السمة الابتكارية للقضاة في مواجهة النزاعات السيبرانية

كيف نجح القضاة في دمج القانون والتكنولوجيا

القاضي/ ياسين عبد الله عبد الكريم

قاضي وزارة العدل المصرية

ماجستير في القانون، جامعة ليدز بيكيت (المملكة المتحدة)

نبذة

إن تشعب علاقات مستخدمي شبكة المعلومات قد أسفر عن توليد نزاعات محورها تضارب مصالحهم في الفضاء السيبراني. وقد تنوعت تلك المنازعات واتخذت تصنيفات متطابقة مع المنازعات التقليدية أمام القضاء، ولكن لكونها ذات طبيعة تقنية ميزتها عن النزاعات التقليدية وجد القضاة أنفسهم يخوضون غمار منازعات ذات طبيعة جديدة مميزة تستقيها من سمات علاقات الفضاء السيبراني التي أنشأتها. هذا الواقع القضائي تطلب تطوير أدوات ومبادئ قانونية متأصلة في النزاعات التقليدية وصبغها بسمة تقنية تتواءم مع تلك المنازعات المستحدثة، وهي المهمة الموكلة للقضاة بحسب وظيفتهم في الفصل في المنازعات من خلال المبادئ القانونية.

يتضمن البحث دراسة مقارنة استقصائية محلها أحكام قضائية صدرت في منازعات سيبرانية تستهدف الوقوف على ما أنتجته عقليات القضاة من مبادئ قضائية طورت من المفاهيم التشريعية لغرض تطويع القواعد القانونية وجعلها قابلة للتطبيق في النزاعات ذات الطابع التقني.

مقدمة

لقد أتت المنازعات السيبرانية حملًا ثقيلًا أتعب قضاة المحاكم الوطنية ومتقاضيها وكانت مجالًا جمّا لقدح أزناد الأفكار وصولًا للتطبيق والتفسير الأنسب للقواعد القانونية القائمة. لا شك أن الطبيعة اللا واضحة والغامضة للفضاء السيبراني قد زودت مجرمي الانترنت بأدوات التخفي والتمويه المتناسبة مع مقاصدهم الإجرامية والتي مكنتهم من العمل مستترين خلف سمات الفضاء السيبراني. هذا التحدي شحذ همة أهل الفقه والقضاء لتطوير ما لديهم من أدوات قانونية لاحتواء المنازعات السيبرانية – دعوى قضائية تنتج عن المعاملات أو الانتهاكات التي تحدث على شبكة المعلومات – وتوظيف ما يتلاءم مع طبيعتها المتميزة عن المنازعات التقليدية. وقد أرغمت هذه النزاعات الصعبة المحاكم الوطنية على تطوير أساليب قانونية للتغلب على هذه العقبة وتسوية النزاعات السيبرانية. ومع ذلك، هناك اختلافات كبيرة في النهج المتبع بين مختلف الهيئات القضائية.

هذا البحث يفحص ما تضمنه الفقه القانوني والتشريعات الوطنية من مواضيع بشأن هذه النقطة، كما أنه يفحص بعض أحكام القضاء الأمريكي والبريطاني والمصري لإظهار ما تبنوه من مبادئ قانونية احتوت الطبيعة التقنية الغامضة للفضاء السيبراني.

توجهات الفقه إزاء النزاعات السيبرانية

لمواجهة الجرائم السيبرانية المستحدثة، اعتمدت سلطات إنفاذ القانون في الولايات المتحدة خطة لتحسين مهارات هيئات إنفاذ القانون. وكان مرتكز تلك الخطة تزويد موظفي القانون بتقنيات التحقيق والتدريب الفني لمكافحة جرائم الفضاء السيبراني بغض النظر عن عامل الوقت[1]. ويشير نيوفيل إلى الطبيعة الصعبة للجرائم السيبرانية لذا يقترح التقنيات المذكورة للتغلب على هذه

[1] Lanny L Newville (2001), 'Cyber Crime and the Courts - Investigating and Supervising the Information Age Offender', 65(2) *Federal Probation* 11.

العقبة. وعلاوة على ذلك ، يدعو إلى إنشاء نظام فيدرالي للإشراف لمراقبة الجرائم السيبرانية من أجل تحسين توصيف المتهمين على المستوى الاتحادي[1].

وبالإضافة إلى ذلك ، قام المركز القضائي الاتحادي بقفزة من خلال بث سلسلة لضباط إنفاذ القانون الأمريكيين بشأن التعامل مع الجرائم السيبرانية[2]. وعلاوة على ذلك، صاغت لجنة القانون الجنائي التابعة للمؤتمر القضائي نموذجا لاكتساب البيانات وضبطها يحد من سلطة البحث بشكل ملحوظ.

