المجلة الدولية للفقه والقضاء والتشريع

المجلد ٣، العدد ٢، ٢٠٢٢

تعليق على حكم المحكمة العليا للولايات المتحدة في قضية فان بورين ضد الولايات المتحدة رقم ١٩-٧٨٣ والصادر في ٣ يونيو ٢٠٢١

معرف الوثيقة الرقمى (DOI) : 10.21608/IJDJL.2022.106642.1130

الصفحات ٣٢٤ - ٣٣٧

إبراهيم أحمد صبره

مدرس مساعد بكلية القانون بالجامعة البريطانية في مصر

باحث بمركز القانون والتكنولوجيا التابع لكلية القانون بالجامعة البريطانية في مصر

المراسلة: إبراهيم أحمد صبره، مدرس مساعد بكلية القانون بالجامعة البريطانية في مصر - باحث بمركز القانون والتكنولوجيا التابع لكلية القانون بالجامعة البريطانية في مصر.

البريد الإلكتروني: ibrahim.sabra@bue.edu.eg

تاريخ الإرسال: ٠٤ ديسمبر ٢٠٢١، **تاريخ القبول:** ٠١ مارس ٢٠٢٢

نسق توثيق المقالة: إبراهيم أحمد صبره، تعليق على حكم المحكمة العليا للولايات المتحدة في قضية فان بورين ضد الولايات المتحدة رقم ١٩-٧٨٣ والصادر في ٣ يونيو ٢٠٢١، المجلة الدولية للفقه والقضاء والتشريع، المجلد ٣، العدد ٢، ٢٠٢٢، صفحات (٣٢٤ - ٣٣٧).

International Journal of Doctrine, Judiciary and Legislation

Volume 3, Issue 2, 2022

Commentary on the United States Supreme Court Decision in Van Buren v. United States No. 19-783 of June 3, 2021

DOI: 10.21608/IJDJL.2022.106642.1130

Pages 324 - 337

Ibrahim Sabra

Assistant Lecturer, Faculty of Law, British University in Egypt

Researcher at the Centre for Law and Emerging Technologies, Faculty of Law, British University in Egypt

Correspondance : Ibrahim Sabra, Assistant Lecturer, Faculty of Law, British University in Egypt - Researcher at the Centre for Law and Emerging Technologies, Faculty of Law, British University in Egypt.

E-mail: ibrahim.sabra@bue.edu.eg

Received Date : 04 December 2021**, Accept Date :** 01 March 2022

Citation : Ibrahim Sabra, Commentary on the United States Supreme Court Decision in Van Buren v. United States No. 19-783 of June 3, 2021, International Journal of Doctrine, Judiciary and Legislation, Volume 3, Issue 2, 2022 (324-337).

Print ISSN : 2682-4213 Online ISSN : 2682-4221

الملخص

ساهمت الثورة التكنولوجية التي نعيشها اليوم بشكل كبير في تطور المجتمعات من نواحٍ عدة، خاصة التحول الرقمي في أماكن العمل سواء داخل مؤسسات القطاع العام أو الخاص، والذي ساعد بشكلٍ كبير على تعزيز الابتكار والأتمتة والشفافية، وإدارة الموارد بشكل أكثر كفاءة، وتوفير الوقت، والحد من البيروقراطية والفساد، وغير ذلك. إلا أن ذلك لا يخل من التحديات والتي يأتي على رأسها ظهور الهجمات الإلكترونية وتصاعد وتيرتها ضد مختلف المؤسسات.

فالاعتقاد السائد عند الحديث عن الهجمات الإلكترونية وعمليات القرصنة أنها تهديدات خارجية تُنفذ من قِبل أشخاص خارجيين تستهدف تلك المؤسسات لتحقيق مكاسب مالية أو لأسباب سياسية أو اجتماعية، غير أن التهديدات الداخلية تُشكل أيضًا خطرًا هائلًا قد يتمثل في موظف حالي أو أيٍ من شركاء العمل ممن لديهم وصول شرعي إلى أنظمة وبيانات الشركة والذين قد يستغلونه في تدمير أو سرقة البيانات أو تخريب أنظمة الشركة، إما نتيجة الإكراه أو بغرض الانتقام أو الابتزاز.

لذلك يحاول هذا التعليق إلقاء الضوء على مسألة التهديد الداخلي عن طريق معالجة تحليلية نقدية للحكم محل النظر والذي يتعلق بأحد أعقد الجرائم الإلكترونية والمتمثلة في جريمة «تجاوز حدود الدخول المصرح به» للكمبيوتر، المنبثقة عن جريمة «الدخول غير المصرح به»، والتي ما زالت محل جدل على الرغم من تعرض عديد المحاكم لمثل تلك المسألة على مدار العقود الثلاثة الماضية.

يبدأ التعليق بسرد وقائع القضية أولًا، ثم يوضح ثانيًا بشكل موجز ما أقرته المحكمة، ومن ثم يعرض الأسباب التي استندت إليها المحكمة، وعقب ذلك ينتقل إلى تحليل تلك الأسباب والتعليق عليها، وأخيرًا ينتهي ببعض الملاحظات الختامية

الكلمات المفتاحية: الجريمة الإلكرتونية، القرصنة الإلكترونية، التهديد الداخلي، جريمة الدخول غير المصرح به، جريمة تجاوز حدود الدخول المصرح به.

Abstract

Our world has witnessed myriad technological breakthroughs that have greatly contributed to the progress of societies in many ways. At the forefront of these contributions comes the digital transformation we have been experiencing in the workplace whether in public or private institutions. This has tremendously helped manage resources more efficiently, save time, reduce bureaucracy, enhance transparency, fight corruption, etc. Nevertheless, such transformation does not come without challenges, on top of which is the prevalence of cybercrime against numerous institutions.

One of the misconceptions about cybercrime is the common belief that they are external threats executed by outsiders, targeting institutions for financial, political or social reasons. But this is not always true since internal threats also pose a huge risk, represented in an existing employee or a business partner who has legitimate access to the company's systems

and data, and who may use such access to destroy or steal data, or sabotage the company's system. This could be a result of coercion, extortion or out of revenge.

Therefore, this Commentary attempts to shed light on the issue of Internal Hackers through an analytical and critical analysis of the court decision in question, which addresses one of the most intricate cybercrimes, namely "exceeding authorised access" to computer systems. This crime stems from the "unauthorized access" cybercrime, which remains controversial despite being tackled by many courts over the last three decades.

The Commentary begins by listing the facts of the case, then stating what the court has held. After that, it presents the court reasoning and later moves to an analysis of those **reasons,** and finally ends with concluding remarks.

key words: Cybercrime, Hacking, Insider threat, Unauthorised Access, Exceeding Authorised Access.

