ارتباطات خفية:

اتساع التعاون بين شركات التكنولوجيا وأجهزة الأمن الغربية

إيهاب خليفة
رئيس وحدة التطورات التكنولوجية، المستقبل للأبحاث والدراسات المتقدمة، أبوظبي

أبرمت شركات التكنولوجيا الأمريكية، مثل جوجل وأمازون عقوداً مع وزارة الدفاع الأمريكية، ما يكشف عن مدى العلاقة بين الجانبين، والتي تتعدى أحياناً تحقيق مصالح برجماتية للطرفين، ولكنها تمتد أحياناً إلى وجود ارتباطات مؤسسية، وهو النمط الذي تتبناه الصين وروسيا، خاصة مع تحوّل التكنولوجيا إلى أحد مقومات قوة الدولة.

يسعى هذا التحليل إلى إلقاء الضوء على أهمية شركات التكنولوجيا باعتبارها أحد عناصر قوة الدولة، وذلك من خلال التركيز على الحالة الأمريكية بصورة أساسية، فضلاً عن توضيح أبرز أشكال التعاون بين الطرفين، وأخيراً الإشارة إلى المعضلات الأخلاقية التي تترتب على مثل هذا التعاون.

أولاً: التكنولوجيا كأحد عناصر قوة الدولة

تمتلك شركات التكنولوجية قوة مؤثرة في عصر الإنترنت والبيانات الضخمة (Big Data)، بالنظر إلى سيطرتها على كم هائل من البيانات والمعلومات الخاصة بالأفراد، بصورة تنافس، إن لم تكن تفوق حجم البيانات التي تملكها الحكومات عن مواطنيها، فهي تعرف عاداتهم الشخصية واحتياجاتهم اليومية وشبكة علاقاتهم الشخصية، وكذلك المعارف والأصدقاء وما يدور بأفكارهم، بل وقد تتوقع ما قد يشغلهم مستقبلاً.

ويتميز العصر الحالي بظاهرة الثورة المعرفية والتكنولوجية والقائمة على المعلومات، والتي أزاحت وحيدت الكثير من عناصر القوة التقليدية عن مواقعها، وباتت المعلومة في حد ذاتها مصدراً للقوة، فمن يمتلك المعلومة هو الذي يمتلك السبق في كل شيء، اقتصادياً وعسكرياً وسياسياً، ولما كانت شركات التكنولوجيا العملاقة مثل جوجل وميكروسوفت وأمازون وفيس بوك وغيرها هي التي تمتلك المعلومات، فكان من الضروري أن تكون محل اهتمام الأجهزة الأمنية كافة للدول التابعة لها هذه الشركات، وأن يحدث تعاون بينهما.

ولا تتوقف أهمية شركات التكنولوجيا على ما تمتلكه من معلومات وبيانات مهمة عن مستخدميها، ولكن كذلك إلى أهميتها كأحد عناصر قوة الدولة. فقد تمثلت معايير قياس قوتها في الناتج المحلي الإجمالي، وحجم السكان، والإنفاق الدفاعي، غير أن هناك اتجاهاً متصاعداً في الأدبيات العسكرية لإضافة بعد جديد، وهو الإبداع التكنولوجي (Innovation in Technology)، باعتباره أحد المؤشرات الرئيسية على قوة الدولة، وذلك على الرغم من الصعوبة الشديدة في تطوير معايير واضحة لقياسه[1].

ثانياً: علاقة تأسيسية مع وادي السيليكون

تعد العلاقة بين وكالات الاستخبارات الأمريكية

ووادي السيليكون قديمة، وترجع إلى ما قبل فترة تأسيسه. ففي نهاية الحرب العالمية الثانية، حصل البروفيسور "فريدريك تريمان" على عقود من وزارة الدفاع الأمريكية لتأسيس معامل ومختبرات في جامعة ستنافورد، التي كان يترأسها، وذلك للعمل على مشروعات خاصة بوزارة الدفاع، وكانت هذه المختبرات نواة لتأسيس "مجمع ستانفورد الصناعي" (Stanford Industrial Park) في بداية الخمسينيات من القرن العشرين، والتي تحوّلت فيما بعد إلى "مجمع ستانفورد للأبحاث".

