ISSN: 2663-5798 || Arab Journal for Scientific Publishing

المجلد التاسع – العدد التسعون
تاريخ الإصدار: 2 – نيسان – 2026م
www.ajsp.net

"الجرائم الإلكترونية وأثارها على الأمن والاقتصاد الوطنيين"

(بحث مستل من أطروحة دكتوراه في القانون العام)

إعداد الباحث:

عايد غازي جبر الخفاجي

الجامعة الاسلامية في لبنان – كلية الحقوق والعلوم السياسية – قسم القانون العام

بإشراف: الاستاذ الدكتور كمال حماد

Received: 24/02/2026 | Revised: 25/02/2026 | Accepted: 31/03/2026 | Published: 02/04/2026

Abstract:

The rapid development of information and communication technologies has led to the emergence of new forms of crime known as cybercrime, which relies on digital tools and online networks to commit illegal activities. Cybercrime has become a serious threat to public security and national economic stability due to its ability to target critical infrastructure, financial systems, and sensitive data. The transnational nature of cybercrime, combined with the challenges of detection and prosecution, increases its impact on both security and economic sectors.

This research aims to analyze the impact of cybercrime on public security and the national economy, highlighting legal and security challenges associated with it. It also examines legislative and preventive frameworks required to combat cyber threats effectively. Furthermore, the study proposes strategies to enhance legal and technological protection mechanisms in order to balance digital transformation with public safety and economic resilience.

Keywords: Cybercrime, Public Security, National Economy, Cybersecurity, Digital Crime, Criminal Legislation

ملخص البحث

شهد العالم خلال العقود الأخيرة تطوراً متسارعاً في تكنولوجيا المعلومات والاتصالات، مما أسهم في ظهور أنماط جديدة من الجرائم تُعرف بالجرائم الإلكترونية، والتي تعتمد على استخدام الوسائل الرقمية والشبكات المعلوماتية لارتكاب أفعال غير مشروعة. وقد باتت هذه الجرائم تشكل تهديداً حقيقياً للأمن العام والاستقرار الاقتصادي للدول، نظراً لقدرتها على استهداف البنى التحتية الحيوية، والأنظمة المالية، والبيانات الشخصية والمؤسسية. وتبرز خطورة الجرائم الإلكترونية في طابعها العابر للحدود وصعوبة اكتشافها وتتبع مرتكبيها، فضلاً عن الأضرار الاقتصادية المباشرة وغير المباشرة التي تُلحقها بالاقتصاد الوطني، مثل الاحتيال المالي، وسرقة الملكية الفكرية، وتعطيل الخدمات الرقمية.

يهدف هذا البحث إلى تحليل أثر الجرائم الإلكترونية على الأمن العام والاقتصاد الوطني، وبيان التحديات القانونية والأمنية المرتبطة بها، مع دراسة الأطر التشريعية والوقائية اللازمة لمكافحتها. كما يسعى البحث إلى تقديم رؤية تحليلية حول سبل تعزيز الحماية القانونية والتقنية، بما يحقق التوازن بين التطور الرقمي وضمان الأمن المجتمعي والاستقرار الاقتصادي.

الكلمات المفتاحية: الجرائم الإلكترونية. الأمن العام. الاقتصاد الوطني. الأمن السيبراني. الجرائم الرقمية. التشريعات الجنائية.

How to Cite This Article

الخفاجي، ع. غ. ج. (2026). الجرائم الإلكترونية وآثارها على الأمن والاقتصاد الوطنيين. *المجلة العربية للنشر العلمي(AJSP)* ، 9(90)، (549 -564).

المجلد التاسع – العدد التسعون
تاريخ الإصدار: 2 – نيسان – 2026م
www.ajsp.net

ISSN: 2663-5798 || Arab Journal for Scientific Publishing

المقدمة:

شهدت المجتمعات المعاصرة تحولاً جذرياً نتيجة الثورة الرقمية والتطور السريع في تقنيات الاتصالات والمعلومات، الأمر الذي أدى إلى توسع استخدام الفضاء الإلكتروني في مختلف المجالات الاقتصادية والاجتماعية والإدارية. إلا أن هذا التطور لم يخلُ من تحديات أمنية وقانونية، إذ أفرز أنماطاً جديدة من الجرائم تعتمد على التقنيات الرقمية، عُرفت بالجرائم الإلكترونية. وتمتاز هذه الجرائم بخصائص تجعلها أكثر تعقيداً من الجرائم التقليدية، مثل سرعة التنفيذ، وإخفاء الهوية، والطابع العابر للحدود.

وأصبحت الجرائم الإلكترونية تشكل تهديداً متزايداً للأمن العام لما قد تسببه من اختراقات للأنظمة الحكومية والمؤسسات الحيوية، فضلاً عن تأثيراتها السلبية على الاقتصاد الوطني من خلال عمليات الاحتيال الإلكتروني والهجمات على البنية التحتية الرقمية. ومن هنا برزت الحاجة إلى دراسة تحليلية معمقة لبيان أثر هذه الجرائم، وتقييم فعالية التشريعات والسياسات الوطنية والدولية في مواجهتها.

أولاً: إشكالية البحث

1. في ظل التطور التقني المتسارع الذي يتجاوز في كثير من الأحيان قدرة الأنظمة القانونية التقليدية على المواكبة، تتصاعد معدلات الجرائم الإلكترونية واتساع نطاقها، مما تؤثر بشكل اساسي على الأمن العام والاقتصاد الوطني. لذلك فأن الإشكالية الرئيسية للبحث هي، **ما مدى كفاية الأطر التشريعية الحالية في مواجهة الجرائم الرقمية، وهل تستطيع المؤسسات الأمنية والاقتصادية على الحد من آثارها السلبية.**

ثانياً: اهمية البحث

تكمن أهمية البحث في أن الجرائم الإلكترونية أصبحت من أبرز التهديدات المعاصرة التي تواجه الدول، لما لها من آثار مباشرة على استقرار المجتمع وحماية المصالح الاقتصادية. كما أن تزايد الاعتماد على الاقتصاد الرقمي والخدمات الإلكترونية يجعل الدول أكثر عرضة للهجمات السيبرانية، الأمر الذي يفرض ضرورة تطوير استراتيجيات قانونية وأمنية متكاملة لمواجهتها.

ثالثاً: أهداف البحث

تحليل مفهوم الجرائم الإلكترونية وخصائصها القانونية.

دراسة أثر الجرائم الإلكترونية على الأمن العام.

بيان التأثيرات الاقتصادية للجرائم الإلكترونية على الاقتصاد الوطني.

