المعهد القومى للملكية الفكرية
The National Institute of Intellectual Property
Helwan University, Egypt

المجلة العلمية للملكية الفكرية وإدارة الابتكار

دورية نصف سنوية محكمة يصدرها

المعهد القومي للملكية الفكرية

جامعة حلوان

العدد الثالث
يوليو٢٠٢٠

الهدف من المجلة:

تهدف المجلة العلمية للملكية الفكرية وإدارة الابتكار إلى نشر البحوث والدراسات النظرية والتطبيقية فى مجال الملكية الفكرية بشقيها الصناعي والأدبي والفني وعلاقتها بإدارة الابتكار والتنمية المستدامة من كافة النواحي القانونية والاقتصادية والادارية والعلمية والأدبية والفنية.

ضوابط عامة:

- تعبر كافة الدراسات والبحوث والمقالات عن رأى مؤلفيها ويأتي ترتيبها بالمجلة وفقا لإعتبارات فنية لا علاقة لها بالقيمة العلمية لأى منها.
- تنشر المقالات غير المحكمة (أوراق العمل) فى زاوية خاصة في المجلة.
- تنشر المجلة مراجعات وعروض الكتب الجديدة والدوريات.
- تنشر المجلة التقارير والبحوث والدراسات الملقاه في مؤتمرات ومنتديات علمية والنشاطات الأكاديمية في مجال تخصصها دونما تحكيم في أعداد خاصة من المجلة.
- يمكن الاقتباس من بعض مواد المجلة بشرط الاشارة إلى المصدر.
- تنشر المجلة الأوراق البحثية للطلاب المسجلين لدرجتى الماجستير والدكتوراه.
- تصدر المجلة محكمة ودورية نصف سنوية.

ألية النشر فى المجلة:

- تقبل المجلة كافة البحوث والدراسات التطبيقية والأكاديمية في مجال حقوق الملكية الفكرية بكافة جوانبها القانونية والتقنية والاقتصادية والادارية والاجتماعية والثقافية والفنية.
- تقبل البحوث باللغات (العربية والانجليزية والفرنسية).
- تنشر المجلة ملخصات الرسائل العلمية الجديدة، وتعامل معاملة أوراق العمل.
- يجب أن يلتزم الباحث بعدم إرسال بحثه إلى جهة أخرى حتى يأتيه رد المجلة.
- يجب أن يلتزم الباحث بإتباع الأسس العلمية السليمة في بحثه.
- يجب أن يرسل الباحث بحثه إلى المجلة من ثلاثة نسخ مطبوعة، وملخص باللغة العربية أو الانجليزية أو الفرنسية، فى حدود ٨ ـ ١٢ سطر، ويجب أن تكون الرسوم البيانية والإيضاحية مطبوعة وواضحة، بالإضافة إلى نسخة إلكترونية Soft Copy، ونوع الخط Romanes Times New ١٤ للعربى، و١٢ للانجليزي على B5 (ورق نصف ثمانيات) على البريد الالكتروني: ymgad@niip.edi.eg
- ترسل البحوث إلى محكمين متخصصين وتحكم بسرية تامة.
- في حالة قبول البحث للنشر، يلتزم الباحث بتعديله ليتناسب مع مقترحات المحكمين، وأسلوب النشر بالمجلة.

مجلس إدارة تحرير المجلة	
أ.د. ياسر محمد جاد الله محمود	أستاذ الاقتصاد والملكية الفكرية وعميد المعهد القومي للملكية الفكرية (بالتكليف) - رئيس تحرير المجلة
أ.د. أحمد عبد الكريم سلامة	أستاذ القانون الدولي الخاص بكلية الحقوق بجامعة حلوان والمستشار العلمي للمعهد - عضو مجلس إدارة تحرير المجلة
أ.د. وكيل المعهد للدراسات العليا والبحوث	سكرتير تحرير المجلة
أ.د. جلال عبد الحميد عبد اللاه	أستاذ الهندسة الانشائية بكلية الهندسة بالمطرية بجامعة حلوان - عضو مجلس إدارة تحرير المجلة
أ.د. هناء محمد الحسيني	أستاذ علوم الأطعمة بكلية الاقتصاد المنزلي بجامعة حلوان - عضو مجلس إدارة تحرير المجلة
أ.د. وزير مفوض/ مها بخيت محمد زكي	مدير إدارة الملكية الفكرية والتنافسية بجامعة الدول العربية - عضو مجلس إدارة تحرير المجلة
اللواء أ.د. عبد القدوس عبد الرزاق العبيدلي	رئيس مجلس إدارة جمعية الامارات للملكية الفكرية - عضو مجلس إدارة تحرير المجلة
Prof Dr. Alexander Peukert	أستاذ القانون المدنى بجامعة جوته فرانكفورت أم ماين – ألمانيا - عضو مجلس إدارة تحرير المجلة
Prof Dr. Andrew Griffiths	أستاذ القانون التجارى بجامعة نيو كاسل - بريطانيا - عضو مجلس إدارة تحرير المجلة

المراسلات

ترسل البحوث إلى رئيس تحرير المجلة العلمية للملكية الفكرية وإدارة الابتكار بجامعة حلوان
جامعة حلوان - ٤ شارع كمال الدين صلاح - أمام السفارة الأمريكية بالقاهرة -جاردن سيتى
ص.ب: ١١٤٦١ جاردن سيتي
ت: ٠٢٠٢ ٢٥٤٨١٠٥٠ + محمول: ٠٢٠١٠٠٠٣٠٠٥٤٨ + ف: ٠٢٠٢ ٢٧٩٤٩٢٣٠ +
http://www.helwan.edu.eg/niip/
ymgad@niip.edu.eg

المعلومات غير المفصح عنها والتصدي للاعتداءات عليها من خلال الجرائم المعلوماتية

رشا جمال لطفي عبد المجيد

المعلومات غير المفصح عنها والتصدي للاعتداءات عليها من خلال الجرائم المعلوماتية

رشا جمال لطفي عبد المجيد

خطة البحث

1/1مقدمة

2 /1حقوق الملكية الفكرية كأصول غير ملموسة وصور التعدي عليها.

1/2/1المعلومات غير المفصح عنها كأحد حقوق الملكية الفكرية

1/2/2التعدي على حقوق الملكية الفكرية

1/3الجرائم المعلوماتية كأحد أوجه التعدي على حقوق الملكية الفكرية.

1/3/1العوامل التي أدت إلي ظهور الجرائم المعلوماتية.

1/3/2صناعة الأدوية كأحد القطاعات التي تستهدفها الجريمة الإلكترونية.

1/3/3أسباب الهجمات الإلكترونية على القطاع الصيدلي

1/4كيفية التعامل مع ظاهرة الجرائم المعلوماتية

1/4/1التدابير الواجب اتخاذها.

1/4/2التصدي للتعدي على المعلومات غير المفصح عنها.

1/5 خاتمة.

1/1مقدمة

لقد باتت الملكية الفكرية جزءًا مهماً من ثروة المؤسسات، حيث أنها تلعب دوراً مهماً في تحقيق مزايا تنافسية في مواجهة منافسيها. وأصبحت تلك الأصول غير الملموسة بمثابة الثروة الحقيقية للمؤسسات والتي يجب أن تبذل العناية الكاملة لوضع الاستراتيجيات اللازمة لإدارة تلك الأصول المتصلة بالملكية الفكرية .