وعمل فريدريك تريمان على تشجيع طلابه لتأسيس شركاتهم الخاصة في المنطقة، وقامت الجامعة بتأجير بعض أراضيها لهذه الشركات، ثم انتقلت إليها أيضاً كبريات الشركات الأمريكية العاملة في مجال التكنولوجيا، مثل "هوليت-باكارد" (Hewlett-Packard)، و"إيستمان كوداك" (Eastman Kodak)، و"جنرال إلكتريك" (General Electric)، و"شركة لوكهيد" (Lockheed Corporation)، والتي كانت نواة لتأسيس السيليكون فالي في مرحلة تالية[2].

واعتمدت هذه الشركات، بصورة أساسية، على العقود التي أبرمتها مع وزارة الدفاع الأمريكية، فمثلاً أبرمت الأخيرة عقوداً مع شركة مثل "فارين أسوسياتس" (Varian Associates) وشركات أخرى ناشئة، في خمسينيات القرن الماضي للعمل على تكنولوجيات، خاصة بموجات الراديو والمايكرويف والرادارات، كما كانت وكالة الاستخبارات المركزية أول عميل لشركة قواعد البيانات العملاقة "أوراكل" (Oracle). وخلال فترة محدودة أصبحت وكالة ناسا ووزارة الدفاع وأجهزة الاستخبارات، خاصة وكالة الاستخبارات المركزية ووكالة الأمن القومي، من أكبر عملاء شركات وادي السيليكون[3].

وكشفت تسريبات "إدوارد سنودن" (Edward Snowden) في يونيو 2013، عن مدى نفوذ وكالة الأمن القومي الأمريكي على شركات التكنولوجيا العملاقة في الولايات المتحدة. فقد تمكنت الوكالة من خلال برنامج "بريزم" (PRISM)، وبالتعاون مع كبريات شركات التكنولوجيا، بما فيها الفيس بوك وجوجل ومايكروسوفت وآبل وغيرها، من الحصول على البيانات والمعلومات كافة التي تمتلكها هذه الشركات عن أي من مستخدميها، حيث يستطيع هذا البرنامج الحصول على معلومات تتضمن، رسائل البريد الإلكتروني، ومحادثات الفيديو والصوت، والصور، وعمليات نقل الملفات، وإخطارات الولوج وغيرها من التفاصيل المتاحة عبر الشبكات الاجتماعية[4].

ثالثاً: أنماط العلاقة بين الطرفين

تأخذ العلاقة بين الشركات التكنولوجية والأجهزة الأمنية أنماطاً متعددة، منها ما هو معلن، مثل القيام بتصميم أسلحة وبرمجيات تجسس للأجهزة الأمنية عبر مشروعات رسمية، ومنها ما هو غير معلن، مثل إبلاغ هذه الأجهزة بالثغرات الموجودة في الأنظمة قبل معالجتها حتى تستطيع استغلالها واختراق الخصوم من خلالها، أو القيام بزرع تقنيات تجسس وأبواب خلفية لصالح هذه المؤسسات في الأجهزة التي تصدرها لبعض العملاء، أو الاستحواذ على شركات أخرى بطلب من المؤسسات الأمنية لتعزيز احتكارها السوق في التقنيات فائقة التقدم، وتوضح السطور القادمة هذه الأنماط بمزيد من التفاصيل:

1- تسهيل عمليات التجسس: تعد من أبرز الأنماط التي تتعاون فيها المؤسسات الأمنية مع شركات التكنولوجيا القيام بعمليات تجسس واختراق خارجي لصالح هذه المؤسسات، فمنذ عدة سنوات قامت وكالة الاستخبارات الأمريكية برشوة مدير إحدى الشركات التكنولوجية لزرع شرائح تجسس إلكترونية في أجهزة سوف تباع لإحدى الدول، وذلك مقابل الحصول على مبلغ 50 ألف دولار، وبالفعل قامت الشركة بزرع شريحة تجسس مشابهة تماماً لإحدى الشرائح الأخرى بالأجهزة[5].

وفي حين تتم التفاهمات بين الجانبين بصورة مباشرة، فإنها في بعض الأحيان الأخرى، تتم بصورة غير مباشرة، عبر شركات الطرف الثالث. وغالباً ما يتم اللجوء إلى هذا الأسلوب بهدف رفع الحرج عن الشركات الكبرى، وتجنب التأثير سلباً على مبيعاتها الخارجية، إذا ما تم اكتشاف تورطها مع الاستخبارات الأمريكية في التجسس عليهم.