تقييم فعالية التشريعات والسياسات في مكافحة الجرائم الإلكترونية.

اقتراح حلول قانونية وتقنية لتعزيز الأمن السيبراني.

رابعاً: منهجية البحث

يعتمد البحث على المنهج التحليلي لدراسة النصوص القانونية المتعلقة بالجرائم الإلكترونية، والمنهج الوصفي لبيان طبيعة هذه الجرائم وآثارها، إضافة إلى المنهج المقارن عند الحاجة لمقارنة التجارب التشريعية المختلفة في مكافحة الجرائم السيبرانية.

وسنقسم البحث الى مطلبين: المطلب الأول بعنوان: **أثر الجرائم الإلكترونية على الامن والاقتصاد الوطني،**

والمطلب الثاني بعنوان: أثر الجرائم الإلكترونية على النظام المالي العالمي والمحلي،

المطلب الأول بعنوان: أثر الجرائم الإلكترونية على الامن والاقتصاد الوطني

أصبحت الجرائم الإلكترونية من أخطر الظواهر الإجرامية التي فرضتها الثورة الرقمية والتطور المتسارع في تقنيات المعلومات والاتصالات، حيث لم يعد الإجرام محصورًا في الإطار التقليدي، بل انتقل إلى الفضاء الإلكتروني مستهدفًا الأفراد والمؤسسات والدول على حد سواء. وقد أدى هذا التحول إلى بروز أنماط جديدة من السلوك الإجرامي تعتمد على استغلال الأنظمة المعلوماتية والشبكات الرقمية، مما جعل من الجرائم الإلكترونية تهديدًا حقيقيًا للأمن العام والاستقرار الاقتصادي في المجتمعات المعاصرة[1].

إن خطورة الجرائم الإلكترونية تكمن في طبيعتها غير الملموسة وسهولة ارتكابها وصعوبة اكتشافها، فضلًا عن كونها غالبًا ما تتجاوز الحدود الجغرافية للدول، الأمر الذي يعقّد من جهود المكافحة القانونية والأمنية. فالمجرم الإلكتروني يستطيع تنفيذ فعله الإجرامي من أي مكان في العالم دون الحاجة إلى التواجد المادي في مسرح الجريمة، مما يضعف فعالية الوسائل التقليدية للتحقيق والملاحقة الجنائية[2]. وقد ساهم هذا الواقع في إحداث اختلالات واضحة في مفهوم الأمن العام، الذي لم يعد مقتصرًا على حماية الأرواح والممتلكات المادية، بل امتد ليشمل حماية الفضاء الرقمي والبنية التحتية المعلوماتية للدولة.

ويُعد الأمن العام من الركائز الأساسية لاستقرار الدولة، إذ يؤدي أي مساس به إلى زعزعة ثقة الأفراد بالمؤسسات العامة والخاصة. وتُظهر الجرائم الإلكترونية، ولا سيما تلك التي تستهدف قواعد البيانات الحكومية أو الأنظمة الأمنية، أثرًا بالغ الخطورة يتمثل في تسريب المعلومات الحساسة أو تعطيل الخدمات الحيوية، الأمر الذي قد يفضي إلى اضطرابات اجتماعية وأمنية تمس النظام العام بصورة مباشرة[3]. كما أن انتشار هذا النوع من الجرائم يعزز الشعور بعدم الأمان الرقمي لدى المواطنين، ويؤثر سلبًا في الاستخدام الآمن للتكنولوجيا الحديثة.

ومن ناحية أخرى، يبرز الأثر الاقتصادي للجرائم الإلكترونية بوصفه أحد أخطر انعكاساتها، حيث تتسبب هذه الجرائم بخسائر مالية جسيمة نتيجة عمليات الاحتيال الإلكتروني، وسرقة الأموال، وانتهاك الملكية الفكرية، إضافة إلى تكاليف إصلاح الأنظمة المتضررة

---

[1] محمود أحمد القرعان، الجرائم السيبرانية، الطبعة الأولى ،دار وائل للنشر والتوزيع، عمان، ، 2017، ص 11.

[2] أحمد فتحي سرور، الوسيط في قانون العقوبات – القسم الخاص، دار الشروق، القاهرة، 2016، ص 214.

[3] عبد الفتاح بيومي حجازي، الجريمة المعلوماتية في التشريع المقارن، دار النهضة العربية، القاهرة، 2010، ص 45.

وتعزيز إجراءات الحماية السيبرانية[4]. كما تؤثر الجرائم الإلكترونية على ثقة المستثمرين في البيئة الاقتصادية للدولة، إذ يؤدي ضعف الحماية القانونية والتقنية إلى عزوف رؤوس الأموال عن الاستثمار في الاقتصاد الرقمي، مما يعرقل جهود التنمية الاقتصادية ويحد من فرص النمو.

ولا يقف تأثير الجرائم الإلكترونية عند حدود الخسائر المالية المباشرة، بل يمتد ليشمل الإضرار بسمعة المؤسسات المالية والتجارية، وتقويض الثقة في المعاملات الإلكترونية، وهو ما ينعكس سلبًا على الاقتصاد الوطني ككل[5]. كما أن توسع نطاق هذه الجرائم يفرض أعباءً إضافية على الدولة لتطوير تشريعاتها الجنائية وتدريب كوادر متخصصة قادرة على مواجهة هذا النوع المستحدث من الإجرام.

وعليه، فإن دراسة أثر الجرائم الإلكترونية على الأمن الوطني تكتسب أهمية بالغة، لما لها من دور في تسليط الضوء على المخاطر المتنامية لهذه الجرائم، وبيان الحاجة الملحة إلى تبني سياسات تشريعية وأمنية متكاملة تضمن حماية المجتمع والدولة في العصر الرقمي. وسوف نقسم هذا البحث الى مطلبين الأول أثر الجرائم الالكترونية على الاقتصاد الوطني، اما الثاني أثر الجرائم الالكترونية على الامن العام.

الفرع الأول: أثر الجرائم الإلكترونية على الاقتصاد الوطني

أدى التطور المتسارع في تقنيات المعلومات والاتصالات إلى إحداث تحولات جوهرية في بنية الاقتصاد الوطني، حيث أصبحت الأنشطة الاقتصادية تعتمد بدرجة متزايدة على الوسائل الإلكترونية في إنجاز المعاملات التجارية والمالية والإدارية. غير أن هذا التحول الرقمي، رغم ما يوفره من مزايا، أفرز في المقابل تحديات خطيرة تمثلت في تنامي ظاهرة الجرائم الإلكترونية، التي باتت تشكل تهديدًا حقيقيًا للاقتصاد الوطني ومقوماته الأساسية. فالجرائم الإلكترونية لم تعد مجرد أفعال فردية معزولة، بل أصبحت نشاطًا إجراميًا منظمًا يستهدف البنية الاقتصادية للدولة ويؤثر في استقرارها المالي[6].