في الآونة الأخيرة مع النمو في استخدام الانترنت، ازدادت الجرائم المستحدثة في المجالات المعلوماتية، وأصبحت تشكل خطراً حقيقياً في قطاعات الأعمال المختلفة ولاسيما في مجالات التعدي على حقوق الملكية الفكرية في المجال الصيدلي .

لذا أصبح من الضروري أن تتخذ المؤسسات التي تمتلك أصولًا للملكية الفكرية التدابير اللازمة للتأكد من حماية ثرواتها غير الملموسة من أعمال القرصنة والتعدي. وتعتمد حماية ما تمتلكه من أصول الملكية الفكرية وتأمين ملكيتها لها من جراء الجرائم المعلوماتية التي قد تتعرض لها خاصة إذا كانت تلك المؤسسات والشركات تمتلك معلومات سرية لها قيمة اقتصادية سواء تعلقت بمعلومات تقنية أو فنية أو إدارية.

ولذلك، يحق القول بأن الإدارة الفعالة لأصول الملكية الفكرية المملوكة للمؤسسات والشركات تستطيع أن تتصدى لمختلف أوجه التعدي عليها، ولاسيما التعدي الذي قد ينشأ نتيجة الجرائم المعلوماتية .

المبحث الأول
المعلومات غير المفصح عنها كأصول غير ملموسة وصور التعدي عليها

المطلب الأول
المعلومات غير المفصح عنها كأحد حقوق الملكية الفكرية

تمتد الملكية الفكرية لتشمل فروعاً عدة، حيث تنقسم إلى حقوق الملكية الأدبية والفنية وحقوق الملكية الصناعية، وتنقسم حقوق الملكية الصناعية وفقًا لما تنص عليه اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية **(Trade-Related Aspects of Intellectual Property Rights)** (TRIPS)

في الفقرة الثانية من المادة الأولى منها أن مصطلح الملكية الفكرية يشمل جميع فئات الملكية الفكرية المنصوص عليها في الأقسام من ١ إلى ٧ من الجزء الثاني وهي حقوق المؤلف والحقوق المتعلقة بها، العلامات التجارية، المؤشرات الجغرافية، التصميمات الصناعية، براءات الاختراع، التصميمات التخطيطية للدوائر المتكاملة وحماية المعلومات غير المفصح عنها.[١]

وبهذا تكون اعتبرت اتفاقية التربس المعلومات السرية شكلًا من أشكال الملكية الفكرية ووضعت نظامًا لحماية الأسرار التجارية أطلقت عليه المعلومات غير المفصح عنها.

الحاجة إلى حماية المعلومات السرية:

وقد ظهرت الحاجة إلى حماية المعلومات السرية حيث أن ليست كل الأفكار الإبداعية أو الابتكارية مما يمكن تسجيله أو إشهاره أو الحصول على براءة عنه، وذلك إما بسبب طبيعتها التي لا يمكن أن تتخذ شكلًا

[١] الصغير، حسام الدين عبد الغنى (٢٠٠٣)، حماية المعلومات غير المفصح عنها والتحديات التي تواجه الصناعات الدوائية في الدول النامية، دار الفكر الجامعي، الإسكندرية، ص: ١٠٦.

ماديًا، أو بسبب تقرير صاحبها إبقائها سراً لمشروعه للحفاظ على تميزه وتفرده وزيادة قدرته على المنافسة.[١]

تعريف المعلومات السرية:

ورغم أنه لا يوجد تعريف واضح للمعلومات السرية في اتفاقية التربس، إلا أنه يمكن تعريفها بأنها مجموع المعارف التكنولوجية النظرية والعلمية والإدارية الجديدة والقابلة للانتقال والتي تحتفظ بها المشروعات بشكل سرى وغير مشمولة ببراءة الاختراع.[٢]

كما أن المعلومات غير المفصح عنها تشمل كافة أنواع المعلومات السرية، بما قد تشمله من ابتكارات، تركيبات، نماذج، توليفات، برامج، آلات، أساليب وطرق ووسائل صناعية لها قيمة اقتصادية طالما لم تكن معروفة إلا للذين يحصلون على قيمتها الاقتصادية من خلال عملهم بها واستخدامهم لها.

ولقد أصبحت المعلومات غير المفصح عنها من أبرز العناصر المعنوية للشركات الصناعية والتجارية لما تمنحها من ميزة تنافسية تجاه الشركات الأخرى المنافسة. وتتعاظم أهميتها يوماً بعد يوم إلى أن أصبحت تندرج في ميزانيات تلك الشركات وتدخل في عناصر تقييمها، حيث أصبحت تعد من الأصول الغير ملموسة التي تمتلكها .

وهنا يجدر القول بضرورة توافر بعض الشروط في المعلومات المُراد حمايتها بواسطة الحماية القانونية للمعلومات غير المفصح عنها. حيث أنها يجب أن تكون سرية، بمعنى أنها غير معروفة أو متداولة ولم يتم الاطلاع عليها من قبل بواسطة طرف آخر أو الإعلان عنها، وأن تكون لها قيمة تجارية عالية بسبب كونها معلومات سرية، كما يجب أن يكون هناك سبب منطقي لجعلها سرية بواسطة الشخص أو الجهة التي تتقدم بطلب لحمايتها.

---

[١] .سلامة، أحمد عبد الكريم) ٢٠١٩(، القانون الدولي الخاص للملكية الفكرية- دراسة للاتفاقات الدولية ومناهج حماية حقوق الملكية الفكرية، القاهرة، ص: ٢٥٤.

[٢] .عيسى، حسام محمد(١٩٨٧)، نقل التكنولوجيا، دراسة في الآليات القانونية للتبعية الدولية، دار المستقبل العربي، القاهرة، ص: ١٣٠.

وبناءاً عليه، فإن الحماية المقررة للمعلومات غير المفصح عنها قد تمتد لتشمل ليس فقط المعرفة الفنية أو التقنية (know–how) بل تشمل أي معلومات لها قيمة اقتصادية مثل المعلومات المتعلقة بالجوانب التجارية والمالية والإدارية مثل الخطط التسويقية، وقوائم العملاء، والدراسات المالية والاقتصادية، وطرق الإدارة المبتكرة.[١]

وعليه، يمكن لأي شركة أن تحمى معلوماتها، التي ترى أنها معلومات سرية، بواسطة المعلومات غير المفصح عنها ضد التنافس غير المشروع أو الإفشاء، ويسرى ذلك أيضاً على موظفيها حيثُ أنهم بموجب اختصاصات وظائفهم داخل الشركة يتمكنون من الاطلاع على هذه المعلومات والبيانات. وتتميز المعلومات غير المفصح عنها بكونها تعطى لصاحبها ميزة احتكارية تضمن له المحافظة على السرية التامة، كما أنها حماية لا تنتهي بمرور فترة من الزمن مثل براءات الاختراع أو العلامات التجارية .