فقد ذكر أحد عناصر وكالة الاستخبارات المركزية أنه في العقد الأول من القرن الواحد والعشرين، قامت الحكومة الأمريكية بإنشاء شركة لإعادة بيع أجهزة كمبيوتر ولاب توب إلى الحكومات الآسيوية، وقامت هذه الشركة بشراء الأجهزة من شركة تدعى حينها "تادبول كمبيوتر" (Tadpole Computer)، ثم قامت بزرع برمجيات تجسس بداخلها تسمح لوكالة الاستخبارات باختراقها عن بعد، وذلك قبل إعادة بيعها لبعض الحكومات الآسيوية[6].

ومن الصور غير المباشرة أيضاً طلب الحصول على الأكواد الخاصة بأي برمجيات يتم تقديمها للهيئات الحكومية من أجل فحصها، ومراجعتها، والتأكد من خلوها من الثغرات، أو الأبواب الخلفية، وذلك لتأمين المؤسسة المستخدمة لهذه البرامج من التجسس الخارجي، غير أنها في واقع الأمر تقوم بتوظيف الثغرات المكتشفة في اختراق أي جهات، محلية أو دولية، تشتري هذه البرامج فيما بعد[7].

وكشفت تحقيقات أخرى لوكالة رويترز للأنباء وبلومبيرج أن شركات تكنولوجية كبرى مثل مايكروسوفت تقوم بإبلاغ وكالات الأمن القومي الأمريكي بالثغرات الموجودة في نظم تشغيلها قبل معالجتها أو الإعلان عنها، وذلك بهدف إعطاء الفرصة للوكالة للاستفادة من هذه الثغرة في التجسس على آخرين، سواء دولاً أو أفراداً، وهو ما تنفيه هذه الشركات على الدوام[8].

ويثار في هذا الإطار كذلك الخلل الفني الذي تم اكتشافه في برنامج "فيس تايم" (FaceTime)، الذي تنتجه شركة آبل الأمريكية، والذي يتيح للمستخدمين الاستماع إلى الأشخاص الذين يتصلون بهم، وحتى مشاهدتهم من خلال

الكاميرا الأمامية، من دون أن يجيب الشخص الآخر على المكالمة. وعلى الرغم من أنه تم إبلاغ الشركة بهذه الثغرة، فإن التباطؤ في إصلاحها جدد الشكوك في مدى التزامها بأمن مستخدميها[9].

2- تطوير برامج عسكرية: قامت جوجل بتطوير برامج لصالح وزارة الدفاع الأمريكية تحت مسمى "مشروع مافن" (Project Maven)، والذي كشف عن قيام شركة جوجل سراً بالعمل على تقنيات ذكاء اصطناعي لزيادة قدرات الأسلحة الأمريكية، حيث طوّرت برامج قادرة على تحليل صور الفيديو، بما يرفع من كفاءة الطائرات المسيّرة (الدرونز) على استهداف الأفراد المراد تصفيتهم، أو المباني التي سيتم تدميرها.

وعلى الرغم من إعلان الشركة تراجعها عن تجديد تعاقدها مع وزارة الدفاع الأمريكية، والذي ينتهي عام 2019، بسبب تهديد العديد من العاملين بالاستقالة، فإن هناك العديد من الشركات التكنولوجية الكبرى العاملة في المجال نفسه، مثل شركة "أمازون"، والتي لاتزال تقوم بتطوير تقنيات لصالح وزارة الدفاع الأمريكية[10].

وفي بريطانيا أعلن "صندوق الاستثمار الاستراتيجي للأمن القومي" (National Security Strategic Investment Fund) عن تعزيز الاستثمار في قطاع تكنولوجيا الأمن في ميزانية عام 2017، وذلك بمبلغ 85 مليون جنية استرليني، وتعد هذه هي المرة الأولى التي يعلن فيها جهاز الاستخبارات الخارجي البريطاني (MI6) عن توجيه استثمارات في القطاع الخاص. وتتمثل المجالات الرئيسية للاستثمار في تحليل البيانات والذكاء الاصطناعي وتكنولوجيا تتبع المعلومات المالية وتحديد هوية الأفراد[11].