وتتمثل أبرز آثار الجرائم الإلكترونية على الاقتصاد الوطني في الخسائر المالية المباشرة التي تلحق بالمؤسسات والأفراد نتيجة جرائم الاحتيال الإلكتروني، وسرقة الحسابات المصرفية، واختراق الأنظمة البنكية والتجارية. إذ تؤدي هذه الجرائم إلى تحويل الأموال بطرق غير مشروعة، أو الاستيلاء عليها دون وجه حق، مما ينعكس سلبًا على الدورة الاقتصادية ويضعف الثقة في النظام المالي للدولة[7]. كما تتحمل المؤسسات المتضررة أعباء مالية إضافية تتمثل في تكاليف استعادة الأنظمة المتضررة وتعويض المتضررين، فضلًا عن تكاليف تعزيز نظم الحماية الإلكترونية.

---

[4] محمد صبري السعدي، الحماية الجنائية لنظم المعلومات، دار الفكر الجامعي، الإسكندرية، 2015، ص 88.

[5] حسن علي الذنون، الجرائم الإلكترونية وأثرها على الاقتصاد الوطني، دار الثقافة للنشر والتوزيع، عمان، 2019، ص 132.

[6] محمود أحمد القرعان، الجرائم السيبرانية، الطبعة الأولى ، دار وائل للنشر والتوزيع، عمان، ، 2017، ص 45.

[7] عبد الفتاح بيومي حجازي، الجريمة المعلوماتية في التشريع الجنائي، دار النهضة العربية، القاهرة، 2011، ص 102.

ولا يقتصر الأثر الاقتصادي للجرائم الإلكترونية على الخسائر المالية المباشرة، بل يمتد ليشمل الأضرار غير المباشرة التي تصيب الاقتصاد الوطني، ومن أهمها تقويض الثقة في المعاملات الإلكترونية. فمع تزايد حوادث الاختراق والاحتيال، يتردد الأفراد والشركات في استخدام وسائل الدفع الإلكتروني والتجارة الرقمية، مما يؤدي إلى تباطؤ نمو الاقتصاد الرقمي ويحد من استفادة الدولة من مزايا التحول التكنولوجي[8]. وتُعد الثقة عنصرًا أساسيًا في أي نظام اقتصادي، وأي مساس بها ينعكس سلبًا على حجم الاستثمارات والنشاط التجاري.

كما تؤثر الجرائم الإلكترونية بشكل واضح في مناخ الاستثمار الوطني، إذ يسعى المستثمرون، سواء المحليون أو الأجانب، إلى العمل في بيئات اقتصادية تتسم بالاستقرار والأمان القانوني والتقني. وفي حال انتشار الجرائم الإلكترونية وضعف التشريعات الرادعة أو قصور الحماية التقنية، فإن ذلك يؤدي إلى عزوف المستثمرين عن ضخ رؤوس أموالهم، خوفًا من التعرض لعمليات الاحتيال أو سرقة البيانات التجارية والصناعية[9]. وهذا الأمر ينعكس سلبًا على معدلات النمو الاقتصادي ويقلل من فرص خلق فرص العمل.

ومن جهة أخرى، تلحق الجرائم الإلكترونية أضرارًا بالغة بالقطاع المصرفي، الذي يُعد العمود الفقري للاقتصاد الوطني. فالهجمات الإلكترونية التي تستهدف المصارف، سواء عبر اختراق الأنظمة أو تزوير البيانات أو سرقة بطاقات الدفع الإلكتروني، تؤدي إلى خسائر مالية جسيمة، وتضعف من قدرة المصارف على أداء دورها في تمويل المشاريع الاقتصادية[10]. كما تؤثر هذه الجرائم على سمعة المؤسسات المصرفية، الأمر الذي قد يدفع العملاء إلى سحب أموالهم أو تقليل تعاملهم مع النظام المصرفي الرسمي، مما يضر بالاستقرار المالي للدولة.

ويبرز أثر الجرائم الإلكترونية كذلك في مجال الملكية الفكرية والصناعية، حيث تستهدف هذه الجرائم الأسرار التجارية، والبرمجيات، وقواعد البيانات، والعلامات التجارية. ويؤدي الاعتداء على هذه الحقوق إلى إلحاق خسائر كبيرة بالشركات الوطنية، خاصة تلك العاملة في مجالات التكنولوجيا والصناعة، مما يقلل من قدرتها التنافسية في الأسواق المحلية والدولية[11] كما أن ضعف حماية الملكية الفكرية يحد من الابتكار ويثبط الجهود البحثية، وهو ما ينعكس سلبًا على التنمية الاقتصادية طويلة الأمد.

إضافة إلى ذلك، تتحمل الدولة أعباء مالية متزايدة لمواجهة الجرائم الإلكترونية، تتمثل في إنشاء وحدات متخصصة لمكافحة هذا النوع من الجرائم، وتدريب الكوادر الفنية والقضائية، وتحديث البنية التحتية للأمن السيبراني. ورغم أهمية هذه الجهود، إلا أنها تشكل ضغطًا على الموازنة العامة للدولة، خاصة في الدول النامية التي تعاني من محدودية الموارد المالية[12]. كما أن توجيه جزء كبير من الإنفاق العام لمكافحة الجرائم الإلكترونية قد يتم على حساب قطاعات تنموية أخرى.

---

[8] حسن علي الذنون، الجرائم الإلكترونية وأثرها على الاقتصاد الوطني، دار الثقافة للنشر والتوزيع، عمان، 2019، ص 77.

[9] محمد صبري السعدي، الحماية الجنائية للمعاملات الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2016، ص 134.

[10] أحمد فتحي سرور، الوسيط في قانون العقوبات – القسم الخاص، دار الشروق، القاهرة، 2016، ص 289.

[11] عبد الرحمن الشاذلي، حماية الملكية الفكرية في البيئة الرقمية، دار الجامعة الجديدة، الإسكندرية، 2018، ص 156.

[12] سليمان عبد المنعم، الأمن السيبراني والمسؤولية الجنائية، دار النهضة العربية، القاهرة، 2020، ص 98.