المقدمة

ساهم التطور التكنولوجي أواخر القرن الماضي، خاصةً مع ظهور الإنترنت والذي أحدث ثورةً في عالم الاتصالات، في انتشار أجهزة الكمبيوتر في كل مكان بدءًا من المؤسسات العلمية ووصولًا للقطاعين العام والخاص، ولكن تبع ذلك أيضًا ظهور نوع جديد من الجرائم، ألا وهي «الجرائم الإلكترونية»[(١)]. حيث بدأ المجرمون باستكشاف طرقًا مبتكرة تمكنهم من التسلل لأجهزة الكمبيوتر واستغلالها بشكل غير مشروع. ونتيجة لعدم قدرة القوانين التقليدية على التصدي لذلك النوع غير التقليدي من الجرائم، عكف المشرعون على استحداث قوانين جديدة يمكنها مجابهة أشكال الجريمة الإلكترونية المختلفة.

فعلى سبيل المثال، أصدر الكونجرس الأمريكي قانون الاحتيال وإساءة استخدام الكمبيوتر عام ١٩٨٦، ومن بعده قانون إساءة استخدام الكمبيوتر لسنة ١٩٩٠ والذي أقره مجلس العموم بالمملكة المتحدة بعد فشل المحاكم البريطانية في معاقبة عدد من قراصنة الانترنت في القضية الشهيرة «ريجينا ضد جولد وشيفرين» لعام ١٩٨٧ والتي قام فيها شخصان بالدخول غير المصرح به لشبكة إحدى الشركات والوصول لعدد من المناطق المؤمنة على الشبكة. وبعد التعرف عليهم والقبض عليهم كان هناك تخبط وحيرة لدى السلطات لعدم وجود توصيف قانوني لأفعالهم، وفي النهاية تمت محاكمتهم استنادًا لقانون التزييف والتزوير، ولكن تمت تبرئتهما لعدم انطباق أي من الجرائم المذكورة في القانون على أفعالهم[(٢)]. ومؤخرًا تم استصدار قانون جرائم تقنية

[(١)] حتى الأن لا يوجد لا يوجد تعريف دولي للجريمة الإلكترونية ولكن بشكل أو بأخر يمكن تقسيم الجرائم الإلكترونية إلى فئتين ١) الجرائم الإلكترونية المعتمدة على الإنترنت «أي جريمة لا يمكن ارتكابها إلا باستخدام أجهزة الكمبيوتر أو شبكات الكمبيوتر أو غيرها من أشكال تكنولوجيا اتصالات المعلومات» «تمس بسرية البيانات أو النظم الحاسوبية وسلامتها وتوافرها»، حيث لا يقتصر دور تكنولوجيا المعلومات والاتصالات فيها على كونها وسيلة لارتكاب الجريمة بل هي كذلك هدفًا للجريمة. ٢) الجرائم الإلكترونية التي يُسهلها الإنترنت «هي جرائم تقليدية، مثل الاحتيال والسرقة، يمكن أن تزداد من حيث النطاق أو الانتشار باستخدام أجهزة الكمبيوتر أو شبكات الكمبيوتر أو غير ذلك من أشكال تكنولوجيا الاتصالات المعلوماتية. أنظر في:

Mike McGuire and Samantha Dowling, 'Cyber crime: A review of the evidence' (UK Home Office 2013) <https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence> Ch1 P 4 and Ch 2 P 4.

[(٢)] R v Gold and Schifreen [1987] QB

المعلومات رقم ١٧٥ لعام ٢٠١٨ من قبل مجلس النواب المصري.

فعلى الرغم من تأصل هذا النوع من القوانين في عديد من الدول واتساع تطبيقه حول العالم في وقتنا الحالي إلا أن تلك القوانين مازالت محلاً للجدل والدراسة، لذا يحاول هذا التعليق إلقاء الضوء على حكم المحكمة العليا للولايات المتحدة في قضية فان بورين ضد الولايات المتحدة رقم ١٩-٧٨٣ والصادر في ٣ يونيو كونه أحد الأحكام الهامة والحديثة المتعلقة بجرائم تقنية المعلومات وتحديدًا جريمة «تجاوز حدود حق الدخول المصرح به للكمبيوتر» (Exceeding Authorized Access) والمنبثقة عن جريمة «الدخول غير المصرح به» (Unauthorised Access)، والتي ظهرت للأفق وتعرضت لها المحاكم منذ تسعينيات القرن الماضي، لكنها لا زالت محل خلاف حتى يومنا هذا، حيث يبدأ التعليق بسرد وقائع القضية أولا، ثم ينتقل ثانيا بشكل موجز إلى ما أقرته المحكمة، وينتهي بتحليل الأسباب التي استندت إليها المحكمة في تكوين رأيها والتعليق عليها.

وقائع القضية

في إطار عملية لمكتب التحقيقات الفيدرالي، تم توقيف رقيب بشرطة جورجيا يدعى ناثان فان بورين لاستخدامه كمبيوتر سيارة الدورية الخاصة به، وذلك من أجل الوصول إلى قاعدة بيانات إنفاذ القانون بهدف الحصول على معلومات عن رقم لوحة ترخيص إحدى السيارات في مقابل المال.

تم توجيه الاتهام لفان بورين لارتكابه جناية انتهاك القسم ١٠٣٠ (أ) (٢) من قانون الاحتيال وإساءة استخدام الكمبيوتر الصادر في عام ١٩٨٦ والذي يُخضع أي شخص «يدخل عمدًا إلى كمبيوتر دون إذن أو يتجاوز حدود الدخول المصرح به»[٣] للمسئولية الجنائية، وذلك لانتهاكه سياسة الإدارة التابع لها والتي تحظر الحصول على معلومات من خلال قاعدة البيانات لأغراض غير متعلقة بإنفاذ القانون، على الرغم من استخدامه للتصريح الممنوح له. وينص قانون الاحتيال وإساءة استخدام الكمبيوتر في هذه الحالة على أن يعاقب كل من ينتهك القسم ١٠٣٠ (أ) (٢) بالسجن أو الغرامة أو كلاهما، بالإضافة إلى المسؤولية المدنية عما يلحق بالمجني عليه من ضرر أو خسارة نتيجة لذلك والتي تسمح للأخير بالمطالبة بتعويضات مالية عادلة.

