



WWW.mecsaj.com/ar

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الابحاث العلمية و التربوية (MECSJ)

العدد الواحد والعشرون (كانون الثاني ) 2020

ISSN: 2617-9563

## الجهود الدولية لمكافحة جرائم الاتصالات International efforts to combat telecommunications crimes

الدكتور اينااس الزهراني  
استاذ مساعد - جامعه الامير سلطان - كلية القانون  
الرياض - المملكه العربيه السعوديه  
xxncexx7@gmail.com

### ملخص

في ظل التطورات التكنولوجية والرقمية في عالم الاتصالات وشبكات الإنترنت ظهرت العديد من المشكلات والتحديات التي بات يعاني منها الأفراد والمجتمعات، وتعتبر جرائم الانترنت والاتصالات من أخطر هذه التحديات وأكثرها أهمية وتأثيراً. مما دفع المجتمعات والدول إلى بذل العديد من الجهود في سبيل مكافحة هذا النوع من الجرائم. لذلك يسعى البحث الحالي إلى مناقشة الجهود الدولية المبذولة في سبيل مكافحة جرائم الاتصالات، بالإضافة إلى مناقشة الاتفاقيات الدولية في مكافحة جرائم الاتصالات. و التعرف على المخاطر المترتبة على وقوع جرائم الاتصالات. ولتحقيق أهداف البحث وللإجابة عن تساؤلاته التي تتمحور حول الجهود الدولية المبذولة في سبيل مكافحة جرائم الاتصالات، تم استخدام المنهج الوصفي الذي يتلائم مع طبيعة البحث.

وقد أكدت نتائج البحث على أن التشريعات والقوانين التقليدية بينت عدم قابلية تطبيقها على مرتكبي جرائم الاتصالات والإنترنت، فهي غير قادرة على تضمين كافة أشكال جرائم الاتصالات، كما تبين أن جرائم الإنترنت والاتصالات هي جرائم مبتكرة ومتسارعة تتسم بالتقنية، ولا تترك أثراً ملموساً ورائها، بالإضافة إلى وجود العديد من التحديات والصعوبات التي تحد من التعاون والتكافل الدولي في مكافحة جرائم الاتصالات والإنترنت. وفي ضوء النتائج التي توصل إليها البحث أوصى الباحث بمجموعة من التوصيات كان أبرزها: ضرورة عقد المؤتمرات والندوات التعريفية بمفهوم جرائم الاتصالات والإنترنت، على المستويين الإقليمي والدولي، ضرورة استحداث قسم أو جهة حكومية تعنى بجرائم الاتصالات والإنترنت ومكافحتها وملاحقة مرتكبيها، بالإضافة إلى ضرورة العمل على تعزيز العلاقات الدولية والتعاون الدولي في ملاحقة ومعاينة مرتكبي جرائم الاتصالات.

**الكلمات المفتاحية:** جرائم الاتصالات، التعاون الدولي، الجهود الدولية، مكافحة، الاتفاقيات، المعاهدات.



WWW.mecsj.com/ar

## Abstract

In the light of technological and digital developments in the world of telecommunications and the Internet, many problems and challenges have been experienced by individuals and communities. Cybercrime and communications are among the most serious and significant of these challenges. This has prompted communities and States to exert many efforts to combat this type of crime. Therefore; the present research seeks to discuss international efforts to combat telecommunications crimes. In addition to discussing international conventions in combating telecommunications crimes, and identify the risks of telecommunications crimes.

In order to achieve the objectives of the research and to answer its questions centered on the international efforts to combat telecommunications crimes, a descriptive approach was adopted that is appropriate to the nature of the research. The results of the research confirmed that the traditional laws have shown that they are not applicable to the perpetrators of communications networks and Internet crimes. Cybercrime and communications have also been shown to be innovative, accelerated, and technically. In addition, there are many challenges and difficulties that limit international cooperation in the fight against cybercrime. In light of the findings of the research, the researcher recommended a set of recommendations, the most important of which were: The necessity of holding conferences and seminars on the concept of telecommunications and Internet crimes, at the regional and international levels, the need to establish a government department or entity concerned with the crimes of telecommunications and the Internet and to combat and prosecute the perpetrators.