ولهذا، نجد أن أصول الملكية الفكرية للشركات قد تتنوع بين فروعها المختلفة، فلا مانع من أن تقتنى المؤسسات أصولًا خاصة بالاختراعات التي حصلت على براءات اختراع لها، والعلامات التجارية الخاصة بمنتجاتها أو أصولًا ترجع إلى تصميمات صناعية أو تصميمات تخطيطية لدوائر متكاملة. وقد تكون أصول الملكية الفكرية للشركات سواء كانت براءات اختراع أو أسرار تجارية أو مجرد معرفة تقنية أكثر قيمة من الأصول المادية التي تمتلكها.

المعلومات غير المفصح عنها في المجال الصيدلي:

بالإضافة إلى اتساع مجالات ونطاق المعلومات السرية التي تشملها الحماية القانونية، إذ قد تمثل معلومات غير جائز تقديم طلبات براءة عنها مثل طرق العلاج والتشخيص والجراحة اللازمة لمعالجة الانسان والحيوان والنبات. كما قد تشمل حماية المعلومات السرية المعارف والابتكارات التي

[١] . محمدين، جلال وفاء (٢٠٠٠)، الحماية القانونية للملكية الصناعية وفقًا لاتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (التربس)، دار الجامعة الجديدة، الإسكندرية، ص: ٨٩.

لا يجوز حمايتها عن طريق نظام براءات الاختراعات مثل الأفكار والمعلومات ذاتها.[١]

إن تمتع المعلومات غير المفصح عنها بحق ملكية عليها باعتبارها من المعارف الفنية حسمته المادة ٣٩ من اتفاقية التربس إذ نصت على المعلومات غير المفصح عنها لأول مرة كصورة من صور حقوق الملكية الفكرية.[٢]

وتضمنت اتفاقية التربس نصًا خاصًا لحماية بيانات الاختبار والمعلومات السرية الأخرى التي يلزم تقديمها إلى الجهات الحكومية المختصة للحصول على ترخيص بتسويق الأدوية أو المنتجات الكيميائية الزراعية. ويلزم في هذا النوع من المعلومات أن يتوافر فيها شروطًا خاصة للحماية بجانب الشروط المطلوبة لحماية المعلومات غير المفصح عنها والتي تخص الأشخاص الطبيعيين أو الاعتبارين وتقع تحت سيطرتهم بصورة قانونية .

وهذه الشروط هي أن يكون تقديم البيانات للجهة الحكومية لازماً للحصول على ترخيص بتسويق الأدوية، وأن يدخل في مكونات الأدوية كيانات كيميائية جديدة، وأن تكون هناك جهود كبيرة قد بذلت من أجل التوصل إلى هذه البيانات.[3]

المطلب الثاني
التعدي على المعلومات غير المفصح عنها

تتعد صور الاعتداء على حقوق الملكية الفكرية بتعدد فروعها وأشكالها. ويحرص حائزو المعلومات السرية على بقائها غير مفصح عنها لما قد يؤدى الوصول اليها بدون اذن من صاحبها إلى أضرار اقتصادية بالغة قد يصعب تداركها، فقد يقع الاعتداء على مثل تلك المعلومات ذات

---

[١] . الصغير، حسام عبد الغنى. ٢٠٠٣، ورقة العمل المقدمة إلى ندوة الوايبو الوطنية عن الملكية الفكرية، القاهرة، ص ٦.

[٢] . القليوبى، سميحة. ٢٠١٦. الملكية الصناعية، دار النهضة العربية، الطبعة العاشرة، القاهرة، ص ٤٤٧.

[3] . الصغير، حسام الدين عبد الغنى ، أنظر المرجع السابق (٢) ،ص:١٢١.

القيمة الاقتصادية الهامة للشركات والمؤسسات من قبل موظفو الشركة أنفسهم .

وتعد جرائم الإضرار بالبيانات من أشد الأنواع خطورة وتأثيراً وأكثرها حدوثاً وتحقيقاً للخسائر للأفراد والمؤسسات. غالبية الجرائم الالكترونية تشمل أنشطة محو أو سرقة أو إتلاف أو تعطيل أو المعلومات وقواعد البيانات الموجودة بصورة الكترونية على الحواسب الآلية المتصلة أو غير المتصلة بشبكات المعلومات أو مجرد محاولة الدخول بطريقة غير مشروعة عليها.[١]

وباعتبار أن المعلومات السرية أو غير المفصح عنها هي في واقع الأمر تعد أصول للملكية الفكرية التي يجب أن يتبع أصحابها سبل إدارة واعية لإدارة تلك الأصول والمحافظة عليها شأنها في ذلك شان باقي أصول الملكية الفكرية من براءات اختراع وعلامات تجارية وغيرها. إلا أن من سبل الإدارة الفعالة للمحافظة على المعلومات السرية هي تنوع الاجراءات والتدابير التي يجب على حائز المعلومات اتخاذها للمحافظة عليها، والتي قد تختلف بحسب طبيعة المعلومات وقيمتها ونوع النشاط الذي تستخدم فيه، ودرجة المخاطرة التي تنطوي على كشف تلك المعلومات.

ومن أمثلة تلك التدابير والاجراءات التي يمكن اتخاذها: حظر دخول أماكن معينة في المنشأة إلا لعدد محدود ممن يشتغلون مستويات الادارة العليا، استخدام رموز أو كلمات سرية لفتح الأبواب المغلقة الخاصة بأماكن تخزين المعلومات، تعيين حراسة دائمة على أماكن وجود المعلومات ومراقبتها بالكاميرات ووضع اخطارات في أماكن العمل تذكر العاملين بالالتزام بالمحافظة على سرية المعلومات.[2]

[١] . طه، وليد، التنظيم التشريعي للجرائم المعلوماتية في اتفاقية بودابست، القاهرة، ص: ١٩.
[2] . الصغير، حسام عبد الغنى. مرجع سابق (٢)، ص ٣٠.

المبحث الثاني
الجرائم المعلوماتية كأحد أوجه التعدي على حقوق الملكية الفكرية

المطلب الأول
العوامل التي أدت إلى ظهور الجرائم المعلوماتية

مع تطور عصر المعلومات الجديد ونموه في جميع مجالات تكنولوجيات الاتصالات، فإنه يفرض تحديات جديدة على النظام القانوني في حماية الأفراد والشركات. وهذه التحديات الجديدة هي نتيجة لزيادة نطاق الإنترنت وتعقيدها. والذي انعكس بشكل إيجابي على حقوق الملكية الفكرية في أكثر من اتجاه؛ حيث أنه زاد إمكانية الوصول إلى المعلومات غير المفصح عنها بأسعار معقولة، واختصار وقت الوصول إلى البيانات، وأتاحت الطريق أمام البلدان النامية للحاق بركب التقدم فيما يتعلق بالوصول إلى بيانات الملكية الفكرية وكيفية ادارتها.

وفي حين أن المجتمع يحصل على فوائد كبيرة من الإنترنت، فإنه يواجه أيضا نوعا جديدًا من الجريمة، هو الجريمة الإلكترونية.[1] وتشمل الجريمة الإلكترونية طائفة واسعة من الأفعال غير المشروعة المرتكبة باستخدام الحاسوب، وبسبب التطورات التكنولوجية المستمرة يستحيل وضع قائمة شاملة بجميع الإجراءات التي تعتبر جريمة إلكترونية. وقد ساعد على سهولة تلك الانتهاكات عبر الوسائط الرقمية عنها في الوسائط التقليدية هو السهولة واليسر التي يمكن لمرتكبيها الوصول إلى بيانات الملكة الفكرية، وكذلك السهولة التي يمكن بها تكرار الانتهاكات عبر الانترنت والتلاعب بحقوق الملكية الفكرية.