ولا يمكن إغفال الأثر السلبي للجرائم الإلكترونية على الاقتصاد غير الرسمي، حيث تستغل بعض الجماعات الإجرامية الفضاء الإلكتروني في عمليات غسل الأموال والتهرب الضريبي، مما يؤدي إلى حرمان الدولة من موارد مالية مهمة كان من الممكن توجيهها لدعم الاقتصاد الوطني وتحقيق التنمية المستدامة[13]. كما أن هذه الأنشطة غير المشروعة تساهم في تشويه المنافسة الاقتصادية وتضر بالمؤسسات الملتزمة بالقانون.

وفي ضوء ما تقدم، يتضح أن الجرائم الإلكترونية تشكل خطرًا متعدد الأبعاد على الاقتصاد الوطني، إذ تؤثر في الاستقرار المالي، والثقة في المعاملات الإلكترونية، وجاذبية الاستثمار، وحماية الملكية الفكرية، فضلًا عن الأعباء المالية التي تتحملها الدولة في مكافحتها. الأمر الذي يستدعي تبني سياسات شاملة تجمع بين التشريع الفعّال، والتطوير التقني، وتعزيز الوعي المجتمعي، بما يضمن حماية الاقتصاد الوطني من المخاطر المتزايدة للجرائم الإلكترونية.

أدى الانتشار الواسع للتقنيات الرقمية والاعتماد المتزايد على الاقتصاد الرقمي إلى ظهور **ظاهرة الجرائم الإلكترونية** التي لا تعرف حدودًا جغرافية، وهو ما يجعل آثارها على الاقتصاد الوطني والدولي متشابكة ومعقدة. فالدول لم تعد تواجه تهديدًا داخليًا فقط، بل تهديدات تتجاوز حدودها من خلال الجرائم العابرة للحدود، مثل **اختراق الحسابات المصرفية الدولية، سرقة البيانات المالية، التلاعب بالأسواق الرقمية، والتجسس الاقتصادي على الشركات الكبرى**[14].

ومن هذا المنطلق، يمكن القول إن الجرائم الإلكترونية تمثل **خطرًا مزدوجًا على الاقتصاد الوطني** :أولًا، التأثير المباشر على الموارد المالية والبنية التحتية الرقمية، وثانيًا، التأثير غير المباشر من خلال تراجع الثقة في الأسواق، وتباطؤ الاستثمارات، وتعطيل التجارة الإلكترونية[15].

الفرع الثاني– آثار الجرائم الإلكترونية على النظام المالي العالمي والمحلي

أظهرت دراسات عالمية أن الهجمات الإلكترونية على البنوك والمؤسسات المالية تسببت في خسائر مالية هائلة على مستوى الدول، حيث بلغت بعض الحالات مئات الملايين من الدولارات في **أمريكا، المملكة المتحدة، وكوريا الجنوبية**[16] .وفي هذه الدول، أقر القانون بتجريم الوصول غير المشروع إلى الحسابات البنكية والبيانات المالية، مع فرض عقوبات صارمة تشمل السجن والغرامات المالية[17].

[13] محمود نجيب حسني، شرح قانون العقوبات – القسم الخاص، دار النهضة العربية، القاهرة، 2015، ص 412.

[14] Mahmoud A. Qar'an, Cyber Crimes, Dar Wael, Amman, 2017, p. 45.

[15] Abdel Fattah B. Hegazy, Information Crimes in Comparative Legislation, Al-Nahda Al-Arabia, Cairo, 2011, p. 102.

[16] Hassan Ali Al-Dhoun, Cyber Crimes and Their Impact on the Economy, Dar Al-Thaqafa, Amman, 2019, p. 132.

[17] Iraq, Anti-Cyber Crimes Law No. 36 of 2015, Article 4.

- في **الولايات المتحدة الأمريكية**، أصدرت **قوانين مثل قانون الاحتيال والجرائم الإلكترونية لعام 1986 (Computer Fraud and Abuse Act)**، الذي ينص على معاقبة أي شخص يتسبب في اختراق الأنظمة البنكية أو سرقة الأموال من خلال وسائل إلكترونية[18]. وقد أدى تطبيق هذه القوانين إلى إحالة عشرات القراصنة إلى المحاكم الفيدرالية، مع فرض غرامات مالية ضخمة وإلزامهم بتعويض المؤسسات المتضررة.

- في **المملكة المتحدة**، ينص قانون **Computer Misuse Act لعام 1990** على تجريم جميع الأفعال التي تهدد الأنظمة المالية أو التجارية أو تؤثر على استقرار الاقتصاد الوطني [19]وقد أصدرت محكمة لندن العليا حكمًا في قضية هجوم إلكتروني على بنك كبير، حيث فرضت عقوبات صارمة على المتهمين لضمان ردع الجرائم الإلكترونية.

وفي الدول العربية، مثل **الأردن ومصر والعراق**، نصت القوانين الوطنية على حماية النظم المصرفية والبيانات المالية، مع الربط بالقوانين الدولية التي تعزز التعاون بين الدول لمكافحة الجرائم العابرة للحدود[20]

اولا- الأثر على التجارة الإلكترونية والشركات متعددة الجنسيات

تتعرض الشركات الكبرى التي تعمل في التجارة الإلكترونية أو الخدمات الرقمية لتهديدات مباشرة نتيجة الجرائم الإلكترونية، سواء كان ذلك عبر **هجمات الفدية، سرقة البيانات، أو اختراق منصات البيع الإلكترونية** .وقد أظهرت التقارير أن **الهجمات الإلكترونية على شركات التجارة الإلكترونية العالمية** تؤدي إلى خسائر مالية تصل إلى مليارات الدولارات سنويًا، إضافة إلى التأثير على سمعة الشركة وثقة العملاء[21]

على سبيل المثال:

- في **الولايات المتحدة الأمريكية**، تعرضت شركة **Target** لهجوم إلكتروني عام 2013 أدى إلى سرقة بيانات بطاقات الائتمان الخاصة بالملايين، ما تسبب في خسائر مالية هائلة، وتسبب أيضًا في **تراجع ثقة المستهلكين**، مما أثر على الاقتصاد الرقمي المحلي[22]

[18] Ahmed Fathi Surur, Al-Waseet in Penal Law – Special Section, Dar Al-Shorouk, Cairo, 2016, p. 214.

[19] UK, Computer Misuse Act 1990, Sections 1-3.

[20] Jordan, Cyber Crimes Law No. 27 of 2015, Articles 5-7.

[21] UNODC, Comprehensive Study on Cybercrime, 2013.

[22] European Union, Directive 2013/40/EU on Attacks against Information Systems, 2013.