**Keywords:** Telecommunications, Internet, cybercrime, laws, networks.



## المقدمة

ساهم ظهور الإنترنت وتكنولوجيا الاتصالات في جعل العالم أشبه بقريّة صغيرة تتناقل فيها الأخبار والمعلومات بسرعة كبيرة في أي وقت ومن أي مكان، فقد عملت على إحداث الكثير من التغييرات والمستجدات في المجتمعات والدول. كما بات الحاسوب من المسلمات الأساسية للتعامل بين الأفراد والمنظمات والمؤسسات (الألفي، 2011)، مما أدى إلى زيادة التوجّه لاستخدام شبكات المعلومات والاتصالات الرقمية في الآونة الأخيرة، وذلك باعتبارها أداة اتصال دولية في كافة جوانب الحياة، بما يساهم في توفير سرعة عالية إلى جانب تقليل الوقت والجهد المبذول من قبل الأفراد، وعلى الرغم من الأهمية والفوائد الكثيرة التي قدمتها هذه التقنيات والتكنولوجيا، إلا أنها قادت إلى الكثير من المشاكل والمخاطر، فهي ساهمت في تقديم أشكالاً جديدة من الجرائم التي لم تعرف من قبل، والتي عُرفت بالجرائم الإلكترونية، أو جرائم الاتصالات (حسنية، 2017).

تمثل تكنولوجيا المعلومات والاتصالات (ICT) أحد أكثر التحديات الحديثة أهمية للأمن العالمي (دكداك و مصطفى، 2016)، كما وتنبأ تقييمات التهديدات بأن الأزمة الدولية الكبرى القادمة قد تكون بسبب قيام دولة أو جماعة إرهابية بتسليح تكنولوجيا المعلومات والاتصالات لتدمير البنية التحتية الحيوية أو شبكات اللوجستيات العسكرية، وأدى انتشار الحروب غير المتماثلة (أي النزاعات بين الأمم أو الجماعات التي لديها قدرات عسكرية متباينة) إلى زيادة استخدام الدول لتكنولوجيا المعلومات والاتصالات، مما يستلزم وضع مدونة دولية للسلوك السيبراني (الحوامدة، 2017).

والاعتقاد الخاطئ الشائع هو أن تهديدات الأمن السيبراني الرئيسية التي تتطلب تعاوناً دولياً عاجلاً هي الهجمات الكبيرة التي ترعاها الدولة والتي تستهدف البنية التحتية الحيوية مثل محطات توليد الكهرباء أو الشبكات الكهربائية، مما يسبب دماراً هائلاً وخسائر بشرية. في الواقع، تهديدات الإنترنت أكثر تنوعاً وتعقيداً، وغالباً ما تستهدف المؤسسات الخاصة وتعرض السلامة الفنية للعالم الرقمي للخطر، كما أن التحويل الرقمي شبه الكلي لنماذج الأعمال يجعل الاقتصاد العالمي أكثر عرضة للهجمات الإلكترونية، ليس فقط من الدول ولكن أيضاً من المنظمات الإجرامية وغيرها من الجهات الفاعلة غير الحكومية.

وفي الغالب يختار مجرمو الإنترنت والاتصالات العمل في بلدان بها قوانين ضعيفة أو غير موجودة تتعلق بمكافحة هذا الشكل من الجرائم؛ وذلك كمحاولة للتقليل من فرص الاكتشاف والمقاضاة.



## مشكلة البحث

مع التطورات والمستجدات التكنولوجية والتقنية التي بات يشهدها العالم في الآونة الأخيرة، وفي ظل ظاهرة العولمة التي باتت تغزو العالم، والتي أحدثت تأثيرات كبيرة في حياة الأفراد والمجتمعات، وعلى الرغم من الفوائد العظيمة التي تم تحقيقها إلا أنها أيضاً ساهمت في ابتكار أساليب ووسائل جديدة وتقنية في النشاط الإجرامي، ليصبح تهديداً عالمياً معقداً (حسنية، 2017). ففي الوقت الحالي باتت جرائم الاتصالات تهديداً أكبر من أي وقت مضى، وذلك بعد أن أصبح عدداً متزايداً من الأشخاص متصلين بالإنترنت عبر أجهزة الكمبيوتر المحمولة والهواتف الذكية والأجهزة اللوحية، وهي واحدة من أكثر الطرق ربحية لكسب المال في العالم الإجرامي. هناك مجموعة كبيرة ومتنوعة من جرائم الاتصالات، والتي يمكن وضعها على نطاق واسع في فئتين: جرائم لمرة واحدة، مثل تثبيت فيروس يسرق بياناتك الشخصية؛ والجرائم المستمرة مثل التسلط عبر الإنترنت أو الابتزاز أو توزيع المواد الإباحية عن الأطفال أو تنظيم هجمات إرهابية، وفي ضوء ذلك، اهتدى الباحث إلى إجراء هذا البحث في سبيل مناقشة الجهود الدولية المبذولة في مكافحة هذا النوع من الجرائم.

