مجلة الحقوق

فصلية علمية محكمة - تصدر عن مجلس النشر العلمي - جامعة الكويت

الحماية الجزائية للأجهزة الطبية الحيوية المحوسبة على ضوء قانون مكافحة جرائم تقنية المعلومات الكويتي .

الدكتور/ عمر عبدالمجيد مصبح

جامعة الكويت
KUWAIT UNIVERSITY

ISSN: 1029 - 6069

العدد ٤ - السنة ٤٧

جمادى الآخرة ١٤٤٥ هـ - ديسمبر ٢٠٢٣م

الحماية الجزائية للأجهزة الطبية الحيوية المحوسبة على ضوء قانون مكافحة جرائم تقنية المعلومات الكويتي

الدكتور/ عمر عبدالمجيد مصبح*

ملخص:

الأهداف: تهدف هذه الدراسة لتناول الحماية الجزائية للأجهزة الطبية الحيوية على ضوء قانون مكافحة جرائم تقنية المعلومات الكويتي، من خلال البحث في موضوع قرصنة الأجهزة الطبية المحوسبة، في محاولة لبيان بعض صور الجرائم المتعلقة بالأجهزة الطبية المزروعة بالمرضى "تقنيات المكروبيولوجية". **المنهج:** اعتمد على المنهج التحليلي النقدي المقارن. **النتائج:** يمكن إيجاز أهم نتائج الدراسة، بما يأتي: ١- تزايد قيمة المعلومات الطبية للمريض المنقولة عبر الأجهزة الطبية المحوسبة، وتشمل نقاط الضعف لهذه الأجهزة من خلال إمكانية الوصول للمعلومات الطبية الخاصة للمريض، وإمكانية التلاعب بها. ٢- بسبب الطبيعة المتطورة للتهديدات السيبرانية، سيتعين على هذه النظم أن يكون لديها إجراءات تعالج التهديدات الإجرامية. ٣- تبين من خلال الدراسة أن قانون مكافحة جرائم تقنية المعلومات الكويتي لم ينص على (التداخل)، وهو فعل يختلف عن الدخول غير المشروع، ويختلف أيضاً عن الالتقاط. وقد خلصت الدراسة لعدة توصيات، منها: ضرورة إفراد نصوص جنائية خاصة بالمسؤولية الجزائية للتقنيات الطبية الحيوية المحوسبة في قانون مكافحة جرائم تقنية المعلومات الكويتي، بالنظر إلى تطور وتنامي هذه المسؤولية، بموازاة مع تصاعد وتيرة قرصنة هذه الأخيرة، فلم تعدو الحالة هذه -القواعد والنصوص الجزائية العامة- بقوالبها الجامدة منسجمة مع واقع هذه المسؤولية ومواكبة لمستجداتها.

مقدمة:

تشكل الأجهزة الطبية الحيوية المحوسبة جزءاً لا يتجزأ من نظام الرعاية الصحية الذي يوفر الخدمات الأساسية للمجتمع، وتعتبر التقنيات الطبية ضرورة لا بد منها في القطاع الطبي، بحيث تساهم في تشخيص الأمراض والوقاية منها وعلاج وتأهيل المصابين، وهي تتنوع من أبسط أدوات مقاييس درجات الحرارة إلى معدات التصوير التشخيصي.

* كلية الحقوق، جامعة السلطان قابوس - سلطنة عُمان، الإيميل: Musbih2003@yahoo.com

- تُسلّم البحث في: ٢٠١٨/١٢/٢٩، أُجيز للنشر في: ٢٠١٩/١٠/٢٧.

للاستشهاد بهذا البحث انظر ص ٣٤٩

بيد أن معظم الأفراد لا تتاح لهم فرصة الاستفادة بالقدر الكافي من فوائد الأجهزة الطبية الحيوية الآمنة والملائمة ضمن النظم القانونية والصحية؛ فتفتقر بعض التشريعات الوطنية في مجال التكنولوجية الحيوية الصحية إلى وجود نصوص قانونية تمكنها من استعمال هذه الأجهزة التكنولوجية بفاعلية، كذلك لا تستخدم غالبية الدول المبادئ التوجيهية أو السياسات أو التوصيات الخاصة لاقتناء الأجهزة الطبية الحيوية، إما لعدم توافرها أو عدم وجود جهة معترف بها لتنفيذها.