ويعتبر قسم الجرائم والملكية الفكرية في وزارة العدل في الولايات المتحدة هو السلطة المختصة بمواجهة الجرائم السيبرانية بموجب قانون الاحتيال السيبراني وإساءة استعمال الانترنت[3] فيما يتعلق بجرائم الاختراق والقوانين المتعلقة بالمراقبة السيبرانية ورصد الأمن السيبراني وجميع الأنظمة الأخرى المتطورة المتعلقة بالتحقيقات السيبرانية[4].

في كتابهم "المجرمين السيبرانيين في المحاكمة"، ألقى روسل سميث ، بيتر جرابوسكي ، وجريجور أورباس نظرة عامة على الجرائم السيبرانية في كل من المملكة المتحدة والولايات المتحدة الأمريكية. واقترحوا تحسين الأدوات التقنية المتاحة لموظفي الجهاز القضائي. كما سلطوا الضوء على الدور البارز الذي تؤديه أجهزة التكييف والتصنيف في رصد الجرائم السيبرانية واستكشافها. وكذلك على أهمية التغلب على الافتقار إلى الأدلة السيبرانية الذي تؤدي إلى إفلات المجرمين السيبرانيين من العقاب ناصحين بزيادة مستوى التعاون المحلي بين المدعين العامين والشرطة من جهة، والتعاون الدولي بين السلطات القضائية للدول من جهة أخرى لمكافحة المجرمين السيبرانيين[5]. ويعتمد هؤلاء المؤلفون طريقة بحث تجريبية تعتمد على دراسة عدة قضايا من سلطات قضائية ذكرت حصراً. وهذه الهيئات القضائية تنتمي لنظام القانون العام، على الرغم من أن الموضوع الذي نوقش يتعلق بجميع الهيئات القضائية التي تدخلت فيها السوابق القضائية الدولية في صياغة لوائح تنظيمية عالمية بشأنها.

ودفعت الطبيعة التقنية للجرائم السيبرانية تاد سيمونز في المعهد التنفيذي القانوني في تومسون رويترز إلى الدعوة إلى إنشاء محكمة خاصة للجرائم السيبرانية. ويدفع بأن المحكمة المتخصصة ستكون فعالة في مكافحة جرائم الفضاء السيبراني، وأن أحكامها ستكون سوابق قضائية تضع مبادئ قانونية. وتؤدي هذه السوابق إلى تعزيز الأداء القضائي ضد الأنشطة السيبرانية غير المشروعة[6].

ويشرح الدكتور خالد ممدوح آلية التوقيع الرقمي، تعزيزا لمصداقية الوثائق السيبرانية. ويدفع بأن هذا التوقيع، بمجرد تزويده

---

[1] ibid13.
[2] ibid 12.
[3] (18 U.S.C. §1030).
[4] Perry E Wallace, Richard J Schroth and William H Delone (2015), 'The Changing Faces of Cybersecurity Governance Cybersecurity Regulation and Private Litigation Involving Corporations and Their Directors and Officers: A Legal Perspective',
<https://www.american.edu/kogod/research/cybergov/upload/cybersecurity-review-2015.pdf>.
[5] Russell Smith, Peter Grabosky and Gregor Urbas (2004), 'Cyber Criminals on Trial', (Cambridge University Press) 285–290.
[6] Tad Simons,(2018), 'Is It Time for a Court Dedicated to Cybercrime?', Thomson Reuters Legal Executive Institute, <https://www.legalexecutiveinstitute.com/justice-ecosystem-cybercrime-court/#>.

بالتشفير المطلوب، يكفي لإثبات نية صاحبه[١]. كما يدعي أن هذا التشفير يحمي سلامة المستندات الرقمية. ولذلك، يوصي باستخدام التوقيع الرقمي لاحتواء الطبيعة المتطورة لتعاملات الإنترنت وتعزيز الجدارة بالثقة في هذه الوثائق. ومن ثم ، فإنه يشرح التفاصيل التقنية التي قد تفيد موظفي القانون الوطنيين.