قامت هيئة المحلفين بإدانة فان بورين، ولذا حكمت عليه محكمة المقاطعة الأمريكية للمنطقة الشمالية من ولاية جورجيا بالسجن ١٨ شهرًا. استأنف فان بورين الحكم أمام الدائرة ١١ من محكمة الاستئناف الفيدرالية الأمريكية، ولكن تم رفض استئنافه وأيدت الأخيرة ما انتهت إليه الأولى بأن فان بورين قد انتهك بالفعل قانون الاحتيال وإساءة استخدام الكمبيوتر.

ونتيجة لذلك قدم فان بورين التماسًا إلى المحكمة العليا بالولايات المتحدة والذي جادل فيه بأن جريمة «تجاوز حدود الدخول المصرح به» لا تنطبق على ما قام به كونها تقتصر فقط على «أولئك الذين يحصلون على معلومات تخرج عن نطاق تصريح الدخول المخول لهم، وليس على أولئك الذين يسيئون استخدام تصريح الدخول الذي لديهم.

في الأخير، قبلت المحكمة العليا للولايات المتحدة الالتماس المقدم من فان بورين لمراجعة قضيته وحسم الخلاف الدائر حول ما إذا كان فان بورين «يحق له الحصول هكذا» على المعلومات، وكذلك إنهاء حالة الانقسام بين المحاكم الأمريكية فيما يتعلق بنطاق المسؤولية في جريمة «تجاوز حدود الدخول المصرح به»

[٣] وفقًا للقسم ١٠٣٠ (هـ) (٦) فإن جريمة «تجاوز حدود الدخول المصرح به» تعني «الدخول إلى جهاز كمبيوتر بإذن، واستخدام هذا الدخول للحصول على معلومات أو تعديل معلومات على جهاز الكمبيوتر والتي لا يحق لمن دخل على الجهاز الحصول عليها أو تغييرها هكذا.»

الخاص بقانون الاحتيال وإساءة استخدام الكمبيوتر.

ما انتهت إليه المحكمة

في هذه القضية قامت المحكمة العليا بالإجابة على سؤال قانوني محدد وهو: هل يعد «تجاوزا للدخول المصرح به» قيامُ شخص مرخص له بالوصول إلى المعلومات الموجودة على جهاز الكمبيوتر، باستخدامها لغرض غير مناسب أو غير مرتبط بمقتضيات العمل أو غير شرعي، وبالتالي انتهاكًا للقسم ١٠٣٠ (أ) (٢) من قانون الاحتيال وإساءة استخدام الكمبيوتر؟

على الرغم من اتفاق أطراف القضية على أن وصول فان بورين لقاعدة بيانات إنفاذ القانون كان مصرحًا به، وأنه قد تحصل على معلومات من على جهاز كمبيوتر عند قيامه بالحصول على رقم لوحة ترخيص إحدى السيارات في مقابل المال، إلا أن نقطة الخلاف بينهم تكمن حول ما إذا كان فان بورين «يحق له» الحصول على رقم لوحة الترخيص على النحو الذي تم.

دفع فان بورين بأن المادة المتنازع عليها وتحديدًا عبارة - لا يحق لمن دخل على الجهاز الحصول عليها أو تغييرها هكذا - تشير بوضوح إلى المعلومات التي لا يُسمح للشخص بالحصول عليها باستخدام جهاز كمبيوتر مصرح له بالوصول إليها. وبالتالي، إذا كان لدى الشخص حق الوصول إلى المعلومات المخزنة في جهاز الكمبيوتر «على سبيل المثال، في «المجلد أ»، والذي يمكن للشخص أن يحصل منه على المعلومات بشكل مسموح به - فإنه لا ينتهك قانون الاحتيال وإساءة استخدام الكمبيوتر بالحصول على تلك المعلومات، بغض النظر عما إذا كان قد حصل عليها لغرض محظور من عدمه. ولكن إذا كانت المعلومات موجودة بدلاً من ذلك في «المجلد ب» والذي لا يستطيع الشخص الوصول إليه لكونه غير مصرح له بالدخول إليه، ومع ذلك دخل إليه وحصل على المعلومات، فإنه بذلك ينتهك قانون الاحتيال وإساءة استخدام الكمبيوتر».

على الجانب الاخر، ترى الحكومة بأن جريمة تجاوز حدود الدخول المصرح به تنطبق على ما قام به فان بورين، حيث إن عبارة «لا يحق لمن دخل على الجهاز الحصول عليها أو تغييرها هكذا» وبالتحديد كلمة «هكذا» تسمح بتطبيق القانون على نطاق أوسع، حيث إنها تجعل من قراءة عبارة «لا يحق له الحصول عليها هكذا» إشارة إلى المعلومات التي لم يكن مصرحًا للشخص الحصول عليها بالطريقة أو الظروف الخاصة التي حصل عليها من خلالها. وبالتالي، دفعت الحكومة بأن «الطريقة أو الظروف» التي يكون فيها للفرد الحق في الحصول على المعلومات من عدمه يتم تحديدها من خلال أي قيود على حق الفرد في الوصول إلى المعلومات يتم الإعلان عنها «بشكل محدد وصريح» في أي مكان. ولذلك وفي القضية محل النظر، وجود قيود منصوص عليها في اللائحة الداخلية لمكان عمل فان بورين يكفي لاعتبار ما قام به فان بورين مخالفة لقانون الاحتيال وإساءة استخدام الكمبيوتر. وضحت الحكومة دفعها بمثال أنه «قد يحصل الموظف على المعلومات بشكل قانوني من المجلد «د» في الصباح لغرض مسموح به كالتحضير لاجتماع عمل - ولكن يحصل على نفس المعلومات بشكل غير قانوني من نفس المجلد «المجلد د» في فترة ما بعد الظهر لغرض محظور - على سبيل المثال، للمساعدة في صياغة سيرة ذاتية لتقديمها إلى صاحب عمل منافس».

بعد النظر في دفوع كل من الطرفين وكذلك آراء المتدخلين في القضية، انتهت المحكمة إلى أن ذلك لا يعد انتهاكًا لقانون الاحتيال وإساءة استخدام الكمبيوتر. صدر رأي المحكمة بأغلبية ٦ إلى ٣ وقدم القاضي توماس رأيًا مخالفًا، انضم إليه فيه رئيس المحكمة العليا القاضي روبرتس والقاضي أليتو.

الأسباب التي استندت لها المحكمة

يحاول هذا التعليق باختصار شرح الأسباب التي بنت عليها المحكمة رأيها في قضية محل النظر، حيث استندت في رأيها لعدة أسباب أهمها تحليل نص المادة وتفسيرها في ظل التعريفات التي قدمها القانون وكذلك نطاق تطبيق المادة وهيكل القانون ذي الصلة.