## أسئلة البحث

وتتمثل مشكلة البحث الحالي في الإجابة عن السؤال الرئيسي التالي:

❖ ما هي الجهود الدولية المبذولة في سبيل مكافحة جرائم الاتصالات؟

وينبثق من السؤال الرئيسي جملة من التساؤلات الفرعية، أهمها ما يلي:

- ما هي خصائص وسمات جرائم الاتصالات؟
- ما هي الاتفاقيات الدولية في مكافحة جرائم الاتصالات؟
- ما هي المخاطر المترتبة على وقوع جرائم الاتصالات؟
- ما هي التحديات والصعوبات التي تحد من مكافحة جرائم الاتصالات؟



## أهداف البحث

يسعى البحث الحالي إلى مناقشة الجهود الدولية المبذولة في سبيل مكافحة جرائم الاتصالات، كما سيسعى الباحث إلى تحقيق الأهداف التالية:

- دراسة خصائص وسمات جرائم الاتصالات.
- مناقشة الاتفاقيات الدولية في مكافحة جرائم الاتصالات.
- التعرف على المخاطر المترتبة على وقوع جرائم الاتصالات.
- تسليط الضوء على التحديات والصعوبات التي تحد من مكافحة جرائم الاتصالات.

## منهجية البحث

ولتحقيق أهداف البحث وللإجابة عن تساؤلاته التي تتمحور حول الجهود الدولية المبذولة في سبيل مكافحة جرائم الاتصالات، تم استخدام المنهج الوصفي الذي يتلائم مع طبيعة البحث، وذلك من خلال دراسة الأدبيات والدراسات السابقة التي تتعلق بموضوع البحث الحالي ومناقشتها وتحليلها، بالإضافة إلى مراجعة الاتفاقيات الدولية المتبعة في مكافحة جرائم الاتصالات والوقوف على مدى فاعليتها في الحد من هذه الجرائم.

## الدراسات السابقة

على الرغم من ندرة الدراسات والأدبيات التي تناولت مفهوم جرائم الاتصالات وفاعلية الجهود الدولية في مكافحتها، إلا أن الباحث قد تمكن من الوصول إلى عدد من الدراسات العربية والأجنبية التي تناولت في طياتها جانب أو أكثر من جوانب البحث الحالي، وفيما يلي سرد لهذه الدراسات:

هدفت دراسة الحوامدة (2017) التي كانت بعنوان "الجرائم المعلوماتية أركانها وألية مكافحتها – دراسة تحليلية مقارنة" إلى الكشف عن مفهوم الجرائم المعلوماتية وخصائصها ومميزاتها التي تميزها عن باقي الجرائم، بالإضافة إلى تسليط الضوء على أساليب مكافحتها وتقليصها، ولتحقيق ذلك تم استخدام المنهج المقارن والتحليلي للنصوص القانونية التي تعنى بمكافحة الجرائم الإلكترونية. وقد توصلت الدراسة إلى أن الجرائم الإلكترونية مثلها مثل باقي أشكال الجرائم يشترط توافر مجموعة من الأركان لحدوثها، كما توصلت أيضا إلى أن الدول سارعت في فرض تشريعات وأنظمة تتعلق بمكافحة الجرائم الإلكترونية.



أما دراسة حسنية (2017) التي كان عنوانها "الجريمة الإلكترونية بين الشرعية الجنائية والإجرائية" فقد هدفت إلى الكشف عن الأضرار والنتائج السلبية المترتبة على وقوع الجرائم الإلكترونية على الأفراد والمجتمعات، بالإضافة إلى مناقشة التحديات والعقبات التي تواجه المختصين والحكومات في مكافحة الجرائم الإلكترونية، ولتحقيق ذلك فقد تم استخدام المنهج الوصفي التحليلي المقارن. خرجت الدراسة بعدة نتائج أهمها أنّ المجتمع الفقهي لم يتفق على تعريف واحد جامع للجريمة الإلكترونية، كما أكد الباحث على أن النصوص القانونية التقليدية غير قابلة للتطبيق على الجرائم الإلكترونية.