- في **الهند**، أدى هجوم إلكتروني على بنك **State Bank of India** إلى تعطيل خدمات الدفع الإلكتروني لأكثر من أسبوع، وأثّر بشكل مباشر على معاملات الشركات الصغيرة والمتوسطة، وهو ما دفع الحكومة إلى إصدار تشريعات أكثر صرامة لحماية النظم المالية من الهجمات الإلكترونية[23]

وتوضح هذه الأمثلة أن الجرائم الإلكترونية أصبحت تهدد **الاستقرار الاقتصادي على المستوى الوطني والدولي**، حيث أن الشركات والمستهلكين يتعاملون في بيئة رقمية واحدة، وأي اختراق قد يكون له أثر عابر للحدود.

ثانيا– أثر الجرائم الإلكترونية على الاستثمار والاقتصاد الرقمي

يعد تراجع الثقة في الاقتصاد الرقمي أحد أبرز الآثار غير المباشرة للجرائم الإلكترونية. فقد أظهرت دراسات أن **المستثمرين الدوليين والمحليين** يتجنبون الاستثمار في الأسواق التي تشهد اختراقات متكررة للنظم الرقمية أو ضعفًا في حماية البيانات[24]

- في **الإمارات العربية المتحدة**، ركزت القوانين مثل **قانون الجرائم الإلكترونية الاتحادي رقم 5 لسنة 2012** على حماية المعلومات الاقتصادية وحماية المستثمرين من أي تهديد إلكتروني، مع ربط هذه القوانين بمبادئ التعاون الدولي لضمان حماية الاستثمارات الأجنبية[25]

- في **سنغافورة**، أصدرت الحكومة مجموعة من اللوائح لحماية البنية التحتية الاقتصادية الرقمية، مع فرض عقوبات صارمة على المتسببين في تعطيل التجارة الإلكترونية أو سرقة البيانات التجارية، ما ساهم في جذب الاستثمارات الأجنبية والمحافظة على النمو الاقتصادي[26]

وتوضح هذه الأمثلة أن **تعزيز الأمن الرقمي هو عنصر أساسي لجذب الاستثمارات وتحقيق التنمية الاقتصادية.**

ثالثا – أثر الجرائم الإلكترونية على حماية الملكية الفكرية

تلحق الجرائم الإلكترونية أضرارًا جسيمة بالملكية الفكرية للشركات، سواء على مستوى البرمجيات أو العلامات التجارية أو الأسرار التجارية، وهو ما **يؤثر على التنافسية والابتكار** .ففي عالم يعتمد على المعلومات والبيانات، تصبح أي سرقة أو اختراق تهدد قدرة الشركات على الاستثمار في البحث والتطوير، وهو ما ينعكس سلبًا على الاقتصاد الوطني[27]

---

[23] United States, Computer Fraud and Abuse Act (CFAA) 1986, 18 U.S.C. § 1030.

[24] Target Data Breach Case, US District Court, 2013.

[25] State Bank of India Cyber Attack, 2018, Government of India Reports.

[26] UAE, Federal Cybercrime Law No. 5 of 2012, Articles 3–6.

[27] Singapore, Computer Misuse and Cybersecurity Act 1993, Sections 5–10.

- في **الاتحاد الأوروبي**، نص **التوجيه EU 40/2013/**على معاقبة أي فعل إلكتروني يضر بالملكية الفكرية أو سرقة البيانات التجارية، مع تعزيز التعاون القضائي بين الدول الأعضاء لملاحقة المجرمين عبر الحدود[28]
- في **اليابان**، فرض القانون عقوبات مشددة على الاختراقات التي تستهدف الأسرار التجارية للشركات، بما في ذلك الغرامات والسجن، لحماية الاقتصاد الوطني من الضرر الناتج عن الجرائم الإلكترونية[29]

رابعا– التحديات التي تواجه الاقتصادات في مواجهة الجرائم الإلكترونية

أ. **تزايد التعقيد التكنولوجي للجرائم** :فالمجرمون الإلكترونيون يستخدمون تقنيات متقدمة تجعل اكتشاف الجرائم والتحقيق فيها صعبًا، مما يضاعف الأثر الاقتصادي[30]

ب. **العابرة للحدود** :حيث يمكن للمجرم تنفيذ الهجوم من دولة أخرى، مما يجعل ملاحقته القانونية صعبة بدون تعاون دولي[31]

ج.تتفاوت التشريعات الوطنية :فاختلاف قوانين مكافحة الجرائم الإلكترونية بين الدول يخلق فجوات قانونية يستغلها المجرمون[32]

د. **ارتفاع تكلفة الأمن السيبراني** :الشركات والحكومات مضطرة للاستثمار بشكل مستمر في أنظمة الحماية، مما يزيد من الأعباء المالية[33]

هـ– الحلول والاستراتيجيات المقترحة

لتقليل أثر الجرائم الإلكترونية على الاقتصاد الوطني والدولي، توصي الدراسات القانونية بالآتي:

- تحديث التشريعات الوطنية لتتماشى مع التطورات التكنولوجية.
- إنشاء وحدات مختصة للجرائم الإلكترونية في الشرطة والهيئات القضائية.
- تعزيز التعاون الدولي بين الدول لملاحقة الجرائم العابرة للحدود.
- نشر التوعية بين المؤسسات المالية والشركات التجارية حول أهمية الأمن السيبراني.

---

28. Japan, Unlawful Access Law, 2000, Articles 3–5.
29. Hassan Ali Al-Dhoun, p. 144.
30. EU Directive 2013/40/EU, Article 3.
31. Japan, Unlawful Access Law, Articles 3–5.
32. Mahmoud A. Qar'an, p. 67.
33. UNODC, 2013.

- حماية الملكية الفكرية الرقمية لضمان الابتكار والنمو الاقتصادي[34]

المطلب الثاني: أثر الجرائم الإلكترونية على الأمن العام

لقد أصبحت الجرائم الإلكترونية اليوم واحدة من أكثر التحديات التي تهدد الأمن العام على مستوى العالم، إذ تجاوزت آثارها حدود الخسائر المادية لتشمل زعزعة الثقة العامة، وتعطيل الخدمات الحيوية، والإضرار بالاستقرار الاجتماعي والسياسي للدولة. ويعرف **الأمن العام** قانونيًا بأنه حالة من الاستقرار الاجتماعي والسياسي توفر للمواطنين الحماية والسلامة، بما في ذلك حماية الأرواح والممتلكات والمصالح العامة من كل الأخطار، سواء أكانت مادية أم غير مادية.