تتعرض حقوق الملكية الفكرية عبر الانترنت لانتهاكات أكثر خطورة من مثيلاتها في الوسائط التقليدية. وتتنوع تلك الانتهاكات بين ثلاثة أنواع رئيسية، أولها الانتهاكات الواقعة على الأصول الملموسة للملكية الفكرية مثل بيع السلع المقلدة عبر الانترنت، إنشاء منصات جديدة لتوزيعها سواء عن طريق الجملة أو التجزئة. وكذلك التعديات على الأصول غير الملموسة

[1] . سمارة، مصطفى ٢٠٠٨. "الجريمة الالكترونية "مجلة المعلوماتية ،العدد ٢٩ـشهر تموز.

للملكية الفكرية مثل القرصنة الرقمية، والتجسس الإلكتروني وانتحال مواقع الانترنت للشركات لإتمام المعاملات الرقمية من خلالها. وهناك نوع آخر جديد من انتهاكات حقوق الملكية الفكرية عبر الانترنت يشمل الانتهاك من خلال الوسطاء مثل موقعmegaupload ، وهو موقع يوفر خدمة التخزين السحابي والمشاركة للعملاء والتحميل متعدد الأغراض، ويعد من أضخم المواقع الشهيرة في تخزين وتبادل الملفات عبر العالم والذي تأسس عام ٢٠٠٥ وتم اغلاقه من قبل الحكومة الأمريكية عام ٢٠١٢ حيث اتهمت الحكومة مالكوه بانتهاك قوانين القرصنة والتسبب في خسارات مالية مهمة للعديد من الشركات العالمية.[١]

المطلب الثانى

صناعة الأدوية كأحد القطاعات التي تستهدفها الجريمة الإلكترونية

تعد صناعة الدواء من أهم الصناعات على مستوى العالم لما تمثله من أهمية في المحافظة على حياة الإنسان؛ وما تتطلبه من استثمارات ضخمة تنتج عن تكاليف البحث والتطوير وما يتم إنفاقه في الدراسات والبيانات الخاصة باختبارات الأمان (safety) والفاعلية(efficacy) ؛ فقد تتجاوز هذه التكاليف ٨٠٠ مليون دولار لإنتاج كيان كيميائي جديد New chemical Entity.[٢]

والسؤال الذي يطرح نفسه هو هل صناعة الأدوية هدفاً للهجمات الإلكترونية؟ أم أن إدارة أصول الملكية الفكرية في المجال الصيدلي بمنأى عن الجرائم المعلوماتية والقرصنة الإلكترونية؟

للإجابة عن هذا السؤال يكفي أن نستعرض أن عملية الاعداد لدواء جديد تستغرق سنوات عديدة قد تصل في بعض الأحيان إلى ١٣ سنة، وأنه من بين كل ٥٠٠٠ مركب جديد يتم اختبارهم، يدخل حوالي ٢٥٠ مركب فقط في الاختبارات قبل السريرية، و١٠ مركبات فقط منها هو ما يجرى عليه التجارب الاكلينيكية. في حين أن مركب واحد فقط هو ما يتم

[1].BBC NEWS, 8 March 2012. https://www.bbc.com/news/technology-16642369.

[2] . Inderjit Singh Bansal (and others) (2009) "Journal of Intellectual Property Rights", Vol 14 , July 2009 , Evergreening – A controversial issue in pharma Milieu, p: 3.

إنتاجه والموافقة على تسجيله من الجهات المختصة. ولذلك فإنه من بين كل ١٠ كيانات كيميائية جديدة؛ ثلاثة أدوية فقط هي التي قد تتجاوز أو بالكاد تنتج إيرادات مطابقة لنفقات البحث والتطوير (R&D) ما قبل انتهاء فترة حماية براءة الاختراع[1] .

وتلعب الملكية الفكرية دورًا هامًا في تعزيز حقوق الشركات الصيدلانية التي تسعى لإنتاج كيانات كيميائية جديدة؛ ومن ثم استرداد نفقات البحث والتطوير والتجارب الاكلينيكية. بالإضافة إلى طول فترة التجارب الإكلينيكية، وكذلك طول الفترة اللازمة لعملية التسجيل الدوائي، والدخول المتأخر للسوق والذي قد يكون من ٨ إلى ١٠ سنوات فقط (الحماية الفعلية).

وعلى الرغم من ذلك؛ فإن شركات الصناعات الدوائية قد تستطيع تجاوز نفقات البحث والتطوير من خلال الإدارة الفعالة لبراءات اختراعها والاستفادة من دورة حياة المنتج المحمي بالبراءة أقصى استفادة والذي قد ينتج من استراتيجيات التسويق الجيدة لمنتجاتها .

وفي أثناء رحلة شركات الادوية للبحث عن كيان جديد، تستخدم شركات الأدوية أيضاً حقوق أخرى للملكية الفكرية لحماية استثماراتها وتعزيز الصحة العامة تمثل أصول للملكية الفكرية بخلاف براءة الاختراع التي تخول لها الحماية الاستئثارية لمدة ٢٠ عامًا أو حماية فعالة لمدة ١٠–١٣ عامًا على النحو السابق ذكره بعد توافر شروط الحصول على البراءة ألا وهي الجدة والخطوة الإبداعية والقابلية للتطبيق الصناعي.

تتعدد صور تلك الأصول حيث تتمثل في العلامات التجارية لمنتجاتها، وحق المؤلف لحماية المصنفات الأصلية اللازمة في مجال البحث والتطوير ودفاتر التجارب المختبرية/المعملية(lab notebook) ، وضمان الموافقة التنظيمية، واليقظة الدوائية، ودعم المنتجات؛ و الأسرار التجارية لحماية المعلومات الحيوية ولكن غير القابلة للبراءة مثل بيانات التجارب السريرية وتركيبات المنتجات وعملية التصنيع و المعلومات

[1] .Nicoleta Tuominen, (2011), "Patenting Strategies of the EU Pharmaceutical Industry Crossroad between Patent Law and Competition Policy" , January 2011, page 5.

الخاصة بالأدوية في طور التطوير للحصول على براءة، بيانات الاختبار السرية والمعلومات الأخرى التي يلزم تقديمها إلي الجهات الحكومية المختصة للحصول على الترخيص بالتسويق، استراتيجيات المنتج وخطط التسويق، بيانات العملاء، معلومات عن التكلفة الداخلية للشركة لإنتاج المنتج، بيانات التسعير وهوامش الربح[1] .

ومع تطور عصر المعلومات وتطوره في كافة المجالات؛ فأصبح تخزين والاحتفاظ بتلك البيانات الهامة والمعلومات السرية والحيوية الخاصة بالشركات تتم عن طريق أجهزة الحاسب الآلي وشبكة الانترنت. مما فرض على شركات الأدوية تحديات كبيرة في الحفاظ على أصولها الرقمية (digital assets)من الانتهاك والتداول الغير مشروع مما قد يعرضها لخسائر كارثية قد يصعب تداركها.