بينما هدفت دراسة نصيرات (2015) التي كان عنوانها "الجهود الدولية في مكافحة الجرائم المعلوماتية والصعوبات التي تواجهها" إلى الكشف عن الجهود الدولية والإقليمية المتبعة في مكافحة الجرائم الإلكترونية، إلى جانب مناقشة الصعوبات والتحديات الدولية والإقليمية التي تواجه عملية مكافحة الجرائم الإلكترونية. ولتحقيق ذلك تم استخدام المنهج الوصفي التحليلي المقارن. وقد بينت النتائج أن نمو الجرائم الإلكترونية يتخطى الحدود الدولية، مما أدى إلى ظهور العديد من التحديات والصعوبات القانونية، أهمها صعوبة إثبات الجرائم الإلكترونية واكتشاف مرتكبيها كونها جرائم لا تخلف ورائها أثرا ملموسا. كما أكدت النتائج أنه من أهم هذه التحديات أيضا هي تنازع الاختصاص بشأن هذه الجرائم كونها جرائم لا تقتصر على حدود الدولة. وفي ضوء هذه النتائج أوصى الباحث بضرورة تكثيف الجهود الدولية في المنطقة العربية وإنشاء منظمة عربية تعنى بمكافحة هذا النوع من الجرائم.

وقد هدفت دراسة نعيم (2013) التي جاءت بعنوان "أليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري" إلى تسليط الضوء على وسائل التحقيق والكشف عن الجرائم الإلكترونية، إلى جانب التعرف على مدى تأثير الإنترنت وتكنولوجيا الاتصالات على الجريمة بمختلف أشكالها. ولتحقيق ذلك تم الاستعانة بالمنهج الوصفي المقارن والمنهج التحليلي والمنهج التأصيلي، وقد أكدت النتائج على أن مفهوم الجرائم الإلكترونية يشير إلى الأفعال والتصرفات التي تصدر من الفرد اعتداء على أنظمة المعالجة الرقمية، للوصول إلى معلومات سرية وخاصة تتعلق بأفراد أو مؤسسات معينة، كما توصلت النتائج إلى قصور في النصوص القانونية في فرض العقوبات الرادعة على مثل هذا النوع من الجرائم، حيث أن النصوص القانونية للعقوبات تطبق على الجرائم ذات الطابع المادي والملموس.



بينما هدفت دراسة الألفي (2011) والتي كان عنوانها "التعاون الدولي في مجال مكافحة المخدرات عبر الفضاء المعلوماتي" إلى مناقشة الجهود الدولية المبذولة في مكافحة الجرائم التي تحدث من خلال الانترنت وخاصة جرائم المخدرات، بالإضافة إلى تسليط الضوء على الاتفاقيات التي قامت الدول بعقدتها في سبيل مكافحة الجرائم الإلكترونية، وقد توصلت الدراسة إلى وجود أوجه قصور في مكافحة الجرائم الإلكترونية في الدول العربية وذلك بسبب قلت الإمكانيات والتجهيزات التقنية والفنية المتطورة اللازمة لمكافحة هذا النوع من الجرائم.

### أولاً: ماهية جرائم الاتصالات

يطلق مصطلح جرائم الاتصالات أو الإنترنت أو ما يعرف بالجرائم الإلكترونية على أي نشاط إجرامي ينطوي على جهاز كمبيوتر أو جهاز متصل بشبكة الإنترنت (المطوع، 2011)، والتي يتم تنفيذها من أجل تحقيق ربح لمجرمي الإنترنت. إذ يتم تنفيذ بعض الجرائم الإلكترونية ضد أجهزة الكمبيوتر أو الأجهزة مباشرة لتلفها أو تعطيلها، بينما يستخدم آخرون أجهزة الكمبيوتر أو الشبكات لنشر البرامج الضارة أو المعلومات غير القانونية أو الصور أو مواد أخرى، كما تقوم بعض الجرائم الإلكترونية - على سبيل المثال - باستهداف أجهزة الكمبيوتر لإصابتها بالفيروسات، التي تنتشر بعد ذلك إلى أجهزة أخرى، وأحياناً إلى شبكات كاملة (الصاعدي، 2010).

وبالتالي يمكننا القول بأن جرائم الإنترنت والاتصالات هي أي نشاط إجرامي يتم تنفيذه باستخدام أجهزة الكمبيوتر أو الإنترنت، وذلك من خلال استخدام مجموعة من الأدوات الرقمية مثل الخداع والفيروسات وبرامج التجسس والمراقبة وغيرها من الأدوات غير القانونية. وقد يتم تنفيذ النشاط الإجرامي عبر الإنترنت وتكنولوجيا الاتصالات من قبل أفراد أو مجموعات صغيرة ذات مهارة تقنية قليلة نسبياً، أو بواسطة مجموعات إجرامية عالمية عالية التنظيم قد تشمل مطورين ماهرين وغيرهم من ذوي الخبرة ذات الصلة.



