب الأمم المتحدة لمكافحة المخدرات والجريمة في مدينة بنجالور الهندية، وكذلك الحال بمبادئ السلوك القضائي التي وضعت من قبل المجلس الاستشاري للقضاة في أوروبا عام 2010.

خاتمة

الإنترنت عبارة عن شبكة معلومات عالمية تربط بين أجهزة الحاسوب في العالم، ويتمكن من خلالها ملايين من البشر من التواصل مع بعضهم البعض، ومن الحصول على هذه الكمية من المعلومات في أي مكان يتواجدون فيه[76]، مما يعني أنه –وفي أي وقت – فإن عشرات الألوف من المستخدمين يكونون متواصلين مع بعضهم البعض بمناقشة أو تبادل أفكار ومعلومات حول عشرات الألوف من المواضيع، حتى إن المحكمة العليا الأمريكية وفي أحد أحكامها أشارت إلى أن عالم الإنترنت – وبدون مبالغة بما يحويه من معلومات – هو أشبه ما يكون بالعقل البشري.[77]

وقد اجتاح العالم في الفترة الأخيرة خطرٌ داهم؛ تَمَثَّلَ في كثرة عمليات الاختراقات لهذه المواقع الإلكترونية، بالرغم من كل الوسائل التي تُبذل للحفاظ على أمنها وضمان عدم اختراقها، وهذا يُثير مدى قدرة التشريعات الجنائية على حماية الفرد المُستخدم لهذا الموقع، وحماية الموقع ذاته من هذه الأخطار كلها، والتي أصبح يُطلق عليها «اختراق المواقع الإلكترونية أو قرصنتها».

وتنبئ القرصنة الإلكترونية بالخطر بسبب خواصها التي تميزها عن الجريمة التقليدية، ذلك أن ضحاياها يتعرضون لتعطيل وتدمير مخازن المعلومات الخاصة بهم، وسرقة أموالهم، والتهديد والابتزاز؛ مما يتسبب للاقتصاد بأضرار كبيرة، ومع تزايد نسبة الجرائم الإلكترونية وتَنَوُّع طرقها فقد أصبحت تُلحقُ خسائر مادية كبيرة وفادحة أكثر مما تُسَبِّبُه الجرائم التقليدية، ليس فقط على مستوى الفرد؛ بل تتعداه إلى مستوى المنظمات والجهات والمؤسسات، فجرائم القرصنة أصبحت تُدارُ إلكترونيًا وتوجد على الشبكة الإلكترونية لفتح قنوات تواصل جديدة؛ بهدف استقطاب شريحة أكبر منَ الناس وزيادة أرباحها.

ولم يقتصرِ الأمر على جانب القطاع الخاص، بل انتقل إلى القطاع الرسمي، حيث ظهر ما يُسمى بمصطلح «الحرب الإلكترونية»، وتعني؛ «عمليات اختراق وقرصنة إلكترونية موجهة سياسيًا من دولة ما بهدف التجسس على شبكة حواسيب هيئات رسمية أو شركات خاصة كبرى في دولة أخرى، أو تخريب وتعطيل تلك الشبكات وما يرتبط بها من أجهزة، وهي شكل من أشكال حرب المعلومات التي ينظر إليها أحيانًا على أنها مماثلة للحرب التقليدية، وربما تكون سببًا يدفع باتجاه مثل تلك الحرب، ويقوم بتنفيذ عملية الاختراق عادة شخصٌ اصْطُلِحَ على تسميته بالقرصان أو «الهاكر» وهو في العادة شخص له معرفة عميقةٌ بالحواسيب وشبكاتها، ويملك مهارةً عاليةً في لغات البرمجة وأنظمة التشغيل، ويُعتبر غالبًا بمثابة خبيرٍ في هذا المجال بحيث يستطيع بمهارته استغلال نقاط الضَّعف في أيِّ شبكة حاسوب لاختراقها.[78]

ومن المسلم به أن قواعد القانون الجنائي؛ بشقّيه الموضوعي والإجرائي، تخضع في تطبيقها من حيث المكان لمبدأ مستقر ومعروف؛ ألا وهو مبدأ الإقليمية، الذي يعني خضوع الجرائم التي تقع في إقليم دولة معينة لقانونها الجنائي النافذ، بحيث تصبح محاكمها هي صاحبة الولاية بنظر الدعوى الناشئة عنها، ولا تخضع من حيث الأصل لسلطان أي قانون أجنبي، وفي المقابل لا يمتد سريان قانون الدولة الجنائي خارج نطاقها الإقليمي وفقًا لحدودها المعترف بها في القانون الدولي؛ إلاّ في أحوال استثنائية اقتضتها حماية المصالح الجوهرية للدولة أو متطلبات التعاون الدولي في مكافحة الإجرام.[79]