إن استخدام أدوات القرصنة والعمليات السرية للدفاع عن حدود الدولة السيبرانية يتم تبنيه بموجب قانون سلطات التحقيق (٢٠١٦) في المملكة المتحدة. وهو يتضمن في الجزء الخامس الآليات التقنية – المشار إليها باسم "التدخل في المعدات"[٢] – اللازمة لمكافحة الأعمال السيبرانية غير المشروعة التي تتطلب الحصول على بيانات من الأجهزة ومواقع الإنترنت. وقد أثر هذا النهج تأثيرا إيجابيا على الأساليب القضائية البريطانية في التصدي للتهديدات السيبرانية، لأنه يطلع هيئات إنفاذ القانون على التكنولوجيات الحديثة المعتمدة في جرائم الفضاء السيبراني . وعلى نحو مماثل ، تؤيد جيما ديفيس حتمية تزويد السلطات القانونية بأدوات اختراق للتصدي لتهديدات الشبكة المظلمة[٣]. وعلى الرغم من تأثرها بخطورة التهديدات السيبرانية، فإنها تحتاج إلى إذن قانوني كشرط مسبق يسمح باستخدام هذه الأدوات. كما تقترح تعديل قانون سلطات التحقيق (٢٠١٦) لتعزيز القدرات القانونية لمراقبة الأنشطة السيبرانية غير القانونية وإحباط تأثيراتها على المجتمع. وفيما يتعلق بالولايات المتحدة الأمريكية، أشار تقرير صادر عن مكتب المفتش العام إلى أن مكتب التحقيقات الاتحادي منخرط في استراتيجية لمواجهة الأجيال القادمة من الهجمات السيبرانية. وذكر التقرير أن مكتب التحقيقات الاتحادي أنشأ شعبة معينة بوصفها "فرقة عمل"[٤] للتصدي للتهديدات السيبرانية ولكنه لا يزال بحاجة إلى تعيين موظفين من ذوي الخبرة التقنية إلى جانب التدريب التقني المكثف لمعالجة النقص في هذه الشعبة. وقد نجح هذا التقرير الرسمي في تحليل التحديات التي واجهها مكتب التحقيقات الفيدرالي فيما يتعلق بالتهديدات السيبرانية. وأوصت ببذل المزيد من الجهود في مجال تبادل المعلومات ووضع الاستراتيجيات[٥].

وفي مصر ، يوجه القانون رقم ٢٠١٨/١٧٥ السلطات القضائية الوطنية إلى التعاون، وفقا للاتفاقات الدولية والإقليمية المنطبقة، ومع مراعاة مبدأ المعاملة بالمثل، مع الحكومات والسلطات الأجنبية في مجال تبادل المعلومات لمنع جرائم الفضاء السيبراني[٦]، وهو أمر يشجعه تقرير مكتب الأمم المتحدة المعني بالمخدرات والجريمة لعام ٢٠١٩[٧]. ويمنح أيضا موظفي إنفاذ القانون سلطة الاستيلاء على جميع نظم المعلومات، وخوادم البيانات، وجميع تدفقات البيانات التي قد تنظر في الأدلة الرقمية

[1] Dr. Khalid Mamdouh (2021), 'The Criminal Digital Evidence and its Proving Authority', Dar Elfikr Elgamey, Alexandria, Egypt, ISBN 978-977-379-603-7, 199.
[2] Investigatory Powers Act 2016 c.25, pt 5.
[3] Gemma Davies (2020), 'Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers' 84(5) *The Journal of Criminal Law* 407, <https://journals.sagepub.com/doi/full/10.1177/0022018320952557>
[4] ibid 5.
[5] ibid 24.
[6] Law No 175/2018, ibid pt 1 art 4.
[7] The Expert Group to Conduct a Comprehensive Study on Cybercrime (2019), 'Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 27 to 29 March 2019', CCPCJ/EG.4, <https://undocs.org/UNODC/CCPCJ/EG.4/2019/2>.
(n 39) pt 2 sec A (c,d).

إلى جانب الحق في الوصول إلى جميع قواعد البيانات المتعلقة بعد إذن من النيابة المختصة[1]. وبالإضافة إلى ذلك ، يمنح هذا القانون النيابة العامة سلطة الشروع في إجراءات منع المواقع عند اعتبارها تهديدا للأمن الوطني. والغرض من المشرع هو دعم سلطات النيابة العامة في مكافحة هذا النوع من الجرائم، الذي يتسم بالتطور المستمر.

المبادئ التي أرستها المحاكم الوطنية لمجابهة الأنشطة السيبرانية غير المشروعة

دافعت محاكم الولايات المتحدة عن سياسة إدارة الموقع بحذف التعليقات والتدوينات التي تحث على الكراهية لحماية المجتمع من خطاب الكراهية على الإنترنت والسلوك في قضية *Shulman v. Facebook.com*[2]. وادعت المحكمة أن قانون سلامة الاتصالات[3] يسمح للناشرين بتقييد منشورات الكراهية التي تعتبر هذا النهج "نشاطاً ناشراً"[4] تحميه المادة ٢٣٠. والواقع أن حصانة الناشرين تحمي سلامة المجتمع من خلال منع خطاب الكراهية على الإنترنت. هذا النهج يتفق مع أهداف قانون ماثيو شيبارد وجيمس بيرد الابن بشأن منع جرائم الكراهية لعام ٢٠٠٩[5]. بيد أن محاكم الولايات المتحدة ابتكرت هذه الأداة لتحقيق تلك الأهداف.