## ثانياً: الاتفاقيات الدولية المبرمة لمكافحة جرائم الاتصالات

وفي ظل التطورات والتقنيات والأساليب الجديدة التي يتم اكتشافها وتصميمها في عالم جرائم الاتصالات والإنترنت، أصبحت القوانين والأنظمة القضائية التي يتم تطبيقها في الدول في سبيل مكافحة جرائم الاتصالات من الأساليب غير الفعالة في محاربة هذا النوع من الجرائم، ويرجع ذلك إلى أن هذا النوع من الجرائم بات لا يقتصر على مجتمع أو دولة معينة بل أصبح يتسم بأنه يتخطى الحدود الجغرافية، حيث يمكن للمجرم الإلكتروني على شبكة الاتصالات والإنترنت أن يقوم بعملية إجرامية في حق الآخرين من الأفراد والمؤسسات و المجتمعات باختلاف مواقعهم ومهما كانت المسافة الجغرافية التي تفصلهم عنه، وبالتالي كان من الضروري التعاون الدولي وبذل الجهود الدولية والإقليمية للعمل على مكافحة هذا الشكل من الجرائم.

وبذلك بدأت المطالبات بفرض القوانين والعقوبات القانونية المترتبة على ارتكاب الجرائم التي تتعلق بتكنولوجيا الاتصالات والمعلومات وشبكات الإنترنت، وبالتالي بدأت الحكومات تدرك مدى خطورة الجرائم المرتبطة بتكنولوجيا الاتصالات والمعلومات، إلى جانب إدراك مدى تفاقمها وسرعة انتشارها وتطورها. مما دعى الدول إلى استحداث قوانين وتشريعات جديدة يمكن من خلالها مكافحة جرائم الاتصالات. بالإضافة إلى مراعاة أن هذه الجرائم تتسم بأنها تتخطى الحدود الدولية. التي أدت إلى قيام الدول بعقد المعاهدات والاتفاقيات الدولية التي تتعلق بمكافحة جرائم الاتصالات والمعلومات. ومن من أبرز هذه الاتفاقيات ما يلي (نصيرات، 2015):

### 1. الاتفاقية الأوروبية لمكافحة جرائم الاتصالات والإنترنت:

وفي ضوء الالتطورات والتغيرات المتسارعة في العالم الرقمي اتفقت الدول الأوروبية على ضرورة إعادة النظر في الإجراءات والقوانين الجنائية المتبعة في مجال الاتصالات وجرائم الإنترنت. حيث قام المجتمع الأوروبي بإصدار عدد من التوصيات في هذا المجال، كما قامو بالاتفاق على إتفاقية سمية بالاتفاقية الأوروبية لمكافحة جرائم الاتصالات والإنترنت (العبيدي، 2015)، و وقد ألزمت هذه الاتفاقية الدول الموقعة عليها بفرض الحد الأدنى من التشريعات والقوانين اللازمة لتعامل مع جرائم الاتصالات والإنترنت، بما يشمل أيضا الدخول غير القانوني على الشبكات والتلاعب ببياناتها، والتزوير والاحتيايل التي تتم باستخدام شبكات الانترنت والاتصالات،



كما شملت أيضا سرقة المحتوى الرقمي وانتهاك حقوق النشر، والمنشورات غير الأخلاقية ونشر المحتوى الإباحي على الإنترنت وشبكات الاتصالات (نصيرات، 2015). وهي أول معاهدة دولية بشأن الجرائم المرتكبة عبر الإنترنت وشبكات الكمبيوتر الأخرى، وتتناول بشكل خاص انتهاكات حقوق الطبع والنشر والاحتيايل المرتبط بالحاسوب واستغلال الأطفال في المواد الإباحية وانتهاكات أمن الشبكات، ويحتوي أيضا على سلسلة من الصلاحيات والإجراءات مثل البحث عن شبكات الكمبيوتر والاعتراض، والتي كان هدفها الرئيسي هو اتباع سياسة تجريرية مشتركة تهدف إلى حماية المجتمع من الجريمة السيبرانية، وخاصة من خلال اعتماد التشريعات المناسبة وتعزيز التعاون الدولي.