تطرقت الدراسة لهذا الموضوع الإجرائي البالغ الأهمية، والسُبل المقترحة للتغلب عليه، من الناحيتين الوطنية والدولية على حد سواء، فهناك واجب تشريعي على كاهل كافة الدول؛ أن تقوم بإجراء التعديلات الملاءمة في تشريعاتها لتضمن حماية

76. The United States Supreme: Reno v. ACLU, 521 U.S. 1997) 50-849 ,844).

77. ACLU v. Reno, 929 F. Supp. 1996) 42-835 ,824).

78. **القرصنة الإلكترونية ... سلاح العصر الرقمي**، قناة الجزيرة، تغطية إخبارية، يناير 2015، تاريخ الدخول للصفحة: 17 يونيو 2017. http://www.aljazeera.net/knowledgegate/newscoverage/2015/1/

79. موسى مسعود ارحومة، **الأحكام العامة لقانون العقوبات الليبي**، (الطبعة الأولى، منشورات جامعة قاريونسبنغازي، 2009) ص. 110 وما يليها، الجزء الأول ، النظرية العامة للجريمة.

مصالحها ومنشآتها ومرافقها وأفرادها من أي اعتراض أو تهديد، ولتضمن الحفاظ على أمنها؛ إذ إن عدم وجود قواعد الاختصاص الشاملة التي تغطي كافة حالاتها سوف يؤدي، لا محالة، لعدم إمكانية ملاحقة مرتكبي هذه الطائفة من الجرائم، وحتى لو تم ملاحقتهم فسوف تكون هناك ثغرات بين الدول سيتم استغلالها من قبلهم للإفلات من العقاب. والتعاون الدولي على درجة أكثر أهمية، من ناحية إبرام الاتفاقيات الثنائية والجماعية بين الدول؛ لتنظيم موضوع الاختصاص في الجرائم الإلكترونية للتغلب على الثغرات التي قد تحدث في الاختصاص بين الدول.

وفي النهاية أوصت الدراسة بمقترح إيجاد «المحكمة الدولية للجرائم الإلكترونية»، وإن كان هذا الموضوع لا يعتبر سابقة، من ناحية –فهناك محاكم وجدت سابقًا من هذا النوع– كما أن اختصاص المحكمة الجنائية الدولية لا يشمل الجرائم الإلكترونية من ناحية أخرى.

ونختم هذه الدراسة بخبر حديث أورده موقع «البوابة العربية للأخبار التقنية» بعنوان: «خسائر الهجمات السيبرانية قد تفوق خسائر الأعاصير»؛ حيث أورد أن «التقديرات في عام 2016 تُشير إلى أن «الهجمات السيبرانية» قد كلفت الشركات ما يصل إلى 450 مليار دولار سنويًا على مستوى العالم، وبالمقارنة مع الكوارث الطبيعية مثل الأعاصير؛ فقد تسبب إعصار كاترينا في خسائر تقدر قيمتها بحوالي 108 مليار دولار، مما جعله أكثر الكوارث كلفة في تاريخ الولايات المتحدة».[80]

ونرجو من الله أن تكون هذه الدراسة قد قدمت عونًا لكل من يبحث في هذا الموضوع، ووجدت أذنا واعية لهذه المقترحات، سواء على المستوى الوطني أو الدولي، والله ولي التوفيق.

المراجع

أولًا: المراجع العربية

القرصنة الإلكترونية سلاح العصر الرقمي، قناة الجزيرة (2017)، تاريخ الدخول للصفحة 21 يونيو 2019
https://www.aljazeera.net/knowledgegate/newscoverage/5/1/2015/%D%8A%7D%9%84D%82%9D%8B%1D%8B%5D%86%9D%8A%-9D%8A%7D%84%9D%8A%5D84%9%D%83%9D%8AA%D%8B%1D%88%9D%86%9D8%9A%D%8A%-9D%8B%3D-%84%9D%8A%7D%8AD-%D%8A%7D%84%9D%8B%9D%8B%5D%8B%-1D%8A%7D%84%9D%8B%1D%82%9D%85%9D8%9A.

السويلمين براهيم وبشارة عواد، جريمة الاحتيال عبر شبكة المعلومات الدولية، (2010)، دراسة مقارنة بين القانون الأردني والقانون المصري، رسالة دكتوراه، جامعة عمان العربية للدراسات العليا.