وقد سهلت موافقة المحاكم الأميركية على استخدام عنوان مزود الخدمة IP Address لتحديد مكان وجود المتهم في قضية *Strike 3 Holdings, LLC v. Doe*[6] ورصد نشاطه. ومن ثم، فإن ميزة عدم الكشف عن هوية المجرمين السيبرانيين يتم تحييدها؛ ويمكن لهذا الأسلوب أن يحددها على نحو فعال. والواقع أن هاتين المحكمتين اعترفتا بقيمة الأدلة الرقمية والبيانات القانونية التي تم الحصول عليها عن طريق الإنترنت بأساليب غير تقليدية والتي يوصى بها في كتاب "المجرمين السيبرانيين في المحاكمة" الذي نشر في عام ٢٠٠٤[7]

قرر القضاء الأميركي ، في قضية *State v. Chebegwen*[8] ، أن محادثة "تطبيق واتس" تكشف عن نوايا أطرافها. لذا ، المحكمة إعتبرتها دليل رقمي أصيل. ورغم أن هذا الموقف قد يتعارض مع حظر اعتراض الاتصالات السلكية أو الشفوية أو السيبرانية والكشف عنها المنصوص عليه في قانون الجرائم والإجراءات الجنائية [9]، فقد أعطت المحكمة الأولوية للحاجة للتكيف مع طبيعة النزاع السيبراني. وعلى نحو مماثل ، اعترف القضاء المصري ، في الجنحة الاقتصادية رقم ٢٠٢٠/٨٨٧ والجنحة الاقتصادية رقم ٢٠٢٠/٢٠٣٠ في المحكمة الاقتصادية بالقاهرة ، بقوة الحجية للأدلة الرقمية في التحرش على الإنترنت ووافقت المحكمة على البحث في الحساب الاجتماعي للمدعى عليه للحصول على الأدلة. وبالمثل ، يدافع الدكتور خالد ممدوح عن قيمة البيانات المشتركة على منصات تبادل الرسائل هذه وفقًا لمعايير معينة[10]. ويقرر أن الحكم ينبغي أن يثبت العلاقة بين المدعى عليه والرسائل الصادرة عن حزب تحرير أوروبا أو عن الحزب الديمقراطي لطرفي الدردشة. وعلاوة على ذلك ، يأذن

---

[1] No 175/2018 pt 2 art 6.
[2] , No. 18-2708 (3d Cir. Oct. 11, 2019).
[3] Communications Decency Act (1996), 47 U.S.C. § 230.
[4] Murphy v. Twitter, Inc., ibid p 17.
[5] 18 U.S.C. § 249.
[6] 319 F. Supp. 3d 406 (D.D.C. 2018).
[7] Russell Smith, Peter Grabosky and Gregor Urbas (2004), ibid.
[8] Appellate Case No. 28337 (Ohio Ct. App. 2020).
[9] 18 U.S. Code § 2511.
[10] Dr. Khalid Mamdouh (2021), ibid 175.

القانون رقم ٢٠١٨/١٧٥ للقضاة بالحصول على أدلة رقمية مخزنة على منصات سيبرانية[١].

اهتم القضاء الأمريكي بمسألة نزاهة الأدلة الرقمية. ففيما يتعلق باستغلال الأطفال في المواد الإباحية على الإنترنت، لم تقبل المحكمة الأدلة الرقمية التي وجدت على الحاسوب المحمول للمدعى عليه في قضية *Donaldson v. State*[٢] ورفضت شهادة خبير بشأن هذه المواد بسبب عدم اكتمال شروط صحة الدليل. واحتجت المحكمة بأن هذا التقصير أدى إلى عدم كفاية الأدلة واستندت في رفضها لتلك الشهادة إلى هذا المبدأ. وهكذا طبقت المحكمة الجزاء الذي فرضه القانون على هذا التقصير في الممارسات التجارية. غير أن هذا وضع ذلك الجزاء في السياق السيبراني يعكس الفراغ القانوني في القواعد الجنائية الذي أجبر المحكمة على تطبيق عقوبة تجارية في سياق جنائي.

لقد تنامى التوظيف القضائي للتكنولوجيا ضد استغلال الأطفال في المواد الإباحية بشكل لافت. سمحت الدائرة الخامسة لمحكمة الاستئناف الأمريكية باستخدام قيم التجزئة المتزامنة كدليل (United States v Reddick[٣] ،). أشارت المحكمة إلى أن مطابقة قيم التجزئة Hash Value الخاصة بالمواد الإباحية للأطفال الموزعة عبر الإنترنت مع تلك الموجودة على أجهزة المدعى عليه تكفي لإنهاء المساءلة. تسمح مقارنات قيم التجزئة بالتوصل إلى حيازة المدعى عليه لمواد إباحية للأطفال بيقين مطلق، وهو ثمرة دمج التقنيات في التفسير القضائي.