## 2. معاهدة بودابست لعام 2001:

وقد تم توقيع هذه المعاهدة في عام (2001)، كوسيلة فعالة في مواجهة الجرائم الإلكترونية والاتصالات، فهي تعتبر أول اتفاقية دولية شاملة تعنى بجرائم الاتصالات، وقد هدفت هذه الاتفاقية إلى التكاتف والتعاون الدولي في مكافحة جرائم الإنترنت والاتصالات، إلى جانب العمل على تقليصها والحد من انتشارها (العبيدي، 2015). وبالتالي منع أي فعل يمس بسرية ومصداقية المعلومات والبيانات المتوافرة على شبكات الانترنت والاتصالات، إلى جانب فرض عدد من الإجراءات المرتبطة بمكافحة هذه الجرائم. حيث أكدت هذه المعاهدة على أهمية فرض الأنظمة والتشريعات الدولية لمواجهة جرائم الاتصالات وتقليصها، إلى جانب العمل على كشف المخاطر المترتبة على وقوع هذه الجرائم. بالإضافة إلى اهتمامها بالتأكد من كشف وملاحقة مرتكبي جرائم الاتصالات والانترنت، وتوفير أنظمة للتحقيق والتحري والمحاكمة إلى جانب الأخذ بعين الاعتبار ضرورة التعاون المحلي والإقليمي والدولي (نصيرات، 2015).

وبالتالي تعتبر هذه المعاهدة الصك الدولي الأهم والملزم بشأن مكافحة جرائم الاتصالات وشبكات الإنترنت، إنها بمثابة مبدأ توجيهي لأي بلد يطور تشريعات وطنية شاملة لمكافحة جرائم الإنترنت وكإطار للتعاون الدولي بين الدول الأطراف في هذه المعاهدة.



### 3. مؤتمر الفضاء الإلكتروني (cyber space) لعام 2011.

بدأت لندن مؤتمراً دولياً لمدة يومين يركز على تهديد هجمات الأمن السيبراني، اجتمع ممثلون عن 60 دولة لمناقشة كيفية معالجة المستويات المتزايدة للجرائم الإلكترونية. عقد وزير الخارجية وليام هيغ مؤتمر لندن حول الفضاء الإلكتروني، وحث على "استجابة منسقة عالمية" بشأن السياسة (دكداك و مصطفى، 2016).

وهو مؤتمر عقد في مدينة لندن في عام (2011) شاركت به العديد من الحكومات والمؤسسات والشركات الدولية غير الحكومية، وقد أشترك بهذا المؤتمر أكثر من 60 دولة من الدول المتقدمة والنامية؛ كالولايات الأمريكية المتحدة والصين وروسيا ودول الاتحاد الأوروبي وغيرها. وقد سعى هذا المؤتمر إلى تعزيز فهم مشترك شامل لأساليب ووسائل تحقيق أعلى درجات الحماية للفضاء الرقمي (العبيدي، 2015).

وقد ركز مؤتمر لندن حول الفضاء الإلكتروني ضرورة أن تتصرف الحكومات بشكل متناسب في الفضاء الإلكتروني ووفقاً للقانون الوطني والدولي، كما أكد على حاجة الجميع إلى امتلاك القدرة من حيث المهارات والتكنولوجيا والثقة والفرصة على الوصول إلى الفضاء الإلكتروني، وحاجة مستخدمي الفضاء الإلكتروني إلى إظهار التسامح واحترام تنوع اللغة والثقافة والأفكار، وضمان بقاء الفضاء الإلكتروني مفتوحاً أمام الابتكار والتدفق الحر للأفكار والمعلومات والتعبير، بالإضافة إلى الحاجة لاحترام الحقوق الفردية للخصوصية وتوفير الحماية المناسبة للملكية الفكرية، وضرورة أن نعمل جميعاً بشكل جماعي للتصدي للتهديد من المجرمين الذين يتصرفون عبر الإنترنت، إلى جانب الترويج لبيئة تنافسية تضمن عائداً عادلاً للاستثمار في الشبكة والخدمات والمحتوى.

#### ثالثاً: الصعوبات والتحديات التي تحد من التعاون الدولي في مكافحة جرائم الإنترنت والاتصالات.

وعلى الرغم من الجهود والمعاهدات والاتفاقيات الدولية التي تم عقدها وتطبيقها في بعض الدول، إلا أن هنالك عدد من التحديات والصعوبات التي تحد من تكثيف الجهود الدولية في مكافحة جرائم المعلومات والاتصالات، وفيما يلي بعض أبرز هذه التحديات (العبيدي، 2015):