3- تمويل برامج ومشرعات أمنية واستخباراتية: تقوم الأجهزة الأمنية بتمويل المشروعات الواعدة التي ترى فيها إمكانية للاستفادة منها مستقبلاً، سواء كان ذلك تمويلاً مباشراً عبر برنامج المسار السريع (Fast-Track) الذي قامت "وكالة مشاريع البحوث المتطورة الدفاعية" "داربا" (Defense Advanced Research Projects Agency) بإنشائه بهدف إتاحة تمويل سريع وصغير للشركات الناشئة المهمة، أو عبر تشجيع شركات كبرى على الاستحواذ عليها وتمويل هذه المشروعات[12].

كما تقوم المؤسسات الأمنية والشركات التكنولوجية الكبرى بالدخول في شراكة للاستثمار في بعض التقنيات الواعدة، أو الشركات الناشئة، التي تتخصص في مجال يخدم مجالات عمل أجهزة الاستخبارات، فمثلاً قامت شركة "إن-كيو-تيل" (In-q-tel)، الذراع الاستثمارية لوكالة الاستخبارات المركزية الأمريكية، بالدخول في شراكة مع جوجل للاستثمار في شركة "ريكورديد فيوتشر" (Recorded Future)، والتي كانت تقوم بابتكار برمجيات تعمل على تحليل البيانات المتوفرة من المصادر العلنية، مثل وسائل الإعلام ومواقع الإنترنت ومواقع التواصل الاجتماعي، بهدف زيادة القدرة على التنبؤ بالأحداث التي يمكن أن تقع في المستقبل القريب[13].

وفي المقابل، تشجع المؤسسات الأمنية هذه الشركات على توظيف العسكريين المتقاعدين وعناصر الاستخبارات في مجالس إدارة الشركات، وتكوين علاقات شخصية مع كبار المديرين التنفيذيين في شركات التكنولوجيا الكبرى، وذلك بهدف امتلاك أوراق ضغط وتأثير على توجهات هذه الشركات.

4- تحجيم الشركات المهددة للأمن القومي: ترتاب الحكومات من شركات التكنولوجيا الأجنبية، التابعة لدول معادية، إذ غالباً ما تتهمها بالتورط في أنشطة لصالح حكومتها، كما في اتهام واشنطن شركة "كاسبرسكي لاب" في أواخر عام 2017 بامتلاكها علاقات وثيقة مع وكالات الاستخبارات في موسكو، وإقدامها على إزالة برامج مكافحة الفيروسات التابعة للشركة من المؤسسات الحكومية كافة، إذ ترى وزارة الأمن الداخلي الأمريكية أن الشركة مجبرة، بموجب القانون الروسي، على التعاون مع وكالات المخابرات الروسية، فضلاً عن توظيفها من قبل موسكو في اعتراض الاتصالات التي تعبر الشبكات الروسية[14].

> تكشف تحقيقات لوكالة رويترز للأنباء وبلومبيرج أن شركات تكنولوجية كبرى مثل مايكروسوفت تقوم بإبلاغ وكالات الأمن القومي الأمريكي بالثغرات الموجودة في نظم تشغيلها قبل معالجتها أو الإعلان عنها، وذلك بهدف إعطاء الفرصة للوكالة للاستفادة من هذه الثغرة في التجسس على آخرين، سواء دولاً أو أفراداً، وهو ما تنكره هذه الشركات على الدوام.

وفي الإطار نفسه، اعتقلت السلطات الكندية، بناء على طلب من الحكومة الأمريكية، "منج وانزو" المديرة المالية لشركة هواوي، عملاق صناعة الاتصالات الصينية، في ديسمبر 2018، وذلك نظراً لانتهاكها العقوبات الأمريكية ضد إيران، فضلاً عن تورط شركتين تابعتين لهواوي في سرقة تكنولوجيا مرتبطة بصناعة الروبوتات من شركة "تي- موبايل" الأمريكية[15].

وتتوافق الاتهامات مع تلك التي يوجهها المشرعون الأمريكيون للشركة بأنها تشكل تهديداً للأمن القومي الأمريكي، معتبرين أن التكنولوجيا التي تستخدمها يمكن أن توظَّف للتجسس من قبل الحكومة الصينية، كما لا يمكن فصل هذه الاتهامات عن الصراع من أجل الهيمنة على التكنولوجيات الفائقة بين الصين، التي تسعى لتقود العالم في مجال التكنولوجيات فائقة التقدم، وبين الولايات المتحدة الأمريكية التي تحاول الحفاظ على مكانتها في مواجهة الأولى.