عنبر أحمد، خسائر الهجمات السيبرانية قد تفوق خسائر الأعاصير، صحيفة الوئام الإلكترونية، (18 يوليو، 2017). تاريخ آخر زيارة للموقع 21 يونيو 2019.
https://www.alweeam.com.sa/474055/%D%8AE%D%8B%3D%8A%7D%8A%6D%8B-1%D%8A%7D%84%9D%87%9D%8AC%D%85%9D%8A%7D%8AA-%D%8A%7D%84%9D8

80. أحمد عنبر، «خسائر الهجمات السيبرانية قد تفوق خسائر الأعاصير»، **صحيفة الوئام الإلكترونية**، 18 يوليو2017. تاريخ آخر زيارة للموقع 21 يونيو 2019.

%B%3D8%9A%D%8A%8D%8B%1D%8A%7D%86%9D8%9A%D%8A%-9D%82%9D%8AF-
%D%8AA%D%81%9D%88%9D%-82%9D%8AE%D%8B%3D%8A%7D%8A6/

بلال أحمد عوض، علم الإجرام، (دار الثقافة العربية، القاهرة، 1995).

لكريني إدريس، مستقبل السلم والأمن الدوليين على ضوء التهديدات الدولية العابرة للحدود، العدد/المجلد 20 المجلة المغربية للسياسات العمومية، (2016) المغرب.

الغرايبة أسعد محمد أحمد، تنازع الاختصاص في المسائل الجزائية، دراسة مقارنة، رسالة دكتوراه، جامعة عمان العربية للدراسات العليا، 2012.

شمس الدين أشرف توفيق، شرح قانون العقوبات القطري، القسم العام، النظرية العامة للجريمة والعقوبة، (الطبعة الأولى، جامعة قطر، 2010).

يوسف أمير فرج، الجريمة المنظمة عبر الوطنية، (دار المطبوعات الجامعية، الإسكندرية، 2008).

المعراوي أنس، ما هي عملة Bitcoin الإلكترونية؟، البوابة العربية للأخبار التقنية، aitnews، 26 أغسطس 2013.
https://aitnews.com/26/08/2013/%D%85%9D%8A%7D%87%9D8%9A-
%D%8B%9D%85%9D%84%9D%8A-9bitcoin-%D%8A%7D%84%9D%8A%5D%84%9D83%9
%D%8AA%D%8B%1D%88%9D%86%9D8%9A%D%8A%9D9%8F/

مساعدة أنور محمد صدقي، «إضاءات وتأملات في قانون الجرائم الإلكترونية القطري الجديد، الصادر بالقانون رقم (14) لسنة 2014»، مجلة مركز الدراسات القانونية والقضائية، العدد الثاني، السنة الثامنة، وزارة العدل، قطر، 2016، ص. 305.

مساعدة أنور محمد صدقي، «مدى كفاية أحكام التجريم الإلكتروني في قانون الجرائم الإلكترونية الأردني الجديد رقم 27 لسنة 2015، دراسة مقارنة»، مجلة الشريعة والقانون، جامعة الإمارات، الإمارات العربية المتحدة، العدد 37، يناير 2018، ص. 455.

تقرير الفريق الرفيع المستوى المعني بالتهديدات والتحديات والتغيير بشأن عالم أكثر أمنًا: مسؤوليتنا المشتركة [A/59/565]، 2 ديسمبر 2004، وثائق الأمم المتحدة، https://undocs.org/A/59/565.

أكبر عملية قرصنة إلكترونية في التاريخ تهاجم 74 دولة حول العالم، آمن...نحو توعية شاملة، 15 مايو 2017، http://amenn.net/index.php?s=1&cat=2&id=978، تاريخ آخر زيارة للموقع 21 يونيو 2019.

حسن سعيد عبد اللطيف، المحكمة الجنائية الدولية، دار النهضة العربية للنشر والتوزيع، القاهرة (2004).
عيساني طه، «القرصنة الإلكترونية، الضرر الاقتصادي والفكري»، مجلة جيل الأبحاث القانونية المعمقة، المجلد الخامس، 2016، ص. 105.

جمال الدين عبد الأحد والصغير جميل، المبادئ الرئيسية في القانون الجنائي، القسم العام، دار النهضة العربية للنشر والتوزيع، القاهرة، 1999.

حجازي عبد الفتاح بيومي، قواعد أساسية في نظام محكمة الجزاء الدولية، دار الفكر الجامعي، الإسكندرية، 2006.

القهوجي عبد القادر، القانون الدولي الجنائي، منشورات الحلبي الحقوقية، بيروت، 2001.