ولذلك؛ فإن أصول الملكية الفكرية في المجال الصيدلي ليست بمنأى عن الجرائم المعلوماتية؛ بل أن شركات الأدوية هي واحدة من أكبر القطاعات التي تعد هدفًا للقرصنة الإلكترونية لما تمتلكه من أصول وبيانات حساسة وقيمة تزامنًا مع تحرك هذه الشركات نحو زيادة الرقمنة (digitalization)وتخزين بيانات قيمة عبر الانترنت[2] .(online)

ومن أمثلة الشركات التي تم الاعتداء على أصولها الرقمية من جراء القرصنة الالكترونية هي شركة ميرك أند شارب (Merck co.)

تعرضت شركة ميرك وهى واحدة من أبرز الشركات الضخمة في مجال الأدوية إلي هجوم برمجي واسع النطاق لطلب فدية من NotPetya Ransomware وذلك فى يوم ٢٧ يونيو من عام ٢٠١٧، والذى أدى إلي إغلاق الشركة لمدة أسبوعين وخسارتها خسائر فادحة وصلت إلي مليار دولار، حيث أدى هذا الهجوم الإلكتروني عليها إلي خلل خطير وتعطيل أنظمة البحث والتطوير وكذلك أنظمة إنتاج المكونات الصيدلانية النشطة

[1] .Andrew Douthwaite, (2019), "How can pharma protect itself from cyberattack.", European Pharmaceutical Manufacturing,30 September 2019.

[2] .Matt Mories, (2017), " Indestrial Cybersecurity Defenses Essential for Pharma Companies", Pharma Manufacturing.

(API)للشركة مما أدى إلي فشل الشركة في سد احتياجات الانتاج من واحد من أهم العقارات التي كانت تنتجها في تلك الآونة وهو مصل GardasilK.[١]

وتتلخص وقائع ذلك الهجوم البرمجي في أن جميع أجهزة الكمبيوتر الخاصة بموظفي شركة ميرك- والذي كان يبلغ عددهم قرابة ٧٠٠٠٠ موظف- أصبحت محجوبة تماماً عن أنظمة الشركة، حيث عرضت رسالة واحدة مضمونها أنه تم تشفير أجهزة الشركة بالكامل وأنه لا وسيلة لاسترداد الملفات إلا في حالة دفع الفدية المطلوبة حتى يتم ارسال مفتاح فك التشفير.[٢]

ولذلك نجد أنه بعد تلك الهجمات الإلكترونية التي تعرضت لها شركة ميرك والتي أدت إلى خسارتها المالية، عملت شركة فايزر وهي من كبرى الشركات أيضًا في الصناعات الدوائية على إطلاق برنامج شامل للأمن المعلوماتي، وكانت من الأهداف الرئيسية لهذا البرنامج الكشف السريع عن التهديدات التي قد تصيب أنظمة التحكم في الإنتاج والتصنيع بشكل دوري، وتحديث القدرة على اكتشاف البرامج الضارة بتكنولوجيا المعلومات الخاصة بالشركة.

[1].Austen Hufford and Peter Loftus, (2017) "Merch Swings to Lose as Cyberattack Harts Sale.", The Wall Street Journal,2017.

[2] .Derek Lowe, 13 December, 2019, " Merck and Its Ransomware Problems in Court, Journal of Science Translational Medicine.

المطلب الثالث

أسباب الهجمات الإلكترونية على المعلومات غير المفصح عنها في القطاع الصيدلي

والسؤال الذي يطرح نفسه الآن هو ما هي استفادة معتدى الجرائم الالكترونية من الهجوم الإلكتروني على أنظمة شركات الأدوية؟

نظرًا لأن البيانات داخل أنظمة تكنولوجيا المعلومات لشركات الأدوية لها قيمة عالية، فإن هذه الصناعة هي محور تركيز مجموعة واسعة من مجرمي الإنترنت. وفي واقع الأمر، هناك أسباب عديدة للقرصنة الإلكترونية على أصول الملكية الفكرية في القطاع الصيدلي[1] .

أحدها هي طلب الفدية مقابل التنازل عن سيطرة المهاجم على أجهزة الشركة كما تم الاستعراض سابقًا في حالة هجوم NotPetya ransomwareعلى شركة ميرك.

كما أن لشركات الأدوية بيانات ومعلومات ذات قيمة اقتصادية عالية كما تم الاشارة سابقاً فيما يتعلق بالتجارب السريرية والمعلومات الخاصة بالأدوية في طور التطوير للحصول على براءة؛ والتي قد تجنى لمرتكبي تلك الجرائم الإلكترونية مكاسب مادية عالية في حالة تسريبها إلى منافسي تلك الشركات. فتباع الأسرار التجارية المقرصنة لشركات أخرى أو جماعات غير قانونية، ويتم تنزيل خطط الشركات والأسرار من قبل القراصنة على قرص كمبيوتر. يمكن نقل المعلومات المسروقة في جميع أنحاء العالم في غضون دقائق. القراصنة السرية التجارية العثور على مسارات في أنظمة الكمبيوتر للشركة وتحميل العناصر التي سيتم نسخها. تحتفظ الشركات بكل شيء تقريبًا في ملفات الكمبيوتر الخاصة بها. تباع النسخ المقرصنة عبر الإنترنت للعملاء الذين يقدمون أرقام بطاقات الائتمان الخاصة بهم ثم يقومون بتنزيل النسخة[2] .

---

[1]. Holger Mettler,(2019), " cybersecurity is an important issue for the pharmaceutical industry.", Healthcare Industry, BW

[2] . Clifford, Ralph D., ed. Cybercrime"The Investigation, Prosecution, and Defense of a Computer-Related Crime ". Durham, NC, Carolina Academic Press, 2001.

بناءاً على ما تقدم؛ فإنه نظرًا للطبيعة القيمة لمعلومات البراءات وبيانات الاختبار الخاصة بالقطاع الصيدلي، وكذلك بسبب الاستثمار الهائل من قبل الشركات في البحث والتطوير لإنتاج كيان كيميائي جديد؛ فقد ظهرت حاجة شركات الأدوية لتحصين أنظمتها الأمنية للمحافظة على ملكيتها لهذه الأصول غير الملموسة من جراء الاعتداء عليها عبر الجرائم المعلوماتية، وأفضل طريقة للحماية هي منع الهجمات الإلكترونية من الحدوث أو على الأقل تقليل خطر الاختراق.

المبحث الثالث

كيفية التعامل مع ظاهرة الجرائم المعلوماتية

المطلب الأول

التدابير الواجب اتخاذها

في جرائم الاعتداء على المعلومات غير مفصح عنها والاستيلاء على معلومات تقنية أو سرية، قد يقع الاعتداء من خلال أحد العاملين بالشركة، أو من قبل شخص من خارج الشركة سواء كان هو المنافس في مجال العمل أو من خلال طرف ثالث لصالح المنافسين.