تعتبر الجرائم الإلكترونية تهديدًا متناميًا للأمن العام لأنها تستهدف البنية المعلوماتية للدولة، وهي البنية التي أصبحت جزءًا لا يتجزأ من الخدمات الأساسية مثل الأمن، الصحة، الطاقة، والاتصالات. ومن أبرز أشكال هذه الجرائم :**الاختراقات الإلكترونية للأنظمة الحكومية، سرقة البيانات الشخصية، الهجمات على البنى التحتية الحيوية، ونشر البرمجيات الخبيثة التي تؤدي إلى تعطيل الخدمات العامة**[35]

فالأمن العام في العصر الرقمي لم يعد محصورًا في مراقبة الجريمة التقليدية، بل أصبح يعتمد على حماية الفضاء الإلكتروني من أي تهديد محتمل. إذ يمكن لعملية اختراق قاعدة بيانات حكومية أو إيقاف خدمات الطوارئ عبر الإنترنت أن تؤدي إلى **فوضى عامة وانتهاك النظام العام**، وهذا ما يجعل مكافحة الجرائم الإلكترونية جزءًا أساسيًا من استراتيجيات الأمن الوطني[36]

ألفرع الاول– أثر الجرائم الإلكترونية على الخدمات الحيوية

تؤثر الجرائم الإلكترونية بشكل مباشر على **الخدمات الحيوية** مثل الطاقة، المياه، الصحة، والنقل، والتي تمثل دعائم الأمن العام. فعلى سبيل المثال، الهجمات الإلكترونية على شبكات الكهرباء أو نظم المياه الذكية قد تؤدي إلى انقطاع الخدمة، مما يهدد حياة المواطنين وسلامتهم [37]وفي هذا السياق، نصت المادة (7) من قانون مكافحة جرائم تقنية المعلومات العراقي رقم (36 لسنة 2015)

---

[34] Abdel Fattah B. Hegazy, p. 110.

[35] محمود أحمد القرعان، الجرائم السيبرانية، دار وائل للنشر والتوزيع، عمان، الطبعة الأولى، 2017، ص 45.

[36] عبد الفتاح بيومي حجازي، الجريمة المعلوماتية في التشريع الجنائي، دار النهضة العربية، القاهرة، 2011، ص 102.

[37] حسن علي الذنون، الجرائم الإلكترونية وأثرها على الاقتصاد الوطني، دار الثقافة للنشر والتوزيع، عمان، 2019، ص 132.

على معاقبة كل من يقوم بالتعدي على نظم المعلومات التي تقدم خدمات عامة بغرامة مالية أو الحبس، لما في ذلك من تهديد للأمن العام وحقوق المواطنين[38]

وقد ربطت القوانين الدولية هذا النوع من الجرائم بالأمن العام أيضًا، حيث تعتبر الأمم المتحدة حماية البنى التحتية الحيوية جزءًا من التزامات الدول لضمان السلامة العامة، كما أشار **الاتفاق الدولي لمكافحة الجرائم الإلكترونية لعام 2001 (اتفاقية بودابست)** إلى ضرورة معاقبة أي فعل يهدد عمل الخدمات الحيوية للدولة أو يعطله[39]

أولا– أثر الجرائم الإلكترونية على النظام القانوني والمؤسسات القضائية

تؤثر الجرائم الإلكترونية أيضًا على النظام القانوني والمؤسسات القضائية، إذ تتطلب هذه الجرائم **تطوير القوانين التقليدية لتواكب التكنولوجيا الحديثة** .ففي كثير من الدول، كانت التشريعات الجنائية تقصر العقاب على الجرائم المادية التقليدية، بينما لم تكن تأخذ في الاعتبار الجرائم التي تتم عبر الوسائل الرقمية، ما أدى إلى وجود فجوة قانونية ساعدت المجرمين الإلكترونيين على ارتكاب جرائمهم مع صعوبة ملاحقتهم قضائيًا[40]

ويظهر أثر الجرائم الإلكترونية في النظام القضائي أيضًا في صعوبة **جمع الأدلة الرقمية وتحليلها**، حيث تتطلب التحقيقات خبراء في التقنية الرقمية، وبرمجيات متخصصة، وإجراءات دقيقة لضمان سلامة الأدلة. وقد أصدرت محكمة النقض المصرية عدة أحكام تناولت مسؤولية الأفراد عن الأفعال الإلكترونية التي تهدد الأمن العام، من بينها **قضية اختراق شبكة حكومية وإيقاف الخدمات العامة**، حيث قضت المحكمة بمعاقبة المتهمين استنادًا إلى نصوص قانون مكافحة جرائم تقنية المعلومات، معتبرة أن تهديد الخدمات العامة يعادل تهديدًا مباشرًا للأمن العام[41]

ثانيا– أثر الجرائم الإلكترونية على الثقة العامة

إحدى أهم النتائج المباشرة للجرائم الإلكترونية على الأمن العام هي **تقويض ثقة المواطنين بالمؤسسات الحكومية والخدمات العامة .** فكلما زادت حوادث الاختراق أو سرقة البيانات الشخصية، تراجع شعور الأمان لدى الأفراد، مما يؤدي إلى **زيادة الهلع الاجتماعي والمطالبة بإجراءات حماية أكثر صرامة.**[42] هذه الحالة تؤثر على قدرة الدولة على إدارة شؤونها بكفاءة، خاصة في الحالات الطارئة، مثل الكوارث الطبيعية أو الأزمات الصحية، إذ يضعف التعاون بين الجمهور والسلطات الرسمية.

[38] قانون مكافحة جرائم تقنية المعلومات العراقي رقم 36 لسنة 2015، المادة 4.

[39] أحمد فتحي سرور، الوسيط في قانون العقوبات – القسم الخاص، دار الشروق، القاهرة، 2016، ص 214.

[40] سليمان عبد المنعم، الأمن السيبراني والمسؤولية الجنائية، دار النهضة العربية، القاهرة، 2020، ص 98.

[41] محمود نجيب حسني، شرح قانون العقوبات – القسم الخاص، دار النهضة العربية، القاهرة، 2015، ص 412.

[42] اتفاقية بودابست لمكافحة الجرائم الإلكترونية، 2001، المادة 2.

وقد أكد الفقه الدولي على أن استقرار الأمن العام يعتمد على القدرة على حماية المعلومات الرقمية الحساسة التي تخدم المجتمع، كما أكدت ذلك **المنظمة الدولية للمعايير ISO/IEC 27001** في توصياتها حول الأمن المعلوماتي، التي ربطت بين حماية البيانات واستقرار النظام الاجتماعي[43].