في قضية State v Hunt[٤] (٢٠٢٠)، أعادت المحكمة تشكيل الفهم التقليدي لنطاق أوامر تفتيش الأجهزة الرقمية للمدعى عليه. وبينما استخرج رجال المباحث مواد إباحية خاصة بالأطفال من جهاز الكمبيوتر المحمول الخاص به بموجب مذكرة تفتيش، طالب المتهم المحكمة برفض هذه الأدلة بسبب تجاوز رجال المباحث لنطاق مذكرة التفتيش. وعلى وجه التحديد، ادعى أن المذكرة سمحت للمحققين بالبحث عن الأجهزة الإلكترونية، وليس تفتيشها، مما يعني العثور عليها وإرسالها إلى الهيئة القضائية المخصصة دون استكشاف محتوياتها. وبالتالي، فإن قيام المباحث بالتنقيب ومصادرة المواد الرقمية المخزنة على الكمبيوتر المحمول يعتبر باطلا ولاغيا، ومع ذلك لا يجوز للمحكمة إدانة المدعى عليه. إن بطلان إجراءات جمع الأدلة يقتضي تبرئة المتهم وفق المنطق القانوني الأساسي. وأعربت المحكمة عن اتفاق ظاهري مع حجة المدعى عليه لأن القواعد التقليدية التي تحكم أوامر التفتيش تتطلب الامتثال النهائي لصياغتها. ومع ذلك، فقد دحضت هذه الحجة، حيث قررت أن السوابق القضائية الأمريكية السابقة تشير إلى عدم جدوى هذه الحجة؛ لقد سمحوا بأدلة استغلال الأطفال في المواد الإباحية التي كشف عنها المحققون على الرغم من أن المذكرة حدت من نطاقها للبحث عن الأجهزة. إن خطورة إشراك القاصرين في هذا النشاط غير المشروع تبرر تفسير المحكمة الموسع لأمر التفتيش بما يضمن المصلحة الفضلى للطفل والتغلب على عقبات ظاهرية النصوص القانونية لتعزيز الحماية القضائية للطفل.

قررت المحاكم الأمريكية أن سرقة بيانات بطاقات الائتمان تشكل "ضررًا في الواقع" وفقًا للمادة ٣ من دستور الولايات المتحدة[٥]

---

[1] Law No 175/2018, ibid.
[2] 262 So. 3d 1135 (Miss. Ct. App. 2018).
[3] 900 F.3d 636 (5th Cir. 2018).
[4] CR-18-0886.
[5] US Constitution Art 3, Sec 2, Clause 1.

ووافقت على تعويض الأضرار الناجمة عن خرقها. وقد طبقت في ذلك قاعدة الخسارة الاقتصادية في *Cmty. Bank of Trenton v. Schnuck Mkts., Inc*[1]. لحماية النظام المصرفي الوطني. علاوة على ذلك، أكدوا أن الخوف من سرقة الهوية الناجم عن خرق البيانات يكفي للدفاع عن انتهاك قانون الخصوصية في *Hartigan v. Macy's, Inc*[2].

من اللافت للنظر أن الهجوم السيبراني من قبل حكومة أجنبية لم يعتبر ضررًا تجاريًا من قبل المحكمة الأمريكية في *Broidy Capital Mgmt. v. Qatar*[3]. إذا احتوت على مفهوم عملية تجسس بموجب الخصائص المتضمنة في قانون التجسس لعام ١٩١٧[4] بسبب الجوانب السياسية لهذه العمليات حيث قررت المحكمة أنه لا يمكن تطبيق الضرر التجاري بسبب الحصانة التي يمنحها القانون الدولي لدولة قطر وبموجب قانون الحصانات السيادية الأجنبية[5].

وقد وافقت الهيئات القضائية الأنجلو ساكسونية محل البحث على تعويض ضحايا الهجمات السيبرانية عن الأضرار التي سببتها هذه الهجمات. في قضية *Carroll v. Macy's, Inc.*[7] قبلت المحكمة اتفاقية التسوية لأنها تلبي معايير طلب التعويض. وقد استند هذا الرأي إلى نظرية الإهمال ومعايير قانون الضرر لضمان شرعية مثل هذه الإعفاءات ومنع الابتزاز. على الرغم من ذلك، رفضت المحكمة الأمريكية، في *Krohm v. Epic Game*[8] طلب التعويض المنصوص عليه في نظرية الإهمال بسبب نقص الأدلة نسبة الإصابة التي لحقت المدعي بالخرق الواقع لبياناته. وبالتالي، يضفي قرار المحكمة على مستخدمي الإنترنت وأنظمة الكمبيوتر مزيدًا من الحماية في الفضاء السيبراني. بالإضافة إلى ذلك، أشار قاضي المقاطعة تيد ستيوارت، في قضية *Jive Commerce, LLC v. Wine Racks Am., Inc*[6]، إلى أنه يجب على المدعي تقديم تعريف واضح للنشاط السيبراني غير القانوني، والذي يطلب تعويضًا عنه، إلى المحكمة.

علاوة على ذلك، وافقت محكمة المملكة المتحدة في قضية *Fentiman v Marsh*[9] على تعويض المدعي الذي عانى من ضرر بسبب خطاب الكراهية عبر الإنترنت ؛ ونظرت في منشورات المدعى عليه ضده التي ألحقت ضررا بالغا بسمعته. وطلبت المحكمة النزعة المتأصلة في الوظائف للموافقة على التعويض.