ويتحتم في مثل هذه الحالات التي تمتلك فيها الشركات أصول للملكية الفكرية تتعلق بمعلومات مهمة وحساسة ذات قيمة اقتصادية أن تتبع الشركات استراتيجيات فعالة لضمان عدم حدوث انتهاكات أو اختلاسات لمثل هذه المعلومات غير المفصح عنها، والتي قد تتسبب في خسائر تفوق الخسائر في الأصول المالية نفسها التي تمتلكها تلك الشركات والتي قد يصعب تدارك آثارها، حيث أنه في حالة عدم اتخاذ حائز هذه المعلومات التدابير والإجراءات اللازمة للمحافظة علي سرية تلك المعلومات، يسقط حقه في التمتع بالحماية المقررة للأسرار التجارية[١] .

[١] . حسن، نصر أبو الفتوح فريد،(٢٠٠٦)، حماية حقوق الملكية الفكرية في مجال صناعة الدواء في ظل اتفاقية التربس والقانون المصري، دار الجامعة الجديدة.

قضية Galaxo Inc. vs. Novopharm Ltd.

تتلخص وقائع تلك القضية التي رفعتها شركة Galaxo ضد Novopharmفي أن الأولى ادعت قيام الثانية بتقليد أحد اختراعاتها الدوائية المحمية ببراءة اختراع فضلًا عن قيامها بسرقة أسرارها التجارية المتعلقة بخطوات وطريقة تحضير الدواء .Zantac

وقضت المحكمة في تلك القضية أن شركة Galaxo لم تقم باتخاذ التدابير اللازمة للمحافظة على سرية المعلومات المتعلقة بالعناصر الداخلة في تركيب الدواء وطريقة تحضيره؛ حيث أنها قد قامت بتقديم الوثائق والمستندات التي تتضمن تلك المعلومات في قضية سابقة دون أن تكفل سريتها، فأتاحت لشركات انتاج الأدوية الأخرى فرصة الاطلاع عليها والحصول على صور منها، وبالتالي فقدت المعلومات سريتها، في حين أنه كان يمكن للشركة أن تقدم الوثائق التي تحتوى على معلومات سرية في مظاريف مغلقة ومختومة وتطلب من المحكمة اتخاذ الاجراءات الكفيلة بالمحافظة عليها[1] .

إن الطريقة الأمثل لحماية السر التجاري من إساءة استعماله هي الاتفاقات أو العقود الكتابية المتعلقة بعدم كشف السر التجاري. حيث تعد الشروط التعاقدية من أهم وسائل تأمين المعلومات. فعادة ما تضع المشروعات والمؤسسات ومراكز الأبحاث شروطًا في العقود التي تبرمها مع الموظفين والباحثين أو غيرهم من الأشخاص الذين تتيح لهم ظروف العمل معرفة الأسرار التجارية تتضمن إلزامهم بكتمان المعلومات وعدم الافصاح عنها للغير أو استعمالها خارج نطاق العمل. كما تتضمن عقود نقل المعرفة الفنية والتقنية شروطًا تلزم المرخص له بعدم افشاء المعلومات السرية التي زوده بها المرخص[2] .

---

[1] .Galaxo Inc. V, Novopharm Ltd., 931 F . Supp. 1280 – Dist. Court, North Carolina 1996.

[2] . ممدوح الشيخ، ٢٠٠٧ , التجسس الإلكتروني– سرقة الاسرار التقنية الاقتصادية, مكتبة بيروت, القاهرة ص ٢٠.

يجب على كل صاحب حق في أي معلومة تجارية ما أن يتصرف بطريقة تثبت رغبته في المحافظة على سريتها. ولابد من اتخاذ تدابير معقولة للحفاظ على سرية المعلومات ومن تلك التدابير المعقولة التي يجب أن تؤخذ في الاعتبار في مثل تلك الانتهاكات التقليدية للحفاظ على سرية المعلومات:

حفظ الوثائق والمستندات في أماكن آمنة يصعب على الغير الحصول عليها مثل الخزائن الحديدية. وتحديد الأشخاص المسموح لهم بالحصول على الوثائق والمعلومات وذلك وفقًا للحاجة الضرورية للاطلاع على هذه المعلومات وفقًا لحاجة العمل. والإشارة على الوثائق والمعلومات أنها ذات طابع سرى وغير مسموح بالاطلاع عليها أو معرفتها. ومنع الغير من تصوير هذه المعلومات للحفاظ على سريها. مع قيام صاحب الحق في المعلومات السرية بالاشتراط كتابة على موظفيه بعدم افشاء تلك المعلومات نظرًا لكونها سرية وذات قيمة تجارية. والاشتراط كتابة على موظفيه بعدم العمل مع منافسيه لمدة محددة بعد انتهاء عقد عملهم لديه. [1] وكذلك استخدام رموز أو كلمات سرية لفتح الأبواب المغلقة مع مراقبة مكان المعلومات عن طريق الكاميرات أو أجهزة الإنذار.

المطلب الثانى

التصدي للتعدي على المعلومات غير المفصح عنها

والسؤال الذي يتبادر إلى الذهن هو هل تكفي مثل هذه التدابير في العصر الحديث للإدارة الفعالة للمعلومات الفنية والتقنية والتنظيمية الادارية التي تشكل قيمة اقتصادية كبيرة للمؤسسات؟

مع تطور عصر المعلومات وتطوره في كافة المجالات؛ فأصبح تخزين والاحتفاظ بالبيانات الهامة والمعلومات السرية والحيوية الخاصة بالشركات لا تتم فقط عبر الطرق التقليدية بالاحتفاظ بها في خزائن حديدية وغرف مغلقة يتم تعيين حراسة عليها، بل أصبح الاحتفاظ بمثل تلك المعلومات الحيوية تتم عن طريق أجهزة الحاسب الآلي وشبكة الانترنت،

[1] . قيس محافظة، (٢٠٠٤)، " الأسرار التجارية في مجال الملكية الفكرية " ، ندوة الوايبو الوطنية عن الملكية الفكرية لأعضاء هيئة التدريس وطلاب الحقوق في الجامعة الأردنية، الفترة من ٦ إلى ٨ أبريل ٢٠٠٤، عمان، ص: ٣.

مما فرض على الشركات تحديات كبيرة في الحفاظ على أصولها الرقمية من الانتهاك والاختراق والتداول غير المشروع مما قد يعرضها لخسائر كارثية قد يصعب تداركها.

لقد كان لظهور الحاسب الآلي والإنترنت أثرا بالغاً على رقي وتقدم البشرية في أغلب مناحي الحياة الاقتصادية والتعليمية والطبية والعديد من المجالات الأخرى. كما صاحبها ظهور خبراء في تطويع هذه التكنولوجيا للقيام بأعمال إجرامية معاصرة تعتمد على التقنية في تنفيذ أفعالهم الإجرامية وبأساليب وطرق جديدة لم تكن معروفة من قبل. وساعد هؤلاء المجرمين ما يشهده العصر من تطور الوسائل المعلوماتية الحديثة، في زيادة سرعة نشر جرائمهم حتى أصبحت تهدد النظام المعلوماتي، بل أصبح في إمكانهم التسبُّب في خلق شلل كامل للأنظمة المدنيّة والعسكريّة، الأرضيّة والفضائيّة، وغيرها بواسطة قنابل معلوماتية ترسلها لوحة مفاتيح الحاسوب من على مسافات تتعدّى عشرات الآلاف من الأميال، وذلك دون أن يترك المجرم المعلوماتي أو الإلكتروني أثرًا ملموسًا لملاحقته ومعرفة مَصدرها[1] .