أولًا: نص/لغة المادة وتفسيرها

(أ)

في تسبيبها ركزت المحكمة بشكل أساسي على «نص القانون» وتحديدًا مفهوم «تجاوز الوصول المصرح به» والذي عرفه القانون بأنه «الدخول إلى جهاز كمبيوتر بإذن، واستخدام هذا الدخول للحصول على معلومات أو تعديل معلومات على جهاز الكمبيوتر والتي لا يحق لمن دخل على الجهاز الحصول عليها أو تغييرها هكذا.»[٤]

من جهة أولى، لم تبد المحكمة اقتناعها بدفع الحكومة بأن عبارة «لا يحق] له[الحصول عليها هكذا» تشير إلى المعلومات التي لم يكن مسموحا للشخص الحصول عليها بالطريقة التي حصل بها على المعلومات أو في الظروف التي تحصل فيها على المعلومات. فالحكومة هنا تدفع بأن كلمة «هكذا» في الفقرة سالفة الذكر تمنح نطاقا أوسع، وبالتالي فإن الطرق أو الظروف التي تسمح للشخص بالحصول على المعلومات يتم تحديدها من خلال أي ضوابط يتم الإبلاغ بها «بشكل محدد وصريح» فيما يتعلق بحق الفرد في الوصول إلى المعلومات. بهذه الطريقة التي تفسر بها الحكومة هذه الفقرة فإنه يُعد قانونيًا قيام الموظف بالحصول على معلومات من المجلد «أ» لغرض مسموح به مثل التحضير لاجتماع عمل، ولكن يعد غير قانونيًا قيامه بالحصول على نفس المعلومات من نفس المجلد لغرض محظور مثل استغلالها في صياغة سيرة ذاتية لتقديمها إلى صاحب عمل منافس.

في هذا الصدد أشارت المحكمة إلى أن كلمة «هكذا» هي بمثابة مصطلح مرجعي يشير إلى «الطريقة التي تم ذكرها» أو «الطريقة الموصوفة»، لذا فإنه وإن كان دفع الحكومة يبدو مقبولًا في ظاهره غير أنه في تفسيره لكلمة «هكذا» قد تجاهل التعليمات التي أضفاها تعريف تلك الكلمة بأن مثل هذه الطريقة أو الظرف المشار له يجب أن يكون قد تم بالفعل» ذكره» أو «تحديده» أو «وصفه». أضافت المحكمة أنه طبقًا للنهج الذي اتبعته الحكومة في تفسيرها فإن الظرف الذي يجعل من سلوك الشخص غير قانوني ليس بالضرورة أن يكون محددًا بشكل مسبق في القانون ذي الصلة، حيث ذهب التفسير لاعتبار أن الظرف المجَرِّم للفعل يمكن أن يكون مصدره أي من قوانين الولايات المتحدة، أو قوانين الولايات، أو اللوائح الداخلية لجهة العمل أو اتفاق خاص، بل وفي أي مكان آخر. وانتهت المحكمة إلى أن الحكومة في تفسيرها قد فشلت في تحديد أي أساس نصي لتفسيرها.

من جهة ثانية، وجدت المحكمة أن تفسير فان بورين للفقرة «لا يحق] له[الحصول عليها هكذا» وتحديدًا كلمة «هكذا» أكثر منطقية، فطبقًا لهذا التفسير فإن كلمة «هكذا» تشير إلى ظرف أو طريقة قد تم ذكرها مسبقًا في نفس النص، مؤكدة على أن كلمة «هكذا» ليست مصطلحًا عائمًا يوفر ربطًا لأي قيد مذكور في أي مكان، بل هي كلمة تستخدم لتجنب الحاجة إلى التكرار.

[4] According to section 1030 (e) (6) the term “exceeds authorized access” means “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter”.

(ب)

رفضت المحكمة أيضًا دفع الحكومة بأن قراءتها لكلمة «هكذا» يقدم مساهمة قيمة لتفسير نص المادة الخاص بتجاوز حدود الدخول المصرح به لأنه يمنح «هكذا» دورًا في تفسير النص، مؤكدة على أن ما تقدم به فان بورين من قراءة لكلمة «هكذا» يجعل من تضمينها في عبارة «لا يحق] له[الحصول عليها هكذا» أمرًا زائدًا غير ضروري إذا كان الهدف فقط الإشارة للطريقة المذكورة سلفًا في النص الخاص بتجاوز حدود الدخول المصرح به، فوجود «هكذا» لا يضيف إلى معنى العبارة شيئًا، وتباعًا فالمعنى لن يتغير حال حذفها من النص.

في هذا الصدد أكدت المحكمة على أن قراءة فان بورين لا تجعل من كلمة «هكذا» غير ضرورية، فبدونها قد يفتح القانون الباب أمام الأفراد لاستخدام «حقهم في الحصول على معلومات في شكل غير رقمي» كدفاع عن مسؤولية وفقًا لقانون الاحتيال وإساءة استخدام الكمبيوتر.

وأعطت المحكمة مثالاً على ذلك بأنه يمكن لشخص قام باستخدام جهاز الكمبيوتر الخاص به لتحميل ملفات لا يحق له الحصول عليها أن يدفع بأنه لم يخالف قانون الاحتيال وإساءة استخدام الكمبيوتر لأنه «يحق له الحصول على» المعلومات كونه يحمل إذنًا بالوصول إلى تلك الملفات من خلال طريقة أخرى (على سبيل المثال، عن طريق طلب نسخ ورقية من الملفات من قسم الموارد البشرية). لكن بإضافة «هكذا» لنص المادة، يغلق قانون الاحتيال وإساءة استخدام الكمبيوتر الباب أمام ذلك النوع من الدفوع، فالقانون يتعلق بما يفعله الشخص على الكمبيوتر؛ فلا يبرر لأي شخص اختراق ملف ليس مصرحًا له الدخول إليه إذا كان من الممكن للمخترق السير في القاعة لالتقاط نسخة ورقية من القسم المختص.

أضف إلى ذلك أن وجود «هكذا» في نص المادة يحدد إطار القانون فيما يتعلق بالحق في الوصول إلى المعلومات فيقصره على «الحق في الوصول إلى المعلومات باستخدام الكمبيوتر»، وبالتالي يضيق من المسؤولية في ظل قانون الاحتيال وإساءة استخدام الكمبيوتر، فبدونها يمكن تفسير نص المادة على أنه يشمل كافة أشكال القيود على حق الفرد في الحصول على المعلومات.