وتكمن خطورة شركة هواوي بالنسبة للأجهزة الأمنية الأمريكية في عدة أمور، فهي من كبريات الشركات المصنعة لتقنيات الجيل الخامس للإنترنت، والتي تعتمد عليه تقنيات الذكاء الاصطناعي وإنترنت الأشياء، كما تُعتبر شركة هواوي أكبر منتج لمعدات الاتصالات في العالم، وثالث أكبر مورّد للهواتف الذكية، وصاحبة عدد هائل من مكاتب البحث والتطوير، ومالكة لعشرات الآلاف من براءات الاختراع.

فقد تمكنت شركة هواوي من أن تصبح أكبر شركة صينية

لإنتاج معدات الاتصالات في العالم، حيث تنتشر منتجاتها في أكثر من 170 دولة، وتمكنت الشركة، حتى يناير عام 2017، من الحصول على 74.307 براءات اختراع، والتقديم على 64.091 براءة اختراع في الصين، و48.758 براءة اختراع خارج الصين. كما أصبحت هواوي الشركة الصينية الوحيدة التي أدرجت علامتها التجارية في تصنيف "فوربس" السنوي لأعلى العلامات التجارية قيمة بالعالم في عام 2018 للعام الثاني على التوالي، حيث بلغت قيمة علامتها التجارية 8.4 مليار دولار أمريكي. ولذلك لا يمكن استبعاد أن توقيف المديرة المالية للشركة وابنة مالكها "منج وانزو" في إطار التصعيد ضد الشركات التكنولوجية الصينية، التي قد تشكل خطراً على المصالح الأمريكية على المدى الطويل.

ومن جانب آخر، تلجأ الدول إلى منع الشركات الأجنبية من السيطرة على الشركات الوطنية، التي تعمل في مجالات تتعلق بالأمن القومي، ومن ذلك منع الرئيس الأمريكي دونالد ترامب شركة "برودكوم ليميتد" السنغافورية من محاولتها الاستحواذ على شركة "كوالكوم" في صفقة تاريخية تُقدر بـ142 مليار دولار أمريكي على خلفية اتهامات بإضعاف المنافسة الأمريكية لصالح الصين[16].

5- رسم خريطة التفاعلات السيبرانية: يتمثل أحد الأنماط الرئيسية للتعاون بين شركات التكنولوجيا وأجهزة الاستخبارات، مثل "وكالة الأمن القومي" في إمداد الأجهزة المعنية بتقارير وبيانات وإحصاءات حول حالة الأمن السيبراني في العالم، وتحديد مصادر الاختراقات الرئيسية، والفواعل الرئيسية التي تقف خلفها، بالإضافة إلى تقييم درجة خطورة القوى الخارجية التي قد تشكل تهديداً محتملاً للأمن القومي الأمريكي[17].

رابعاً: التداعيات الأخلاقية

عادة ما يثير تعاون الشركات التكنولوجية، مثل جوجل وأمازون وميكروسوفت مع المؤسسات الأمنية والدفاعية إشكاليات أخلاقية كبيرة، خاصة أن عملها لا يقتصر على التعاون مع هذه المؤسسات، بل يمتد إلى المستخدمين المدنيين حول العالم.

ويطرح ما سبق تساؤلات حول حدود التعاون بين هذه الشركات والمؤسسات الأمنية والعسكرية، وحجم التداخل بين التقنيات التي توفرها للمدنيين، وتلك التي توفرها للعسكريين، فضلاً عن تحديد ماهية القواعد الأخلاقية الخاصة بتطوير هذه الشركات تقنيات عسكرية متقدمة للمؤسسات الأمنية، وإذا ما كان تطوير هذه الشركات تقنيات الذكاء الاصطناعي يتسبب في استهداف وقتل البشر، أم أنه قد يستخدم في الحفاظ على حياتهم داخل المعارك العسكرية، وأخيراً مدى تشارك هذه الشركات لما يتوافر لديها من معلومات حول مستخدميها مع الأجهزة الأمنية.