ووفقاً لـ تقرير مايكروسوفت، تتسبب الجرائم الإلكترونية بخسارة ما يقارب ٥٠٠ بليون دولار على مستوى العالم سنوياً.

في جميع الشركات، بغض النظر عن نوعها يعتبر أمن المعلومات أمراً مهماً لاستمرار عملهم وتطوره. أمن المعلومات هو أحد العوامل الحساسة والمهمة جداً التي قد تؤثر على مصير شركتك. خلال السنوات الماضية، زادت أهمية امن المعلومات وأصبحت جزء لا يتجزأ من إدارة أي عمل. ومكلفة أيضاً الشركات الصغيرة والمتوسطة قد تضطر إلي دفع الكثير في حالة تعرضها إلى اختراق في خصوصية البيانات، عدم وجود سياسة أمان البيانات هي أحد الأسباب الرئيسية أيضاً. قد تكون شركتك معرضك لـ الاختراق في أي وقت، فمن الجيد أن يكون لديك سياسة لـ حماية وأمان البيانات أو بعض الشروط التي يجب على الموظفين اتباعها. فلم تعد تفلح التدابير الخاصة بالحماية التقليدية للمعلومات والبيانات السرية في العصر

[1] . رحاب فايز أحمد سيد،(٢٠١٥)،جرائم الكتب الإلكترونية– دراسة تحليلية لوضع استراتيجية حماية لها، مجلة مكتبة الملك فهد الوطنية، مجلد ٢١.

الحديث، وأصبح لزامًا على أصحاب حقوق الاسرار التجارية حمايتها ضد الاختراقات التي تحث على أنظمة التخزين والتداول الخاصة بها.

وتعد الخطوة الأولى لحماية أصول الملكية الفكرية الرقمية هي إجراء التقييم الكامل لها ولمواقع تخزينها لبيان الطريقة المثلى لحمايتها. فهناك عدد لا نهائي من الآليات والخطط والحيل التي يمكن أن تستخدمها الشركات في حماية نظم الملكية الفكرية والنظم الإلكترونية. وينبغي للشركات أن تنفذ برنامجا كاملا لأمن الفضاء الإلكتروني يشمل الحوكمة والرقابة ووضع بروتوكولات لحماية النظم الحساسة لديها.[١]

من الأهمية بمكان أن ندرك أن موظفي الشركة يشكلون حلقة وصل بالغة الأهمية في هذه العملية. فقد يكون موظفي الشركة هم السبب الأول لضعف أمن المعلومات وفقدان البيانات إن لم يكونوا ذو خلفية جيدة بأمن المعلومات وحماية البيانات. قد يقوم أحدهم بالضغط على أحد الروابط المرفقة بالبريد الإلكتروني العشوائي الظاهر كبريد إلكتروني عادي. وقد يقوم أيضاً هذا الرابط بتوجيهك إلى أحد مواقع الخداع، مما سيجعل الخطر أكبر. تدريب الموظفين وتعليمهم كيفية التعامل مع البريد الوارد والتعرف على الرسائل المزيفة التي قد تحتوي على روابط ومرفقات مضرة أمر في غاية الأهمية.

فالبريد الإلكتروني هو المدخل إلى نظام كمبيوتر الشركة، لا يزال يتعين على الشركات أن تشارك في عملية حاسمة لحماية نفسها من سرقات الملكية الفكرية ومن الانتهاكات الإلكترونية. وينبغي للشركات تثقيف موظفيها بشأن العقوبات المدنية والجنائية الشديدة التي ستوقع في حال الاطلاع على معلومات الشركة السرية دون إذن على الحاسوب. وقد تشكل هذه التهديدات رادعاً كبيراً للموظفين غير المخلصين المحتملين.[٢]

---

[1]. Burke, Francis J., "Cyber Security and Cyber Risk Issues for Boards of Directors", Audit Committee Hot Topics Panel, Foley National Directors Institute, November 6, 2014.

[2]. Ernest E. Badway, 2012, "Protecting Companies' Intellectual Property From Cyber Crime", New York Law Journal, November 5, 2012.

ولكن تثقيف وتدريب الموظفين وحدة لا يكفي. ويجب على الشركات أيضاً أن ترصد رسائل البريد الإلكتروني الخاصة بالموظفين لضمان الامتثال لبروتوكول عدم نشر المعلومات السرية. ويجب على الشركات أن تستعرض وتستكمل، إذا لزم الأمر، سياسات ودليل للموظفين بحيث تشمل اتفاقات استخدام الحاسوب التي يجب على الموظفين أن يوقعوا عليها اعترافاً بأنهم يستخدمون معلومات الشركات المسجلة الملكية. ويجب على هؤلاء الموظفين أن يتفقوا على أن هذه المعلومات لا يجوز استخدامها إلا للأعمال المشروعة للشركة، داخل الشركة، وألا ترسل إلى طرف ثالث دون إذن صريح من الشركة، ولا يجوز نقلها أو حفظها إلى أي حاسوب شخصي أو ناقل أي جهاز تخزين آخر. ويتعين على الشركات، مع إداراتها المعنية بتكنولوجيا المعلومات، تقييد الوصول إلى قاعدة البيانات بالنسبة للموظفين الذين يحتاجون إليها فقط، وإنشاء قواعد بيانات محمية بكلمة سر.

وعلاوة على ذلك، ينبغي مطالبة الموظفين بإعادة جميع المعدات الحاسوبية للشركة وإجراء تقييم للأجهزة لضمان بقاء جميع الملفات والمعلومات سليمة عند مغادرة الموظف. نتيجة لذلك، تتطلب حماية شركتك من اختلاس الموظفين الحد من إمكانية الاطلاع على بيانات الموظفين، وصياغة اتفاقات محددة لحماية المعلومات السرية والنظر في اتخاذ إجراءات قانونية ضد الموظفين الحاليين والسابقين بسبب هذه المخالفات أو السرقات. فإن العديد من السياسات إذا نُفِّذت ستحمي أيضاً الملكية الفكرية للشركة من مصادر خارجية. كما يجب أن تتمتع الشركات بحماية خاصة للاتصالات في مجالس الإدارة وغرف الاجتماعات لأن هذه المناقشات قد تتضمن معلومات سرية[1] .

استخدام رموز أو كلمات سرية لفتح الحواسب الإلكترونية الخاصة بتخزين المعلومات ومراقبة وصول الموظفين للمعلومات، إذ يجب توزيع بيان سياسة يوضح أن الشركة ستقوم بعمليات تفتيش على نظم الكمبيوتر للتأكد من أن المعلومات السرية تستخدم لأغراض العمل فقط.

[1] . مصري، عبد الصبور عبد القوى على. ٢٠١٠ ، التجارة الالكترونية والقانون، دار العلوم– ط.١، القاهرة.