عبود السراج، شرح قانون العقوبات، القسم العام، جامعة دمشق، دمشق، 2007.

الخطيب عدنان موجز القانون الجزائي، الكتاب الأول، المبادئ العامة في قانون العقوبات، مطبعة جامعة دمشق، 1963.

السعيد كامل، شرح الأحكام العامة في قانون العقوبات الأردني، دراسة مقارنة، المركز العربي للخدمات الطلابية، عمان، 1998، الطبعة الأولى.

القاضي كمال أنور محمد، تطبيق قانون العقوبات من حيث المكان، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 22 إبريل 1985.

عنان كوفي، مواجهة تحديات عالم متغير، التقرير السنوي لأعمال المنظمة، منظمة الأمم المتحدة، 2006.

كنوش ليلى ودربان كريم، أحكام اختصاص المحكمة الدولية لقانون البحار، مذكرة تخرج في القضاء، الدفعة السادسة عشر، يوليو 2008. منشورة على موقع الأوراس القانوني، 29 نوفمبر 2010.
http://sciencesjuridiques.ahlamontada.net/t1611-topic، تاريخ آخر زيارة للموقع 21 يونيو 2019.

المحكمة الجنائية الدولية...تأسيسها واختصاصاتها، شبكة الجزيرة الإخبارية، 4 مارس 2009. تاريخ آخر زيارة للموقع 21 يونيو 2019.
https://www.aljazeera.net/news/international/4/3/2009/%D%8A%7D%84%9D%85%9D8%AD%D%83%9D%85%9D%8A%-9D%8A%7D%84%9D%8AC%D%86%9D%8A%7D%8A%6D8%9A%D%8A%-9D%8A%7D%84%9D%8AF%D%88%9D%84%9D8%9A%D%8A%-9D%8AA%D%8A%3D%8B%3D8%9A%D%8B%3D%87%9D%8A%-7D%88%9D%8A%7D%8AE%D%8AA%D%8B%5D%8A%7D%8B%5D%8A%7D%8AA%D%87%9D%8A7

بسيوني محمد شريف، المحكمة الجنائية الدولية، المعهد الدولي لحقوق الإنسان، جامعة شيكاغو، دار الشرق، القاهرة، 2004.

ارحومة موسى مسعود، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 28-29 أكتوبر 2009. ص. 17.

ارحومة موسى مسعود، الأحكام العامة لقانون العقوبات الليبي، الجزء الأول، النظرية العامة للجريمة، (الطبعة الأولى،

منشورات جامعة قاريونس بنغازي، 2009).

المجالي نظام، شرح قانون العقوبات، القسم العام، دار الثقافة، عمان، 2009.

هجمات إلكترونية تضرب مؤسسات أوروبية وروسية وأميركية، العربية نت، 27/06/2017. تاريخ آخر زيارة للموقع 24 يونيو 2019.
https://www.alarabiya.net/ar/arab-and-world/0/20176/27/%D8%A7%D9%84%D8%A8%D9%86%D9%83-%D8%A7%D9%84%D9%85%D8%B1%D9%83%D8%B2%D9%8A-%D8%A8%D9%86%D9%88%D9%83-%D8%B1%D9%88%D8%B3%D9%8A%D8%A9-%D8%AA%D8%B9%D8%B1%D8%B6%D8%AA-%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D9%83%D8%AA%D%8B%1D%88%9D%86%9D8%9A%D8%A9

الهجوم الإلكتروني يستنفر الدول الكبرى، شبكة الجزيرة الإعلامية، 13 يونيو2017.

اختراق موقع النادي الأهلي الإماراتي، إرم نيوز، 27 مايو 2017. تاريخ آخر زيارة للموقع 24 يونيو 2019.
https://www.eremnews.com/sports/football/arab/uae/852599

ثانيًا: المراجع الإنجليزية

Comprehensive study on cybercrime, United Nations Office on Drugs and Crime, Vienna, February 2013.

Weber Amalie M. the Council of Europe's Convention on Cybercrime, 18 Berkeley Tech. L.J. ,227 2003.

Amberhawk Training Limited, "Should Computer Misuse Act offences committed in UK be prosecuted in UK? Take back control... that's the plan, right?", The Register, a leading global online tech publication, 4 October 2016. https://www.theregister.co.uk/04/10/2016/should_computer_misuse_act_offences_committed_in_the_uk_be_prosecuted_in_the_uk/. Last visited 24 June 2019.

Dominic Carucci, David Overhuls & Nicholas Soares, Computer Crimes, 48 AM. CRIM. L. REV. ,375 2011) 378). (The article further differentiates between a computer being the object of a crime and the subject of a crime. Generally, a computer is an object of a crime when its hardware or its software is stolen. A computer is generally the subject of a crime in when it is targeted in other ways, including those listed above the line here.)