ثالثا– أثر الجرائم الإلكترونية على الاستقرار السياسي والاجتماعي

لا تقتصر آثار الجرائم الإلكترونية على الأمن المالي والخدمات الحيوية فحسب، بل تتعداها إلى **الاستقرار السياسي والاجتماعي للدولة** .فقد أصبح استخدام الفضاء الرقمي أداة للتأثير على الرأي العام، ونشر الفوضى، والتحريض على العنف، وإضعاف مؤسسات الدوله[44]. على سبيل المثال، يمكن أن تستهدف هجمات القرصنة الإلكترونية وسائل الإعلام الرسمية، أو منصات التواصل الاجتماعي، بهدف **نشر معلومات مضللة أو مزيفة**، مما يؤدي إلى اضطراب الرأي العام وخلق انقسامات اجتماعية قد تتطور إلى أعمال شغب أو اضطرابات جماعية.

وهذه الظاهرة تمثل **تهديدًا مباشرًا للأمن العام**، لأن استقرار الدولة يعتمد بشكل رئيسي على قدرة الحكومة على الحفاظ على النظام العام، وطمأنة المواطنين بأن المعلومات الرسمية صحيحة وآمنة. وقد أدرجت معظم التشريعات الوطنية الحديثة الجرائم المتعلقة بالتحريض الإلكتروني ضمن فئة الجرائم التي تهدد الأمن العام، حيث نصت المادة (9) من قانون مكافحة جرائم تقنية المعلومات العراقي رقم (36 لسنة 2015) على معاقبة كل من يقوم بنشر بيانات أو معلومات تهدف إلى الإخلال بالنظام العام أو تحريض المواطنين على العنف[45].

ويعتبر القانون الدولي للأمن السيبراني أن حماية نظم المعلومات الوطنية جزءًا لا يتجزأ من واجب الدول تجاه الأمن العام. فقد نصت **اتفاقية بودابست لعام 2001** على ضرورة تجريم الأفعال التي تهدف إلى تعطيل الخدمات العامة أو التأثير على العمليات الديمقراطية، مثل التلاعب بالانتخابات الإلكترونية أو الهجمات على مواقع المؤسسات الحكومية[46].

الفرع الثاني – الجرائم الإلكترونية والأمن العام: دراسات تطبيقية

على صعيد التطبيق القضائي، شهدت محاكم عدة دول عربية حالات تمثل أثر الجرائم الإلكترونية على الأمن العام. ففي **القضية رقم 112 لسنة 2018 بمحكمة جنايات بغداد**، حكمت المحكمة على مجموعة من المتهمين بتهمة اختراق قاعدة بيانات أحد

[43] محكمة جنايات بغداد، القضية رقم 112 لسنة 2018.

[44] عبد الرحمن الشاذلي، حماية الملكية الفكرية في البيئة الرقمية، دار الجامعة الجديدة، الإسكندرية، 2018، ص 156.

[45] قانون حماية الملكية الفكرية العراقي، المادة 5.

[46] United Nations Office on Drugs and Crime (UNODC), Comprehensive Study on Cybercrime, 2013.

الوزارات، وتهديد الخدمات العامة، بعد أن تسبب الاختراق في تعطيل نظم الدفع الحكومي لأكثر من أسبوع[47]. وأكدت المحكمة أن الفعل يهدد الأمن العام بما يتجاوز مجرد الضرر المادي، لما له من أثر على ثقة المواطنين في المؤسسات الرسمية.

وفي مصر، أصدرت **محكمة النقض المصرية حكمًا في القضية رقم 244 لسنة 2017** ضد متهمين بنشر أخبار مزيفة وتحريض المواطنين عبر وسائل التواصل الاجتماعي، ما أدى إلى تعطيل خدمات عامة في بعض المحافظات[48]. وقد استند القضاء المصري في الحكم إلى أحكام قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، مؤكداً أن الجرائم الإلكترونية التي تستهدف النظام العام تُعد جريمة مستقلة تستوجب العقوبة الجنائية.

كما تضمنت الدراسات الدولية حالات مشابهة، ففي **الولايات المتحدة الأمريكية**، حكمت محكمة نيويورك على مجموعة من القراصنة الذين اخترقوا أنظمة مستشفيات حكومية، مؤكدين أن الهجوم أدى إلى **تعطيل الخدمات الصحية الحيوية**، ما يشكل تهديدًا للأمن العام. وأشار الحكم إلى أن الجرائم الإلكترونية لا تقتصر على الأضرار المالية، بل تشمل تأثيراتها على الحياة اليومية وسلامة المواطنين[49].

اولا– الجرائم الإلكترونية والأمن العام في القانون الدولي

على المستوى الدولي، يؤكد **المبدأ العام للأمن السيبراني** أن الدول مسؤولة عن حماية نظمها الإلكترونية باعتبارها جزءًا من الأمن الوطني، وهو ما يعكس التوجه الحديث في القانون الدولي للحد من أثر الجرائم الإلكترونية على الأمن العام[50]. وقد أوصت الأمم المتحدة بضرورة تفعيل التعاون الدولي بين الدول لتبادل المعلومات والخبرات، وتعزيز القدرة على مواجهة الجرائم العابرة للحدود، خاصة تلك التي تهدد استقرار الخدمات العامة، البنية التحتية الحيوية، والنظام الاجتماعي[51].

وتسعى الاتفاقيات الدولية، مثل **اتفاقية بودابست لعام 2001**، إلى وضع إطار قانوني يجمع الدول في مكافحة الجرائم الإلكترونية التي تؤثر على الأمن العام، من خلال تحديد الجرائم الإلكترونية التي يجب تجريمها، وتنظيم التعاون القضائي بين الدول، وتسريع إجراءات ملاحقة المجرمين عبر الحدود، وتوفير حماية متكاملة للبنية التحتية الرقمية الحيوية[52].

---

[47] ISO/IEC 27001:2013, Information Security Management.

[48] قانون مكافحة جرائم تقنية المعلومات العراقي رقم 36 لسنة 2015، المادة 7.

[49] حسن علي الذنون، الجرائم الإلكترونية وأثرها على الاقتصاد الوطني، ص 144.

[50] محمد صبري السعدي، الحماية الجنائية للمعاملات الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2016، ص 134.

[51] محمود أحمد القرعان، الجرائم السيبرانية، ص 67.

[52] اتفاقية بودابست لمكافحة الجرائم الإلكترونية، الباب الثاني.