(ج)

أخيرًا، رفضت المحكمة ما دفعت به الحكومة، والتي تراجعت عنه الأخيرة في النهاية، بأن المتحدث المعتاد للغة الإنجليزية قد يرى أن فان بورين قد تجاوز الوصول المصرح له به عندما دخل لقاعدة بيانات إنفاذ القانون وحصل على معلومات لوحة الترخيص لأغراض شخصية. وأشارت المحكمة إلى أن عبارة «تجاوز الوصول المصرح به» ليست هي كل ما يتم النظر فيه، بل يجب أن يُؤخذ في الاعتبار التعريف الصريح لتلك العبارة والذي نص عليه قانون الاحتيال وإساءة استخدام الكمبيوتر وليس المعنى العادي للعبارة. وبالتالي فإن تحديد مسؤولية فان بورين يتطلب تحديد ما إذا كان قد تجاوز حق الوصول المصرح له به في ظل التعريف الذي أقره القانون سالف الذكر، وفي تلك الحالة ترى المحكمة أن التعريف القانوني يخدم موقف فان بورين. علاوة على ما سبق، وجدت المحكمة أن هذا التصور يتماشى مع الشكل الذي سيفهم به المتحدث المطلع معنى «يتجاوز الوصول المصرح به». لذلك انتهت المحكمة إلى أن التفسير الأوسع للحكومة ليس هو التفسير الوحيد الممكن ولا حتى بالضرورة الأكثر طبيعية.

أضافت أيضًا أن المحاكم، عند تفسير القوانين، تأخذ في اعتبارها المصطلحات ذات المعنى الفني، و»الوصول» يعد أحد تلك المصطلحات الفنية التي تحمل منذ مدة طويلة معنى ثابتًا من المنظور الحسابي، ولذا فمن

الضروري أخذ هذا المعنى في الاعتبار عند تفسير قانون يتعلق بمسألة تقنية كالقانون محل النظر. فالوصول يُشير إلى فعل الدخول لنظام الكمبيوتر أو جزء معين من هذا النظام مثل الملفات أو المجلدات أو قواعد البيانات. ومن ثم فإنه يتفق مع هذا المعنى مساواة فعل «تجاوز الوصول المصرح به» بفعل دخول جزء من النظام لا يمتلك مستخدم الكمبيوتر امتيازات الوصول إليه.

ثانيًا: تطبيق المادة

فيما يخص تطبيق نص المادة محل النظر، أشارت المحكمة إلى أن التفسير الذي قدمته الحكومة للمادة الخاصة بتجاوز حدود الدخول المصرح به سينتج عن تطبيقه ربط المسؤولية الجنائية بعدد كبير من أنشطة الكمبيوتر الشائعة، وتباعًا ستجرم عبارة «تجاوز حدود الدخول المصرح به» كل انتهاك لسياسة استخدام الكمبيوتر، أي أن الملايين من المواطنين الملتزمين بالقانون سيتحولون إلى مجرمين. أعطت المحكمة مثال على ذلك بمكان العمل، حيث ينص بشكل عام أصحاب العمل على أنه لا يمكن استخدام أجهزة الكمبيوتر والأجهزة الإلكترونية الخاصة بالعمل إلا لأغراض العمل. وبالتالي، عند تبني تفسير لنص المادة سالفة الذكر، فإن قيام موظف بإرسال بريدًا إلكترونيًا شخصيًا أو قراءته للأخبار باستخدام كمبيوتر العمل يعد انتهاكًا لقانون الاحتيال وإساءة استخدام الكمبيوتر. لذلك أكدت المحكمة على أن مثل تلك التداعيات تؤكد عدم معقولية تفسير الحكومة.

ثالثًا: بناء القانون وسياقه

هنا أكدت المحكمة على أنه بجانب كون لغة المادة محل النظر تمثل مشكلة لموقف الحكومة، ينبغي أيضًا النظر بشكل أوسع على بناء القانون، فالتفاعل بين فقرتي «بدون تصريح» و»تجاوز حدود الدخول المصرح به» في القسم (أ) (٢) يؤكد على ضرورة ذلك، حيث ترى المحكمة أن قراءة فان بورين لعبارة «لا يحق له الحصول عليها هكذا» تضع فقرتي المادة السابقتين في تناغم، في حين فشلت قراءة الحكومة في تحقيق ذلك.

فطبقًا لقراءة فان بورين فإن فقرة «بدون تصريح» تسعى لحماية أجهزة الكمبيوتر نفسها من خلال استهداف المخترقين الخارجيين الذين «يدخلون إلى جهاز كمبيوتر دون أي إذن على الإطلاق». أما بالنسبة لفقرة «تجاوز حدود الدخول المصرح به» فهي تهدف لمد نطاق الحماية لبعض المعلومات داخل أجهزة الكمبيوتر من خلال استهداف ما يسمى بالمخترقين الداخليين الذين لديهم إذن بالدخول إلى جهاز الكمبيوتر، ولكنهم يقوموا بالدخول إلى منطقة من الكمبيوتر لا يمتد إليها ذلك الإذن.

هنا ترى المحكمة أن قراءة فان بورين تعكس بناء قانوني أكثر اتساقًا، فالمسؤولية في كلتا الحالتين تنبع من فكرة وجود «بوابات تعمل صعودًا وهبوطًا»، قد تسمح أو لا تسمح بالوصول إلى نظام الكمبيوتر، ويمكن أن تجيز أو تمنع الوصول إلى مناطق معينة داخل النظام. تلك القراءة لكلا الفقرتين يتوافق مع مفهوم «الوصول» كانعكاس لمعنى «دخول» في سياق مجال الحوسبة.

التعليق على الحكم

تعد مسألة تجاوز الموظفين لتصريح الدخول المخول لهم من المعضلات التي واجهها القضاء في عديد من الدول عند النظر في قضايا تتعلق بجرائم الإنترنت وتحديدًا الدخول غير المرخص به للكمبيوتر، وفي هذا الصدد يتفق هذا التعليق مع الرأي الذي تبنته المحكمة في القضية الحالية حيث إنه يعد أكثر عملية وملاءمة لواقع

الأمور. فالمحكمة العليا في القضية الحالية أصابت في قرارها كونها أشارت لخطورة التفسير الفضفاض الذي انتهجته الحكومة لمواد قانون الاحتيال وإساءة استخدام الكمبيوتر، رافضة بشكل صريح الحجج التي قدمتها الحكومة للاحتفاظ بسلطات واسعة في هذا الصدد من شأنها أن تؤدي لإساءة توظيف القانون وتطبيقه اعتباطيًا.