منعًا لمستخدمي الإنترنت غير القانونيين من جمع البيانات من الحسابات عبر الإنترنت، محكمة المملكة المتحدة في *Green v Group Ltd & Ors*[10] أقرت الأدلة التي تم الحصول عليها من خوادم المدعى عليه لإثبات مسؤولية الأخير عن مخاوف انتهاك البيانات. نفذت المحكمة قانون حماية البيانات في المملكة المتحدة لعام ٢٠١٨[11] الذي يلزم إدارات الخوادم باتخاذ الإجراءات اللازمة لحماية بيانات العملاء.

---

[1] 887 F.3d 803 (7th Cir. 2018).
[2] Civil Action No. 20-10551-PBS (D. Mass. Nov. 5, 2020)
[3] No. 18-56256 (9th Cir. Dec. 2, 2020).
[4] 18 U.S.C. ch. 37, Pub.L. 65–24, 40 Stat. 217.
[5] 28 U.S.C. § 1602.
[6] Case No.: 2:18-cv-01060-RDP (N.D. Ala. June 5, 2020).
[7] 408 F. Supp. 3d 717 (E.D.N.C. 2019).
[8] No. 1:18-CV-49 TS-BCW (D. Utah Aug. 15, 2018).
[9] [2019] EWHC 2099 (QB).
[10] [2019] EWHC 954 (Ch).
[11] Data Protection Act 2018, 2018 c. 12.

فيما يتعلق بالبيع بالتجزئة عبر الإنترنت، حددت المحاكم الأمريكية، في قضية *Bolger v. Amazon.com*[1]، مسؤولية بائع التجزئة والشركة المصنعة عن عيوب عملية البيع بالتجزئة والتجارة السيبرانية عبر الإنترنت بموجب قانون دعم ثقة المتسوقين عبر الإنترنت لعام ٢٠١٠[2] الذي وتضمن المسؤولية التجارة السيبرانية لأنها قد تشمل الأطراف عبر الوطنية والنظم المالية.

من اللافت للنظر أن السيد القاضي ساينى أدمج قواعد الإجراءات المدنية لعام ١٩٨٨[3] في التقاضي بشأن الهجمات السيبرانية. في *Weaver & Ors v British Airways Plc*[4]، وافقت المحكمة، على الرغم من أن الطرفين اتفقا على تاريخ قطع محدد للتقادم، على طلب المدعي لتمديد هذا التاريخ. وجاء في الحكم أن التطوير أو الخاصية التي تبرر تمديد الموعد النهائي تنطبق على طلب المدعي الانضمام إلى الدعوى. وبالتالي، لم تنتهك المحكمة قانون الإجراءات المدنية المذكور لأن التمديد كان مطلوبًا للوصول إلى العدالة في تلك الدعوى كون القاعدة ١٩,١٣ (هـ) من هذا القانون تجعل هذا التاريخ اختياريًا وليس إلزاميًا.

وقد وافقت المحاكم البريطانية ، لحماية حقوق التأليف والنشر من الانتهاكات المتصاعدة على الإنترنت ، في *Capitol Records v British Telecommunications Plc*[5] و *Matchroom Boxing Ltd v BT Plc*[6] ، على طلب المدعي من مقدمي خدمات الإنترنت في المملكة المتحدة حجب موقع على شبكة الإنترنت لتخزين الملفات يعرض مواد غير مرخصة ، مملوكة للمدعي، لحماية حقوق ملكيته الفكرية. وطبقوا مفهوم براءات الاختراع المعنون في قانون حقوق التأليف والتصميم وبراءات الاختراع لعام ١٩٨٨[7] بشأن المواد المتاحة على الإنترنت للدفاع عن الإبداع والابتكار في الفضاء السيبراني .

ومن الجدير بالذكر أن السلطة القضائية في المملكة المتحدة أعادت توصيف مفهوم الملكية في القانون. وفي قضية *AA v Persons Unknown & Ors, Re Bitcoin*[8] ، اعتبرت الشركة الأصول المشفرة ملكية قابلة للتعويض عند الاستيلاء عليها حيلةً. وبالمثل، اعتبرت أن نطاق الإنترنت ملكية في *Hanger Holdings v Perlake Corp SA*[9] بموجب قواعد الملكية في القانون العام. وهكذا ، أضافت العنصر السيبراني إلى مفهوم حق الملكية الذي يعكس التحول إلى التشفير والرقمنة في التجارة السيبرانية[10]. وعلى الرغم من الطبيعة الصعبة لعملية الترميز، فقد نجح القضاء في المملكة المتحدة في احتواء التشفير كعنصر اقتصادي.

فيما يتعلق بالعقود على الإنترنت، اعترف القضاء المصري في الاستئناف رقم ٨٩/١٧٦٨٩ (ق) والاستئناف رقم ٨٧/١٢٤١٥ (ق) ، دائرة محكمة النقض التجارية ، بالقوة الملزمة للبريد الإلكتروني. واعتبرتهما المحكمة طريقة تعاقد إذا وقعتا رقميا ودقيقا.