حماية البيانات المتنقلة باستخدام تقنيات تشفير قوية، بروتوكولات واستخدام كلمات سر قوية ومعقدة يصعب كشفها مع تغيير كلمات السر بشكل دوري أيضاً. فكلمات السر الضعيفة قد تكون أيضاً أحد الأسباب للاختراقات المعلوماتية، وكذلك تثبيت أحد البرامج من مصادر غير موثوقة والذي سيعرضك إلي خطر الاختراق أو البرمجيات الخبيثة. فتثبيت البرامج التي ستحميك من خطر الاختراق والابتزاز. حيث يجب حماية البيانات من الابتزاز Ransomware ، وهي الهجمات التي تقوم بتشفير بياناتك ومنع الوصل إليها قبل أن تدفع مبلغ من المال كفدية. مع إجراء نسخ احتياطي لبياناتك بشكل دوري، حيث أنه إذا حدث وأن فقدت جزء من بياناتك، فستفقدها للأبد إن لم تكن قد أخذت نسخة احتياطية منها بالفعل. النسخ الاحتياطي يضمن لك خطة استرجاع ويجعلك جاهز في حال حدوث أمر ما، كل هذا بأقل الأضرار وأقصر وقت. تثبيت برنامج مكافحة الفيروسات والبرمجيات الخبيثة هو أحد الحلول التي يجب تطبيقها على الأجهزة النهائية. حتى وإن تعرضت لهجوم فإن موقعك جاهز للكشف عن الفيروسات والبرمجيات الخبيثة ومسحها واستعادة الوضع الطبيعي من موقعك Malware Removal[1]

1/5 خاتمة

إن الجرائم المعلوماتية أصبحت تحتل مؤشرًا مرتفعا في انتهاكات الملكية الفكرية ربما يتجاوز جرائم الانتهاكات التقليدية في بعض الصناعات. وأن أصول الملكية الفكرية للأفراد والمؤسسات باتت من عناصر التقييم الأساسية لأي مشروع والذي قد تفوق في بعض الأحيان الأصول الملموسة للشركات والمؤسسات وتمثل ثروة حقيقية تعتمد عليها مثل تلك الشركات في الحصول على ميزات تنافسية بين منافسيها. والتي قد تتعدد ما بين براءات اختراع أو علامات تجارية أو خدمية أو تصميمات ونماذج صناعية أو معلومات سرية تتعلق بالخطط التسويقية والمعلومات التقنية والتنظيمات الإدارية وغيرها.

[1] . 19 Essential Cybersecurity Best Practices",published by Virtual Armour, 2018, December 7, 2018.

لذا أصبح لزامًا على أصحاب حقوق الملكية الفكرية المحافظة على تلك الأصول من الاعتداءات التي تنتهكها من خلال الجرائم المعلوماتية. وأن تنتهج الشركات والمؤسسات وتضع الاستراتيجيات لتحقق الأمان المعلوماتي للشركة من خلال المراقبة الدورية لشبكات المعلومات واستخدام أحدث التقنيات لتشفير البيانات والمعلومات الهامة التي قد تتعرض للانتهاكات.

وضع خطط وبرامج لمكافحة التعديات الواقعة على أصول الملكية الفكرية هي من أهم الاستراتيجيات لإدارة تلك الأصول عن طريق رؤية واضحة ومدروسة لكيفية التعامل في حالة حدوث اختراقات معلوماتية وكيفية الاسترداد السريع للبيانات بدون التأثير على وضع الشركات بين نافسيها.

قائمة المراجع

أولا المراجع العربية:

❖ مؤلفات وكتب قانونية:

- أحمد عبد الكريم سلامة (٢٠١٩) ، القانون الدولي الخاص للملكية الفكرية– دراسة للاتفاقات الدولية ومناهج حماية حقوق الملكية الفكرية، القاهرة.
- جلال وفاء محمدين (٢٠٠٠) ، الحماية القانونية للملكية الصناعية وفقًا لاتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (التربس)، دار الجامعة الجديدة، الإسكندرية.
- حسام الدين عبد الغنى الصغير(٢٠٠٣)، حماية المعلومات غير المفصح عنها والتحديات التي تواجه الصناعات الدوائية في الدول النامية، دار الفكر الجامعي، الإسكندرية.
- حسام محمد عيسى (١٩٨٧)، نقل التكنولوجيا، دراسة في الآليات القانونية للتبعية الدولية، دار المستقبل العربي، القاهرة
- سميحة القليوبى(٢٠١٦) ، الملكية الصناعية، دار النهضة العربية، الطبعة العاشرة، القاهرة.
- ممدوح الشيخ (٢٠٠٧) التجسس الإلكتروني– سرقة الاسرار التقنية والاقتصادية، مكتبة بيروت، القاهرة .
- عبد الصبور عبد القوى على مصري (٢٠١٠) التجارة الالكترونية والقانون، دار العلوم– الطبعة الأولى، القاهرة.

- نصر أبو الفتوح فريد حسن (٢٠٠٦)، حماية حقوق الملكية الفكرية في مجال صناعة الدواء في ظل اتفاقية التربس والقانون المصري، دار الجامعة الجديدة.

❖ **أوراق عمل وأوراق بحثية:**

- حسام عبد الغنى الصغير(٢٠٠٣) ، ورقة العمل المقدمة إلى ندوة الوايبو الوطنية عن الملكية الفكرية، القاهرة.
- قيس محافظة(٢٠٠٤)، ندوة الوايبو الوطنية عن الملكية الفكرية لأعضاء هيئة التدريس وطلاب الحقوق في الجامعة الأردنية، الأسرار التجارية في مجال الملكية الفكرية، الفترة من ٦ إلى ٨ أبريل ٢٠٠٤، عمان.
- رحاب فايز أحمد سيد،(٢٠١٥)،جرائم الكتب الإلكترونية- دراسة تحليلية لوضع استراتيجية حماية لها، مجلة مكتبة الملك فهد الوطنية، مجلد ٢١.

ثانيا: المراجع الأجنبية:

❖ **مؤلفات:**

- Journal of Intellectual Property Rights, Vol 14, July 2009, Evergreening – A controversial issue in pharma Milieu,p
- Nicoleta Tuominen, Patenting Strategies of the EU Pharmaceutical Industry Crossroad between Patent Law and Competition Policy,January 2011,

- Austen Hufford and Peter Loftus, October 2017," Merch Swings to Lose as Cyberattack Harts Sale.", The Wall Street Journal,2017
- Derek Lowe, 13 December, 2019, "Merck and Its Ransomware Problems in Court, Journal of Science Translational Medicine.
- Andrew Douthwaite, (2019), "How can pharma protect itself from cyberattack.", European Pharmaceutical Manufacturing,30 September 2019.
- Clifford, Ralph D., ed. Cybercrime"The Investigation, Prosecution, and Defense of a Computer-Related Crime" . Durham, NC, Carolina Academic Press, 2001
- Holger Mettler,(2019), " cybersecurity is an important issue for the pharmaceutical industry.", Healthcare Industry, BW.
- Matt Mories, (2017), " Indestrial Cybersecurity Defenses Essential for Pharma Companies", Pharma Manufacturing.

❖ **تقارير وقضايا:**

- Galaxo Inc. V, Novopharm Ltd., 931 F. Supp. 1280 – Dist. Court, North Carolina 199