- عدم التوصل إلى مفهوم موحد وشامل لجرائم الإنترنت والاتصالات، وهذا بسبب أن الأفعال الجرمية على شبكات الاتصالات والإنترنت لا تخضع جميعها للأنظمة والتشريعات الدولية المتفق عليها. فهذا النوع من الجرائم يتخذ نماذج وصور كثير ومبتكرة لا يمكن تضمينها جميعها بالتشريعات والقوانين الدولية.
- قصور التعاون الدولي بما يتعلق بالعقوبات الجنائية. حيث أننا نعاني من قلت التنسيق بالعقوبات الجنائية، وخاصة فيما يتعلق بالتعقب والتحقيق.
- اختلاف والتنوع في الأنظمة والتشريعات القانونية الإجرائية. فإن التنوع والاختلاف في القوانين والتشريعات الجنائية يؤثر في عملية ملاحقة مرتكبي الجرائم على شبكات الاتصالات والإنترنت. فقد نجد أن هنالك بعض القوانين التي تثبت فعاليتها وأهميتها في مكافحة مثل هذا النوع من الجرائم في بلد ما لا يتلائم مع بلد آخر.
- مشكلات تنازع الاختصاص القضائي، تثير جرائم الاتصالات مسألة الاختصاص على المستوى الدولي. ويرجع ذلك إلى الاختلاف في طبيعة وشكل جرائم الاتصالات وكونها تتخطى الحدود الدولية والجغرافية. فبإمكان شخص ما يوجد في بلد معين ارتكاب جريمة رقمية في حق شخص آخر أو مؤسسة ما في بلد آخر.
- عدم توافر قنوات اتصال بين الدول، وهذا يؤدي إلى عرقلة عملية مكافحة جرائم الاتصالات والإنترنت. وبالتالي فإنه لنجاح عملية مكافحة الجرائم الإلكترونية وجرائم الاتصالات يجب تحسين العلاقات والاتصالات الدولية، وذلك للسماح للجهات المعنية والمسؤولة عن التحقيق بمثل هذه الجرائم بسهولة ويسر.
- قلت المعاهدات الثنائية أو الجماعية بين الدول، وعدم فاعليتها في توفير الحماية المطلوبة في ظل التطورات والتغيرات التكنولوجية الجديدة والمبتكرة والمتسارعة في عالم الإجرام الرقمي.



## رابعاً: الآثار المترتبة على جرائم الاتصالات

إن انتشار جرائم الاتصالات والإنترنت بين الأفراد والمُجتمعات أدى إلى ظهور العديد من المخاطر والتهديدات، كالتحديات الاقتصادية ومخاطر الأمن الوطني، المساس بالاقتصاد والأمن الوطني وتهديده المساس بالعلاقات الأسرية وتشكيل الخلافات بين أفراد الأسرة مما يؤدي إلى التفكك الأسري، وذلك بسبب الكثير من النتائج التي تُسببها بعض أنواع الجرائم الإلكترونية كالتشهير ببعض الأفراد ونشر الأخبار الكاذبة والإشاعات.

من الآثار الرئيسية للجرائم الإلكترونية تأثير مالي، ويمكن أن تشمل الجرائم الإلكترونية العديد من أنواع الأنشطة الإجرامية المدفوعة بالربح، بما في ذلك هجمات الفدية والبريد الإلكتروني والاحتيال عبر الإنترنت والاحتيال في الهوية ، بالإضافة إلى محاولات سرقة الحساب المالي أو بطاقة الائتمان أو معلومات بطاقة الدفع الأخرى. قد يستهدف مجرمو الإنترنت المعلومات الشخصية الخاصة، فضلاً عن بيانات الشركات المتعلقة بالسرقة وإعادة البيع.

## النتائج والتوصيات

ومن خلال مراجعة الأدبيات والدراسات والمستندات التي تعلق بجرائم الاتصالات والإنترنت، والجهود والمواثيق الدولية التي ترتبط بهذا الموضوع، فقد تمكن الباحث من الوصول إلى عدد من النتائج كان من أبرزها ما يلي:

- إن التشريعات والقوانين التقليدية بينت عدم قابلية تطبيقها على مرتكبي جرائم الاتصالات والإنترنت، فهي غير قادرة على تضمين كافة أشكال جرائم الاتصالات.
- وقد تبين أن جرائم الإنترنت والاتصالات هي جرائم مبتكرة ومتسارعة تتسم بالتقنية، ولا تترك أثراً ملموساً ورائها.
- باتت الجرائم الرقمية والاتصالات واقع مفروضاً على الأفراد والمجتمعات يجب التعامل معه ومعالجته.
- تعتبر جرائم الإنترنت والاتصالات من الأزمات الكبيرة التي تعاني منها دول العالم أجمع.
- تتسم جرائم الإنترنت والاتصالات بأنها جرائم عابرة للحدود الإقليمية والدولية.