---

[1] 53 Cal.App.5th 431 (Cal. Ct. App. 2020).
[2] 15 U.S.C. §§ 8401-8405.
[3] 1998 No. 3132 (L. 17).
[4] [2021] EWHC 217 (QB)
[5] [2021] EWHC 409 (Ch)
[6] [2020] EWHC 2868 (Ch)
[7] 1988 c. 48.
[8] [2019] EWHC 3556 (Comm).
[9] [2021] EWHC 81 (Ch).
[10] Chiara Zilioli (2020), 'Crypto-assets: Legal Characterisation and Challenges under Private Law', 45(2) *European Law Review* 251.

وأكدوا صحة المستندات السيبراني ة في الأدلة القانونية. ويغلب هذا النهج على أمر غريب يتمثل في أن المعاملات المباشرة التي تتم على الإنترنت حيث أن قواعد الإثبات التقليدية في القانون المدني المصري[1] تقتصر على الوثائق الورقية لإثبات الحقوق والواجبات. ونتيجة لذلك ، عززت المرونة التي أبدتها المحكمة بإضافة القوة الملزمة إلى الوثائق الرقمية ثقة العقود الرقمية. ثم تُقبل صحة المستندات السيبراني ة لأنها تعبر عن نوايا الأطراف بما يؤدي لازدهار الاقتصاد الرقمي.

وبالمثل ، ادعت محكمة الولايات المتحدة في قضية *Cullinane v. Uber Techs, Inc*[2]. أن ذات القواعد المنطبقة على العقود التقليدية قابلة للتطبيق كذلك على العقود الرقمية كونها تحوي بيانات موثوق بها في بنودها، كما أن أن التشريعات ذات الصلة لم تفرض شكلًا معينًا للاتفاقات الرقمية. وبالإضافة إلى ذلك ، قررت محكمة المملكة المتحدة ، في قضية *Price v Walton Civil Engineering and Surfacing Contractors Ltd*[3] ، كفاية التوقيع الرقمي لصاحب المطالبة للموافقة على المطالبة المتعلقة بالأموال على الإنترنت. وبالمثل ، يجادل إريك غولدمان بأنه إذا أعرب طرف العقد الرقمي عن إرادته بتوقيع المستند ، فإن هذا التوقيع الرقمي ينشئ عقدا صحيحا بموجب مفهومه القانوني[4]. وبالإضافة إلى ذلك ، فإنه يعتبر أن وضع الشرطة على صندوق الموافقة علي الشروط على مواقع الإنترنت يكفي كتوقيع رقمي.

حمايةً للمنافسة عبر الإنترنت، قرر القضاء البريطاني، في *Lifestyle Equities CV v Amazon UK Services Ltd*[5]..، أن إدراج السلع ذات العلامات التجارية في مكان قانوني لا يتضمن انتهاكًا للعلامة التجارية. أيضًا، في *Gascoigne Halman Ltd v Agents' Mutual Ltd*[6]، اعتبرت المحكمة أن إنشاء بوابة عبر الإنترنت لتحدي البوابات الأخرى وخفض التكاليف ليس منافيًا للمنافسة الموضوعية. وعزز هذا الرأي سياسات المنافسة الوطنية بتنظيم المفهوم القانوني المنافسة.

بشكل ملحوظ، في *AA v Persons Unknown & Ors, Re Bitcoin* ، أخفت المحكمة هوية الأطراف لحمايتهم من الهجمات السيبرانية. على الرغم من أن القاعدة هي جلسة الاستماع العلنية، إلا أن إخفاء هوية الأطراف في هذا النزاع كان يهدف إلى حمايتهم من الهجمات السيبرانية الانتقامية.

الخلاصة

في الختام، يفيد البحث أن الهيئات القضائية محل البحث قد دمجت الأدوات التقنية مع القواعد القانونية التقليدية الحالية للتغلب على الطبيعة التقنية للنزاعات السيبرانية. ومن ثم، فقد أنشأوا آلية فريدة لحماية الحدود السيبرانية، وهي آلية ذات ركنين: القانون والتكنولوجيا. هذا الهيكل الهجين منح تلك الآلية سمة المرونة حيث قام بتكييف الهيئات القضائية الوطنية مع الطبيعة التقنية للنزاعات السيبرانية وعزز قدرة المحاكم الوطنية على مواجهة التهديدات السيبرانية. وبالتالي، يصبح الفضاء السيبراني أكثر أمانًا للأفراد والكيانات.

---

[1] Law No 131/1948, Egypt.
[2] 893 F.3d 53 (1st Cir. 2018).
[3] [2017] 2 WLUK 533.
[4] Eric Goldman (2019), 'Online Contracts', from Eric Goldman (2019), 'Internet Law: Cases & Materials' (2019 edition), Santa Clara University Legal Studies Research Paper, <https://ssrn.com/abstract=3201352> .
[5] [2021] EWHC 118 (Ch).
[6] [2019] EWCA Civ 24.