ففقهاء القانون الجنائي ينظرون إلى مبدأ الشرعية من نواحي مختلفة أهمها أنها ترسخ قاعدة محورية تقضي بضرورة تفسير القوانين الجنائية بشكل ضيق فيما يتعلق بتوصيف الجرائم ونطاقها[٥]، وبناء على ذلك يرى الفقه أن «القوانين الجنائية يجب أن تفسر بشكل صارم ضد الحكومة»، وأن تفسر المحكمة أي غموض لصالح المدعى عليه.[٦]

أيضًا فالتعليق العام رقم ٣٤ الصادر عن لجنة الأمم المتحدة لحقوق الإنسان، والمتعلق بالمادة ١٩ من العهد الدولي الخاص بالحقوق المدنية والسياسية الخاصة بالحق في حرية التعبير والتي ينبثق منها الحق في الوصول إلى المعلومات، قد أكد على أن أي قاعدة قانونية من شأنها الحد من الحق في حرية التعبير والوصول للمعلومات، «يجب أن تُصاغ بدقة كافية لتمكين الفرد من تنظيم سلوكه وفقًا لذلك، فلا يجوز للقانون أن يمنح سلطة تقديرية غير مقيدة لتقييد حرية التعبير [والوصول للمعلومات] للمكلفين بتنفيذها.»[٧] وهو ما لا نجده في نص القسم ١٠٣٠ (أ) (٢) من قانون الاحتيال وإساءة استخدام الكمبيوتر والمتعلقة بـ «تجاوز الحق في الدخول المصرح به» وكذلك تفسير الحكومة للمادة سالفة الذكر. وبالتالي يثمن هذا التعليق على قرار المحكمة العليا كونه فسر المادة محل النظر تفسيرًا ضيقًا يلغي التفسير الواسع المبهم الذي تبنته الحكومة.

بجانب ذلك، يرى هذا التعليق أنه عندما يتعلق الأمر بتفسير النصوص القانونية، يجب دائمًا أخذ سياق وبناء القانون في الاعتبار وذلك استنادًا لقاعدة «القانون الكامل» (The Whole Act Rule)، والتي تنص على أنه في حالة تفسير النصوص القانونية فهناك دائمًا قرينة على التماسك والتَرَابُط بين نصوص القانون الواحد، لذا يجب تفسير النص ككل. فالوثيقة القانونية تحتوي عادةً على العديد من الأجزاء المترابطة، وبالتالي توفر الوثيقة بشكل متكامل سياقًا لكل جزء من أجزائها.[٨] وفي هذا الصدد، يرى كل من أنطونين سكاليا وهو أحد أشهر قضاة المحكمة العليا للولايات المتحدة وبريان أ. غارنر وهو محامٍ ومؤلف معاجم ومحاضر ويعد من أشهر الفقهاء القانونيين بالولايات المتحدة الأمريكية، أن هذا النهج عادةً «يثبت أن واحدًا فقط من المعاني المحتملة التي يمكن أن تحملها كلمة أو عبارة يتوافق مع استخدام نفس الكلمة أو العبارة في أي مكان آخر في القانون».[٩] وهذا التوجه هو ما أتبعته المحكمة في تسبيبها لرأيها، وهو ما يجده التعليق أمرًا موفقًا.

إضافة لما سبق، وتعقيبًا على بعض الآراء التي ترى أن اتباع هذا التفسير من شأنه أن يغلق الباب أمام أي محاولة لمقاضاة الموظفين الذين «تجاوزوا الحد المسموح للدخول المصرح به» وهذا مردودٌ عليه بأنه أولًا، لا حاجة لأن يتم اللجوء للقضاء في كل حالة من حالات سوء سلوك الموظف فيما يتعلق بـ «بتجاوز الحد المسموح

---

[5] Peter Westen, 'Two Rules of Legality in Criminal Law' (2007) 26 Law and Philosophy 229-305

[6] 'The New Rule of Lenity', (2006) 119 Harvard Law Review 2420-2441

[7] Human Rights Committee, 'General Comment No. 34, Article 19: Freedoms of opinion and expression' (2011) CCPR/C/GC/34

[8] Suraj Kumar and Taylor Beech, 'A Guide to Reading, Interpreting and Applying Statues' (The Writing Center at GULC 2017)7

[9] Antonin Scalia and Bryan A. Garner, Reading Law: The Interpretation of Legal Texts (West Group 2012) 167

للدخول المصرح به» حيث يمكن لصاحب العمل معالجة معظم تلك الحالات بالطريق التأديبي أو فصل الموظف إذا لزم الأمر. وثانيًا، يمكن للهيئات التشريعية استصدار قوانين تحمي خصوصية المعلومات السرية وتطبيقها فيما يخص التعدي على البيانات الخاصة والمحمية وهو ما حدث بالفعل في عديد من الدول، فوجود قانون يخاطب هذه المسألة بشكل محدد سيكون أكثر عدالة وفعالية إذا ما قورن بالاعتماد على التفسيرات الفضفاضة لقوانين إساءة استخدام الكمبيوتر.[١٠]

وفي هذا الصدد من الضروري أن يشير التعليق إلى أحكام القضاء الإنجليزية فيما يتعلق بهذه المسألة كونه تعرض لمسألة «تجاوز حدود الدخول المصرح به» منذ تسعينيات القرن الماضي. ففي عام ١٩٩٧ وفي قضية مشابهة لقضية الحال قام رجل شرطة يدعى بول وزوجته فيكتوريا والتي أيضًا تعمل ضابط شرطة بالدخول لقاعدة بيانات الشرطة الوطنية لاستخلاص معلومات عن سيارة الشريك الحالي لزوجة بول السابقة، حيث قررت المحكمة الجزئية أن ما قام به الزوجان يعد خرقًا لقانون إساءة استخدام الكمبيوتر لعام ١٩٩٠ تحت بند «الدخول غير المرخص» ولكن الزوجان قاما بالطعن على الحكم أمام محكمة التاج مدعيين بأنه «بالرغم من أن الدخول للحصول على المعلومات كان لأسباب شخصية إلا أن الدخول بذاته كان بترخيص» وبالتالي ففعلهما لا يقع تحت تعريف «الدخول غير المرخص». قبلت محكمة التاج تظلم الزوجان، ولكن النيابة طعنت على الحكم أمام محكمة الاستئناف والتي رفضت الطعن المقدم من الأخيرة وأيدت حكم محكمة التاج. فتسبيب محكمة الاستئناف، والذي يتماشى مع ما ذهبت إليه المحكمة العليا بالولايات المتحدة، استند إلى أنه بالرغم من أن الغرض من الدخول من الممكن أن يكون غير مصرح به إلا أن الدخول في حد ذاته كان مصرحًا به مؤكدة على أن ذلك الأمر لا يحد من سلطة أصحاب العمل في التحكم في استخدام موظفيهم للكمبيوتر الخاص بالعمل وأنظمة الشركة، حيث يبقى الزوجان عرضة للخضوع لإجراءات تأديبية داخلية، بالإضافة لإمكانية محاكمتهم وفقًا لأحكام قانون حماية البيانات.[١١]