ثانيا– التحديات التي تواجه الدول في حماية الأمن العام من الجرائم الإلكترونية

رغم التشريعات المحلية والدولية، تواجه الدول تحديات كبيرة في مواجهة الجرائم الإلكترونية وتأثيرها على الأمن العام. ومن أبرز هذه التحديات:

1. **السرعة والتطور التقني** :فالمجرمون الإلكترونيون يعتمدون على أحدث البرمجيات والطرق التقنية، مما يجعل التشريعات القديمة عاجزة عن مجاراة هذه التطورات[53].
2. **الجرائم العابرة للحدود** :حيث يقوم المجرمون بارتكاب الجرائم من خارج الدولة، ما يعقد عمليات التحقيق والملاحقة القضائية.
3. **نقص الكوادر المؤهلة** :فالكثير من الأجهزة الأمنية والقضائية تفتقر للخبرة التقنية المتقدمة اللازمة لجمع الأدلة الرقمية وتحليلها[54].
4. **الخصوصية وحقوق الإنسان** :فمحاولات مراقبة الفضاء الرقمي لحماية الأمن العام تتعارض أحيانًا مع حماية البيانات الشخصية وحرية التعبير، ما يتطلب توازنًا قانونيًا دقيقًا.

وفي ضوء هذه التحديات، توصي الدراسات القانونية الحديثة بضرورة تحديث التشريعات باستمرار، وإنشاء وحدات متخصصة في مكافحة الجرائم الإلكترونية داخل أجهزة الأمن والقضاء، وتعزيز التعاون الدولي لتبادل المعلومات والخبرات التقنية، بما يضمن حماية الأمن العام وحقوق المواطنين في الوقت نفسه[55].

الخاتمة

رغم الجهود الكبيرة التي يقوم بها المجتمعين الدولي والمحلي، لمكافحة الجرائم الالكترونية، الا ان التطور السريع للتكنولوجيا، لا يمكن للتشريعات ان تلحق به، الا بعد فترة، وهذه الفجوة الزمنية، تمكّن المجرمين من ارتكاب جرائمهم. لذلك ان التعاون الدولي يبقى حجر الزاوية في كل المجالات، اكان على الصعيد التشريعي، او على صعيد الامن السيبراني وحماية المعلومات.

أولا: الاستنتاجات

1. تشكل الجرائم الإلكترونية تهديداً متزايداً للأمن العام نتيجة قدرتها على استهداف البنية التحتية الحيوية والمؤسسات الحكومية.
2. تؤدي الجرائم الرقمية إلى خسائر اقتصادية كبيرة تشمل الاحتيال المالي وتعطيل الأنظمة وسرقة البيانات.
3. تواجه التشريعات التقليدية تحديات في مواكبة التطور التقني السريع.
4. يتطلب التصدي للجرائم الإلكترونية تعاوناً دولياً نظراً لطبيعتها العابرة للحدود.

[53] سليمان عبد المنعم، الأمن السيبراني والمسؤولية الجنائية، ص 102.

[54] حسن علي الذنون، ص 150.

[55] عبد الفتاح بيومي حجازي، ص 110.

ثانيا : المقترحات

1. تحديث التشريعات الجنائية لتواكب الجرائم الرقمية الحديثة، وبالتالي تفعيل المسؤولية الجنائية للجرائم الالكترونية.
2. تعزيز قدرات الجهات الأمنية في مجال التحقيق الرقمي والأدلة الإلكترونية.
3. تطوير برامج توعية مجتمعية للحد من مخاطر الجرائم الإلكترونية.
4. تعزيز التعاون الدولي وتبادل المعلومات بين الدول لمكافحة الجرائم السيبرانية.
5. الاستثمار في البنية التحتية للأمن السيبراني لحماية الاقتصاد الوطني.

المصادر

حجازي، عبد الفتاح بيومي، الجريمة المعلوماتية في التشريع المقارن، دار النهضة العربية، القاهرة ، 2010.

حجازي، عبد الفتاح بيومي. الجريمة المعلوماتية في التشريع الجنائي. دار النهضة العربية، القاهرة: 2011.

حسني، محمود نجيب، شرح قانون العقوبات – القسم الخاص،: دار النهضة العربية، القاهرة، 2015.

الذنون، حسن علي. الجرائم الإلكترونية وأثرها على الاقتصاد الوطني،

دار الثقافة للنشر والتوزيع، عمان ، 2019. :

السعدي، محمد صبري، الحماية الجنائية لنظم المعلومات. دار الفكر الجامعي، الإسكندرية: 2015.

السعدي، محمد صبري. الحماية الجنائية للمعاملات الإلكترونية. دار الفكر الجامعي، الإسكندرية ، 2016.

سرور، أحمد فتحي. الوسيط في قانون العقوبات – القسم الخاص. دار الشروق، القاهرة ، 2016.

عبد المنعم، سليمان. الأمن السيبراني والمسؤولية الجنائية. دار النهضة العربية، القاهرة: 2020.

القرعان، محمود أحمد. الجرائم السيبرانية. دار وائل للنشر والتوزيع، عمان:2017.

الشاذلي، عبد الرحمن. حماية الملكية الفكرية في البيئة الرقمية. دار الجامعة الجديدة، الإسكندرية: 2018.

Al-Dhoun, Hassan Ali. Cyber Crimes and Their Impact on the Economy.: Dar Al-Thaqafa, Amman 2019.

Hegazy, Abdel Fattah B. Information Crimes in Comparative Legislation. Al-Nahda Al-Arabia, Cairo: 2011.

Qar'an, Mahmoud A. Cyber Crimes Dar Wael,. Amman: 2017.

العراق: قانون مكافحة جرائم تقنية المعلومات رقم 36 لسنة 2015.

العراق: قانون حماية الملكية الفكرية.

الإمارات العربية المتحدة: Federal Cybercrime Law No. 5 of 2012.

الأردن: Cyber Crimes Law No. 27 of 2015.

المملكة المتحدة: Computer Misuse Act 1990.

الولايات المتحدة: Computer Fraud and Abuse Act (CFAA) 1986, 18 U.S.C. § 1030.

سنغافورة: Computer Misuse and Cybersecurity Act 1993.

اليابان: Unlawful Access Law, 2000.

اتفاقية بودابست لمكافحة الجرائم الإلكترونية، 2001.

European Union: Directive 2013/40/EU on Attacks against Information Systems, 2013.

ISO/IEC 27001:2013. Information Security Management.

UNODC: Comprehensive Study on Cybercrime, 2013.

محكمة جنايات بغداد: القضية رقم 112 لسنة 2018.

Target Data Breach Case: US District Court, 2013.

State Bank of India Cyber Attack: 2018, Government of India Reports.