وهكذا، عالجت الهيئات القضائية الوطنية أوجه القصور في التشريعات ذات الصلة المتعلقة بالتهديدات السيبرانية – كونها لم توجه القضاة إلى الآليات المناسبة لمعالجتها بل أطلقت العنان للسلطة التقديرية للقضاة لابتكار ما يرونه مناسبًا من أدوات تتناسب مع حالة كل قضية على حدة. إلى جانب ذلك، تثبت هذه الآلية أن السمة البارزة لمساهمة السلطة القضائية الوطنية في الفضاء السيبراني هو ***الابتكار***. إن الابتكار هو المفتاح الذي مكّن القضاة من التغلب على الصعاب التقنية للنزاعات السيبرانية وركود التشريعات من خلال الجمع بين القانون والتكنولوجيا. وقد أدرك مجلس الاتحاد الأوروبي أهمة سمة الابتكار لأنه يدفع القضاة إلى التكيف مع التطورات التقنية للفضاء السيبراني[1]. علاوة على ذلك، ذكر مساعد المدعي العام بريان أ. بينتشكوفسكي السمة التقنية للفضاء السيبراني وأوضح الحاجة إلى تزويد العمل السيبراني القضائي بالمهارات المبتكرة المطلوبة لمواجهة التهديدات السيبرانية المبتكرة[2]. تمنح المهارات المبتكرة للسلطة القضائية مساهمتها أهمية فريدة في تأمين الحدود السيبراني ة للدولة لأنها تعيق أنشطة مجرمي الإنترنت وتحتوي على الطبيعة التقنية للفضاء السيبراني .

بيد أن إسهام السلطات القضائية لا ينفي دور المشرع في الفضاء السيبراني. فالقوانين هي أساس الممارسة السيبرانية للمحاكم. ولكن تفسير القضاة للقوانين يعالج ركودها ، وينفذ قواعدها بفعالية. يوجه هذا التفسير المشرّع إلى التعديلات المطلوبة لتعزيز سيادة القانون في الفضاء السيبراني.

مراجع

- Lanny L Newville (2001), 'Cyber Crime and the Courts – Investigating and Supervising the Information Age Offender', 65(2) Federal Probation 11.
- Perry E Wallace, Richard J Schroth and William H Delone (2015), 'The Changing Faces of Cybersecurity Governance Cybersecurity Regulation and Private Litigation Involving Corporations and Their Directors and Officers: A Legal Perspective', <https://www.american.edu/kogod/research/cybergov/upload/cybersecurity-review-2015.pdf>.
- Russell Smith, Peter Grabosky and Gregor Urbas (2004), 'Cyber Criminals on Trial', (Cambridge University Press) 285–290.

[1] The Council of the European Union Conclusions on Improving Criminal Justice in Cyberspace (2016), Luxemburg, <https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf>.

[2] US Department of Justice (2020), 'Assistant Attorney General Brian A. Benczkowski Deliver Remarks at the "Justice in Cyberspace" Symposium', Justice News on 5 February 2020, <https://www.justice.gov/opa/speech/assistant-attorney-general-brian-benczkowski-delivers-remarks-justice-cyberspace>

- Tad Simons,(2018), 'Is It Time for a Court Dedicated to Cybercrime?', Thomson Reuters Legal Executive Institute, <https://www.legalexecutiveinstitute.com/justice-ecosystem-cybercrime-court/#>.
- Dr. Khalid Mamdouh (2021), 'The Criminal Digital Evidence and its Proving Authority', Dar Elfikr Elgamey, Alexandria, Egypt, ISBN 978-977-379-603-7, 199.
- Gemma Davies (2020), 'Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers' 84(5) The Journal of Criminal Law 407,
- The Expert Group to Conduct a Comprehensive Study on Cybercrime (2019), 'Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 27 to 29 March 2019', CCPCJ/EG.4, <https://undocs.org/UNODC/CCPCJ/EG.4/2019/2>.
- Chiara Zilioli (2020), 'Crypto-assets: Legal Characterisation and Challenges under Private Law', 45(2) European Law Review 251.
- Eric Goldman (2019), 'Online Contracts', from Eric Goldman (2019), 'Internet Law: Cases & Materials' (2019 edition), Santa Clara University Legal Studies Research Paper
- The Council of the European Union Conclusions on Improving Criminal Justice in Cyberspace (2016), Luxemburg, <https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf>.
- US Department of Justice (2020), 'Assistant Attorney General Brian A. Benczkowski Deliver Remarks at the "Justice in Cyberspace" Symposium', Justice News on 5 February 2020, <https://www.justice.gov/opa/speech/assistant-attorney-general-brian-benczkowski-delivers-remarks-justice-cyberspace>

تابع المزيد من إصدارات

الأكاديمية الدولية للوساطة والتحكيم IAMA

iamaeg.net