أيضًا يتفق هذا التعليق مع الآراء التي تؤكد على أن التطبيق الواسع لقوانين إساءة استخدام الكمبيوتر فيما يتعلق بتجاوز حدود الدخول المصرح به من شأنه أن يشجع الشركات على الانتقام من الموظفين المبلغين عن المخالفات التي تقوم بها شركاتهم حال تقديمهم أدلة، وصلوا لها عن طريق نظام الكمبيوتر الخاص بشركاتهم، عن تلك المخالفات للجهات المعنية. وهو ما قامت به بعض الشركات الأمريكية بالفعل عن طريق استخدام الشق المدني من قانون الاحتيال وإساءة استخدام الكمبيوتر في مهاجمة المبلغين من موظفي تلك الشركات والذين تحصلوا على بيانات من أنظمة الشركة التابعين لها وقدموها إلى الحكومة كدليل لدعم قضايا قانون الادعاءات الكاذبة.[١٢]

فالأمر لا يتوقف عند هذا الحد، بل يعد انتصارًا لكافة مستخدمي الانترنت لأن قرار المحكمة أغلق الباب أمام إمكانية الاستناد للمواد الجنائية بقانون الاحتيال وإساءة استخدام الكمبيوتر من قبل مقدمي الخدمات عبر الإنترنت «لفرض قيود على كيفية أو سبب استخدام خدمتهم، بما في ذلك لأغراض مثل جمع أدلة على

[10]David J. Rosen, 'Limiting Employee Liability Under the CFAA: A Code-Based Approach to "Exceeds Authorized Access"' (2012) 27 Berkeley Technology Law Journal 737-766

[11]Andrew Murray, Information Technology Law: The Law and Society (4th eds Oxford University Press 2019) 478; DPP v Bignell [1997] EWHC Admin 476

[12]Todd Yoder, Supreme Court Computer Access Decision has Positive Implications for Whistleblowers (The National Law Review, June 4, 2021) <https://www.natlawreview.com/article/supreme-court-computer-access-decision-has-positive-implications-whistleblowers> accessed 04 October 2021

التمييز العرقي وغيره من أشكال التمييز أو العنصرية أو تحديد نقاط الضعف الأمنية.» بالتالي، وعلى سبيل المثال، «إذا كانت إعلانات الإسكان متاحة لك كمستخدم على الانترنت، فليس من جريمة القرصنة أن تستخدمها في مشروعك البحثي عن التحيز في السكن، حتى لو كانت شروط الخدمة تحظر ذلك.» كذلك يعتبر القرار خبرًا سارًا للباحثين في مجال الأمن الإلكتروني، فعملهم يعد أمرًا حيويًا للمصلحة العامة حيث يعتمد على اكتشاف الثغرات الأمنية والابلاغ عنها للجهة المنوطة وهو ما قد يتطلب أحيانًا الدخول إلى أنظمة الكمبيوتر أو المواقع التي تقدم خدمات على الانترنت بطرق لا تتماشى مع شروط الخدمة.[١٣]

إضافة لذلك فعند الحديث عن مسألة «الدخول غير المصرح به» أو «تجاوز حدود الدخول المصرح به» للكمبيوتر نجد أن ما ذهب إليه الفقه والقضاء الأمريكي فيما يتعلق بتفسير وتحليل تلك الحالات يتمحور حول ثلاث منهجيات هم النهج القائم على الوكالة (Agency-Based Interpretation)والنهج القائم على العقد (Contract-Based Interpretation) وأخيرًا النهج القائم على الكود البرمجي .(Code-Based Interpretation)

ففيما يتعلق بالحالة الأولى فإن النهج القائم على الوكالة يستند إلى مبادئ الوكالة الموجودة في القانون العام والتي تفرض واجبات خاصة على الموظف غير موجودة في عقود الأداء، والتي منها أن الموظف مدين بالولاء لصاحب العمل، فهو مطالب بالتصرف فقط بالشكل الذي يخدم مصالح صاحب العمل. وتباعًا فإن سلطة الموظف في التصرف نيابة عن صاحب العمل تنتهي حال حصول الموظف على مصلحة معاكسة لمصالح صاحب العمل مثل أن يبدأ العمل لدى أحد المنافسين. بالتالي فإن تطبيق هذه المبادئ في سياق «تصريح الدخول» لموظف للكمبيوتر يصبح ملغي ضمنيًا إذا كان دخوله للكمبيوتر لأغراض لا تخدم مصالح صاحب العمل.[١٤]

أما النهج المستند للعقد فقد ظهر تحديدًا في الدعاوى المدنية، والذي يتطلب وجود عقد يحدد صراحة أو ضمنًا حدود التصريح المخول لمستخدم الكمبيوتر وحدوث انتهاك لهذا العقد من قبل الأخير وقد يتمثل هذا العقد في اتفاق سرية أو مدونة قواعد السلوك الخاصة بالشركة وما إلى ذلك. وهنا ينبغي أن نشير إلى أن اللغة المستخدمة في عقود العمل والوثائق الأخرى ذات الصلة قد تختلف اختلافًا كبيرًا فبعضها تشير بشكل غامض إلى ضرورة الحفاظ على السرية من قبل الموظفين وعدم إفشاء الأسرار التجارية والبعض الآخر ينص صراحة على أن الموظف غير مصرح له بالوصول إلى أو توزيع معلومات سرية محددة، فالمحاكم التي استندت لهذا التفسير أكدت أكثر من مرة على أهمية أن تكون العقود محددة وواضحة فيما يتعلق بهذه المسألة.[١٥]

أخيرًا ووصولًا للنهج الثالث القائم على الكود البرمجي فيستند بشكل أساسي على مفهوم تشغيل أنظمة الكمبيوتر، فالدخول لجهاز الكمبيوتر يكون غير مصرح به إذا تجاوز المستخدم بشكل غير شرعي أحد الحواجز البرمجية (مثل كلمة المرور) المصممة إما للحد من دخول المستخدمين لجهاز الكمبيوتر أو لقصر الدخول على أجزاء محددة من الكمبيوتر دون غيرها. فالدخول يصبح غير شرعي حال قيام الشخص باستخدام كلمات مرور مسروقة أو تخمين كلمة المرور للدخول لجهاز الكمبيوتر أو لدخول منطقة محددة في الكمبيوتر محمية بكلمة