ومع ذلك، فقد أثار مشروع "مافن"، على سبيل المثال، ضجة داخل شركة جوجل، دفعت الكثير من المطورين والمحللين داخل الشركة للاعتراض على المشاركة في تقنيات قد توظف عسكرياً، الأمر الذي دفع الشركة إلى الإعلان عن عدم تجديدها لعقدها مع وزارة الدفاع الأمريكية بعد انتهائه، كما أعلنت الشركة عن سبعة مبادئ رئيسية تحكم عملها في مجال تطوير تقنيات الذكاء الاصطناعي في محاولة لامتصاص غضب العاملين من التعاون مع جهات عسكرية[18].

ومع ذلك، فإنه لا ينبغي تجاهل استمرار دخول شركات التكنولوجيا الأخرى في تعاون عسكري مع وزارة الدفاع الأمريكية، خاصة مع احتفاظ كل شركات التكنولوجيا تقريباً، بما في ذلك شركة جوجل، بعلاقات تعاونية قوية مع الأجهزة الأمنية والعسكرية في دولها، بل ومن المتوقع أن يزداد هذا التعاون في ضوء تبني الدول الأخرى، خاصة روسيا والصين المسلك نفسه، فضلاً عن الطبيعة المزدوجة الاستخدام للتكنولوجيا، أي إمكانية استخدامها في الجوانب المدنية والعسكرية على حد سواء.

وأخيراً لا ينبغي إغفال تحوّل القدرات التكنولوجية إلى أحد معايير قوة الدولة، وهو ما يعني أن الدول الكبرى لن تتنازل عن أحد مقومات قوتها، وستسعى للحفاظ عليه بكل الوسائل، وتنميته عبر الدخول في شراكات مع أي جهة لتعزيز قدراتها في هذا المجال.

1- Gregory F. Treverton and Seth G. Jones, **Measuring National Power,** (Santa Monica: Rand Corporation: 2005), p. ix.
2- Joseph Menn, Strong ties bind spy agencies and Silicon Valley, **Reuters,** July 3, 2013, accessible at: https://reut.rs/2B4zhLV (Last accessed: December 12, 2018).
3- Joseph Menn, **Op.cit.**
4- NSA Prism program slides, **The Guardian,** November 5, 2013, accessible at: https://bit.ly/1qmj46r (Last accessed: December 20, 2018).
5- Joseph Menn, **Op.cit.**
6- **Ibid.**
7- **Ibid.**
8- Carl Franzen, Tech companies are cooperating with US intelligence agencies more than you think, **The verge,** July 4, 2013, accessible at: https://bit.ly/2HAYbZi (Last accessed: December 14, 2018).
9- Nicole Perlroth, Apple Was Slow to Act on FaceTime Bug That Allows Spying on iPhones, **The New York Times,** January 29, 2019, accessible at: https://nyti.ms/2TkGFKh
10- Ryan Jenkins, When it comes to AI and weapons, the tech world needs philosophers, **Washington Post,** June 12, 2018, accessible at: https://wapo.st/2sS3fi3 (Last accessed: December 14, 2018).
11- Tech companies targeted in mission to develop new spy tools, **Financial Times,** accessible at: https://on.ft.com/2Q6l4mV (Last accessed: December 15, 2018).
12- Joseph Menn, **Op.cit.**
13- Silicon Valley And The Intelligence Agencies, **Fast Company,** October 6, 2013, accessible at: https://bit.ly/2BaDRs8 (Last accessed: December 16, 2018)
14- الحكومة الأمريكية تأمر بإزالة برامج "Kaspersky" من أجهزة وكالاتها.. والسبب؟، **سي إن إن عربي**، 16 سبتمبر 2017، موجود على الرابط التالي: https://cnn.it/2B8PRdM
15- واشنطن تتهم هواوي بسرقة تكنولوجيا وانتهاك العقوبات على إيران، **جريدة البيان**، 29 يناير 2019، موجود على الرابط التالي: https://bit.ly/2DHkVD9
16- Cecilia Kang and Alan Rappeport, Trump Blocks Broadcom's Bid for Qualcomm, **New York Times,** March 12, 2018, accessible at: https://nyti.ms/2FMVSjO
17- Carl Franzen, **Op.cit.**
18- Sundar Pichai, AI at Google: our principles, **Google Blog,** June 7, 2018, accessible at: https://bit.ly/2Kjn39e (Last accessed: December 17, 2018)