Campbell Duncan, "Lauri Love wouldn't get justice in the US. UK courts must try his hacking case", January 2017 ,9, The Guardian, https://www.theguardian.com/commentisfree/2017/jan/09/lauri-love-justice-us-uk-courts-hacking-case-extradition. Last visited 24 June 2019.

Podgor Ellen S., Cybercrime: National, Transnational, or International? 50 Wayne L. Rev. 2004 ,97.

Thomas James M., The Computer Fraud and Abuse Act: A Powerful Weapon vs. Unfair Competitors and Disgruntled Employees, In-House Defense Quarterly, Chicago, 2007.

Janet (UK), All-Party Internet Group enquiry into the Computer Misuse Act, 2004.

Mayer Jonathan, Cybercrime litigation, University of Pennsylvania Law Review, 164 U. Pa. L. Rev. 10521 ,1453, May. 2016.

Goldberg Mark, From Latvia, without love: EU-US cybercrime extradition in the global rights conversation, European Legal Studies Center, Columbia University, Columbia Journal of European Law, Spring, 21 ,2015 Colum. J. Eur. L. 329.

Vatis Michael A., The Council of Europe Convention on Cybercrime, a chapter in: Proceedings of a Workshop on Deterring Cyberattacks, Informing Strategies and Developing Options for U.S. Policy, The National Academic Press. Washington, D.C. 207 & ,2010.

Miquelon-Weismann, Miriam F., Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, Cuba, August -27September 335 & ,1990 ,7.

Miquelon-Weismann Miriam F., The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?, 23 J. Marshall J. Computer & Info. L. 2005 ,329.

Chawki Mohamed, Darwish Ashraf, Ayoub Khan Mohammad, and Tyagi Sapna, Cybercrime, Digital Forensics and Jurisdiction, Springer International Publishing Switzerland, 2015ed.

Perlroth Nicole, Fake Twitter Followers Become Multimillion-Dollar Business, The New York Times, April 5, p. 201.

Kerr Orin Samuel Vagueness Challenges to the Computer Fraud and Abuse Act, Minnesota Law Review, Vol. 94, Issue 2010 ,5.

Smith Russel, Grabosky Peter and Urbas George, Cyber Criminals on Trial, Cambridge University Press, Cambridge, 2004.

Schjolberg, Stein, the History of Cybercrime: 2014-1976, Volume 9, Cybercrime Research Institute GmbH, 2014.

UK hotel booking website fined after theft of payment card data, article posted on 25 October 2014. https://www.pcibooking.net/blog/uk-hotel-booking-website-fined-after-theft-payment-card-data, last visited 16 June 2018.

Amberhawk Training Limited, What lies beneath the extradition of hacker Gary McKinnon to the USA, 2009.

175,000£ fine for data breach, article posted Thursday October 2018 ,1, https://www.enterprisetimes.co.uk/01/10/2018/bupa-fined-175000-for-data-breach/, last visited 24 June 2019.

ثالثًا: المواقع الإلكترونية

1. الاتفاقيات والمواثيق الدولية التي صادقت عليها دولة قطر. http://qatar.smetoolkit.org
2. عالم التقنية. http://www.tech-wd.com
3. المجلس الاستشاري للقضاة في أوروبا عام 2010. http://www.coe.int/ccje
4. منظمة الكومونولث. http://thecommonwealth.org
5. شبكة قنوات الجزيرة. http://www.aljazeera.net
6. الميزان – مجموعة التشريعات والأحكام القطرية. http://www.almeezan.qa

7. بي بي سي. http://www.bbc.com
8. موقع إرم الإخباري. http://www.eremnews.com
9. أمن الإنترنت. http://www.securityfocus.com
10. سكاي نيوز. http://www.skynewsarabia.com
11. مكتب الأمم المتحدة لمكافحة المخدرات والجريمة. http://www.unodc.org
12. منظمة شرق غرب غير الحكومية. https://www.eastwest.ngo
13. الأحكام الإنجليزية. https://www.judiciary.gov.uk
14. جامعة أثاباسكا. www.athabascau.ca
15. مركز تكنولوجيا المعلومات الوطني – نيبال. http://www.nitc.gov.np
16. مركز تكنولوجيا المعلومات الوطني – إنجلترا. http://www.nitc.gov.np
17. اتحاد تكنولوجيا المعلومات العالمي. http://www.witsa.org
18. التشريعات الإنجليزية. www.legislation.gov.uk