[13]Aaron Mackey and Kurt Opsahl, 'Van Buren is a Victory Against Overbroad Interpretations of the CFAA, and Protects Security Researchers' (Electronic Frontier Foundation, June 3, 2021) <https://www.eff.org/deeplinks/2021/06/van-buren-victory-against-overbroad-interpretations-cfaa-protects-security> accessed 10 October 2021

[14]Katherine Mesenbring Field, 'Agency, Code, or Contract: Determining Employees' Authorization under the Computer Fraud and Abuse Act' (2009) 107 Michigan Law Review 819-852

[15]Ibid

مرور. هذا النهج يقصر الحالات التي يعد فيها الدخول غير مرخص على الحالات التي «يتلاعب فيها المستخدم صراحة بنظام الكمبيوتر لمنحه امتيازات وصول واستخدام أكبر مما كان سيحصل عليه بخلاف ذلك»، فبناءً على النهج القائم على الكود البرمجي، لا يمكن اتهام المستخدم أو الموظف بتجاوز الحق في الاستخدام طالما أن الأخير كان لديه ترخيص يمكنه من «الوصول إلى قاعدة البيانات أو نظام الكمبيوتر»، حتى وإن استخدم حقه في الوصول لغرض غير مناسب أو غير متصل بمتطلبات الوظيفة أو غرض غير شرعي.[١٦]

يرى هذا التعليق أن المحكمة في القضية محل التعليق وإن كانت قد أصابت في رأيها إلا أن امتناعها عن تبني النهج القائم على الكود البرمجي بشكل صريح يترك الكثير من العمل للمحاكم المستقبلية،[١٧] لذلك يرى التعليق أنه كان يجب على المحكمة الاعتماد على النهج الثالث فيما يتعلق بجرائم إساءة استخدام الكمبيوتر، فالنهج القائم على الكود البرمجي يتوافق مع أهداف قانون الاحتيال وإساءة استخدام الكمبيوتر الأمريكي وغيره من قوانين مكافحة الجرائم الإلكترونية والتي صممت بشكل رئيسي لمواجهة جرائم إساءة استخدام الكمبيوتر وليس الجرائم التقليدية التي يُستخدم فيها الكمبيوتر، فهو يركز بشكل كامل على الأفعال التي من شأنها أن تمس بسلامة نظام الكمبيوتر.[١٨]

أخيرًا، فالتأثير العملي للاعتماد على النهج القائم على الكود البرمجي هو تحجيم نطاق قوانين إساءة استخدام الكمبيوتر وتركيز تطبيقها على الحالات الأساسية، وذلك على النقيض من النهج الأول القائم على الوكالة والثاني القائم على العقد والذين لا يتماشيا مع أهداف تلك القوانين التي تستهدف جرائم إساءة استخدام الكمبيوتر بل قد ينتج عن تبنيهما إساءة استعمال تلك القوانين بطرق مختلفة ومثيرة للقلق، فعلى سبيل المثال قد يتمكن صاحب العمل من مقاضاة أحد موظفيه جنائيًا لقيامه باستخدام كمبيوتر الشركة للبحث عن وظيفة أخرى لدى شركة منافسة أو مشاهدته لليوتيوب بل قد تصل إلى إمكانية أن يقاضي مالك موقع إلكتروني أحد الأشخاص التابعين للحزب الديمقراطي لقيامه باستخدام الموقع الخاص به على الرغم من أن أحكام وشروط الموقع تنص على عدم جواز الدخول للموقع إلا من قبل أعضاء الحزب الجمهوري فقط. فاتباع النهج القائم على الكود البرمجي يرسم خطًا أكثر توازنًا بحيث يسمح لمستخدمي الإنترنت باستخدام الإنترنت وزيارة مواقع الويب وإرسال رسائل البريد الإلكتروني دون التخوف من أي عقوبات جنائية محتملة قد تنشأ نتيجة خرق شروط الخدمة أو شروط الاستخدام أو غيرها من الشروط التعاقدية، دون الانتقاص من الحماية اللازمة لضمان سلامة أنظمة الكمبيوتر والبيانات المحمية والمحفوظة عليها.[١٩]

الخاتمة

في الختام، يرى التعليق أن المحكمة أحسنت برفضها استخدام القياسات التي تعتمد على النظريات القانونية المرتبطة بالعالم المادي باستخدامها لتفسير وتطبيق قوانين تم استحداثها لتنظيم العالم الرقمي، حيث إنه من

[16]Orin S. Kerr, 'Cybercrime's Scope: Interpreting "access" and "authorization" in Computer Misuse Statutes' (2003) 78 New York University Law Review 1596-1668

[17]Will Duffield, 'Van Buren Decision Is a Step in the Right Direction' (Cato Institute, 14 June 2021) <https://www.cato.org/blog/van-buren-decision-step-right-direction> accessed 04 October 2021

[18]Katherine Mesenbring Field, 'Agency, Code, or Contract: Determining Employees' Authorization under the Computer Fraud and Abuse Act' (2009) 107 Michigan Law Review 819-852

[19]Orin S. Kerr, 'Cybercrime's Scope: Interpreting "access" and "authorization" in Computer Misuse Statutes' (2003) 78 New York University Law Review 1596-1668

المؤكد وجود اختلافات جوهرية بين العالمين حتى وإن تشابها في بعض النقاط، فتلك القياسات المغالِطة قد أدت في الماضي إلى بعضٍ من أخطر أشكال إساءة استخدام القانون محل النظر والقوانين المماثلة في مواجهة مستخدمي الانترنت والموظفين وأعاقت البحوث الأمنية المهمة والصحافة الاستقصائية، لذا فالقرار يأتي متماشيًا مع مقتضيات العصر الرقمي الذي نعيشه حاليًا، ويعد مكسبًا للكافة.

في النهاية يود أن يشير التعليق إلى قانون جرائم تقنية المعلومات المصري رقم ١٧٥ لعام ٢٠١٨، وبالتحديد إلى المادة رقم ١٥ والمتعلقة بجريمة «تجاوز حدود الحق في الدخول»، حيث إن المادة قصرت تحقق تلك الجريمة فقط على الشخص الذي يتعدى «حدود [حقه في الدخول] من حيث الزمان أو مستوى الدخول»، وبما أن اللائحة التنفيذية لم تأت بجديد في هذا الصدد، وبالأخص ما يعنيه «مستوى الدخول»، فمن المحتمل بشكل كبير ألا يمتد تطبيق نص المادة الحالي على الشخص الذي قد يستخدم حقه في الدخول لغرض غير مشروع، وهو ما يراه التعليق مساحة مشجعة للباحثين على دراسة تلك المسألة في ضوء الفقه والقضاء والتشريع المصري.