- تم عقد العديد من الاتفاقيات والمعاهدات الدولية فيما يتعلق بمكافحة جرائم الاتصالات وشبكات الإنترنت، وملاحقة مرتكبيها ومعاقبتهم.
- هنالك العديد من التحديات والصعوبات التي تحد من التعاون والتكافل الدولي في مكافحة جرائم الاتصالات والإنترنت.
- تقتصر الدول العربية بشكل خاص على القوانين والتشريعات الرادعة لجرائم الاتصالات والإنترنت.

**وفي ضوء النتائج التي توصل إليها البحث، أوصى الباحث بمجموعة من التوصيات التي تعزز مكافحة جرائم الاتصالات والإنترنت، وكان من أبرزها ما يلي:**

- ضرورة عقد المؤتمرات والندوات التعريفية بمفهوم جرائم الاتصالات والإنترنت، على المستويين الإقليمي والدولي.
- ضرورة استحداث قسم أو جهة حكومية تعنى بجرائم الاتصالات والإنترنت ومكافحتها وملاحقة مرتكبيها.
- ضرورة العمل على إجراء المزيد من الدراسات والأبحاث العربية التي تتعلق بجرائم الاتصالات والجهود الدولية المبذولة في مكافحتها.
- العمل على تعزيز العلاقات الدولية والتعاون الدولي في ملاحقة ومعاقبة مرتكبي جرائم الاتصالات.
- تعزيز التعاون المشترك بين دول العالم العربي فيما يتعلق بمكافحة جرائم الاتصالات والإنترنت.



WWW.mecsaj.com/ar

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الابحاث العلمية و التربوية (MECSJ)

العدد الواحد والعشرون (كانون الثاني ) 2020

ISSN: 2617-9563

## قائمة المراجع

- الألفي، محمد محمد. (2011). *التعاون الدولي في مجال مكافحة المخدرات عبر الفضاء المعلوماتي. الجمعية العربية للتحكيم الإلكتروني.*
- الحوامدة، لورنس سعيد. (2017). *الجرائم المعلوماتية أركانها وألية مكافحتها – دراسة تحليلية مقارنة. جامعة طيبة ، كلية الحقوق ، المملكة العربية السعودية.*
- الصاعدي، محمد. (2010). *جرائم الإنترنت وجهود المملكة العربية السعودية في مكافحتها. أعمال ندوات: مكافحة الجريمة عبر الإنترنت - وورشة عمل: أمن المعلومات والتوقيع الإلكتروني. المملكة العربية السعودية: المنظمة العربية للتنمية الإدارية .*
- العبيدي. أسامة بن غانم. (2015). *الجهود الدولية لمكافحة الجرائم المعلوماتية. مجلة الحقوق، المجلد 39 (العدد الرابع). تم الاسترداد من*  
[file:///C:/Users/user1/AppData/Local/Temp/Rar\\$DIa0.112/0318-039-004-003.pdf](file:///C:/Users/user1/AppData/Local/Temp/Rar$DIa0.112/0318-039-004-003.pdf)
- المطوع، عبدالله بن محمد. (2011). *الاحتساب الإلكتروني في المملكة العربية السعودية على الجرائم الأخلاقية في شبكة المعلومات الدولية - الإنترنت. جامعة الإمام محمد بن سعود الإسلامية ، قسم الدعوة والاحتساب - كلية الدعوة والإعلام، المملكة العربية السعودية.*
- حسنية، حمد أسامة. (2017). *الجريمة الإلكترونية بين الشريعة الجنائية والإجرائية. مجلة جامعة الأزهر - غزة، المجلد 19. تم الاسترداد من*  
<file:///C:/Users/user1/Downloads/criminal.pdf>
- دكداك، صلاح الدين ؛ مصطفى، عائشة بن قارة. (2016). *الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية. مجلة الفقه والقانون (العدد 42).*



- نصيرات، وائل محمد عبدالرحمن. (2015). الجهود الدولية في مكافحة الجرائم المعلوماتية والصعوبات التي تواجهها. جامعة الإمام محمد بن سعود الإسلامية ، كلية علوم الحاسب والمعلومات. الرياض، المملكة العربية السعودية: المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية ICACC. تم الاسترداد من-file:///C:/Users/user1/AppData/Local/Temp/Rar\$DIa0.424/7025-000-000-011x.pdf
- نعيم ، سعداني. (2013). آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري. جامعة الحاج لخضر - باتنه ، كلية الحقوق والعلوم السياسية. الجمهورية الجزائرية: وزارة التعليم العالي والبحث العلمي . تم الاسترداد من file:///C:/Users/user1/Downloads/dr%20%D8%B3%D8%B9%D9%8A%D8%AF%D8%A7%D9%86%D9%8A%20%D9%86%D8%B9%D9%8A%D9%85.pdf