وعوداً على بدء، فقد أسفرت التطورات التقنية الأخيرة عن تحولات في تقديم الرعاية والخدمات الصحية لتحسين رعاية المرضى، ومن الأمثلة على ذلك زيادة الترابط بين الأجهزة الطبية وأنظمة الاتصال والمعلومات، هذا الترابط ترك الأجهزة الطبية الحيوية عرضة للانتهاكات المجرمة، وهناك احتمال من أن الربط بين الأجهزة الطبية وشبكة الاتصالات والإنترنت سيؤثر مباشرة على سلامة المرضى، فالعديد من الأجهزة الطبية تحتوي على أنظمة الحاسب الآلي[1]، وهي جزءاً لا يتجزأ منها والتي يمكن أن تكون عرضة للانتهاكات الإلكترونية.

وفي هذا الإطار، تنصب هذه الدراسة على: الحماية الجزائية للأجهزة الطبية المحوسبة في ضوء قانون مكافحة جرائم تقنية المعلومات الكويتي رقم (٦٣) لعام ٢٠١٥؛ فشبكات الرعاية الصحية فريدة من نوعها من جانبين هامين: أولهما، أنه يتم من خلالها نقل المعلومات والبيانات التي تعد حساسة بشكل فريد للمرضى ولخصوصيتهم؛ ثانيهما، تعقد وتنوع الأجهزة - وخاصة الأجهزة المتصلة بشبكات الاتصال والإنترنت - والتي تشكل البنية التحتية لتعرض شبكات الرعاية الصحية لمجموعة واسعة من المخاطر الجنائية والاعتداء على الخصوصية عبر خوادم الشبكة أو مستلم البيانات.

وبناءً على ماتم ذكره، تعد الأجهزة الطبية المتصلة بشبكة الإنترنت والتطبيقات الصحية هدفاً لقراصنة المعلومات، فهناك المخاطر التي يمكن أن تطال المستخدمين في المستشفيات والمراكز الصحية من جهة، والمرضى من جهة أخرى، في حال نجح الجناة

(١) أوردت المادة الأولى من قانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات الكويتي تعريف نظام الحاسب الآلي بأنه: «مجموعة برامج وأنظمة معلوماتية معدة لتحليل المعلومات والبيانات والأوامر وبرمجتها وإظهارها أو حفظها أو إرسالها أو استلامها، ويمكن أن تعمل بشكل مستقل أو بالاتصال مع أجهزة أو أنظمة معلوماتية أخرى».

في اختراقها[٢]؛ وذلك، لتقدم الأجهزة والأنظمة الطبية القابلة للزرع من خلال تطور العلوم الهندسية وخاصة في مجال الإلكترونيات الدقيقة النانونية (تقنية الصغائر)[٣] والتكنولوجيات الحيوية المحوسبة.

حيث أضحى الموضوع المثار من المسائل القانونية والأخلاقية التي ترتبط بالتقنية الحيوية الحديثة، فالاعتداء على البيانات الشخصية وسوء استخدامها، حيث لم يعد هناك حماية لحق المرضى في خصوصيتهم الحيوية، فمن المحتمل أن يكون هناك مجموعة من التداعيات القانونية الناشئة عن التقارب بين تقنيات الميكروبولوجية (الأجهزة الطبية الملصقة أو المزروعة في جسم الإنسان) وتكنولوجيا المعلومات وتكنولوجيا النانو وخاصة في مجال البيانات، لذلك تعد من الجرائم الإلكترونية وتخضع لقانون مكافحة جرائم تقنية المعلومات والقوانين الخاصة.

أهداف البحث، تسعى هذه الدراسة إلى:

١ - التعريف بماهية الأجهزة الطبية الحيوية المحوسبة.

٢ - البحث في موضوع قرصنة الأجهزة الطبية (المحوسبة) الملصقة أو المزروعة في جسم الإنسان.

٣ - محاولة التعرف على الضوابط القانونية للمسئولية الجزائية لانتهاك حق الخصوصية عبر الأجهزة الطبية الحيوية المحوسبة.

٤ - يان بعض صور الجرائم المتعلقة بقرصنة الأجهزة الطبية المزروعة بالمرضى «تقنيات الميكروبولوجية».

(٢) Zoll PM. Resuscitation of the heart inventricular standstill by external electric stimulation, Neug1 J MED.

(٣) يعرف علم النانو بأنه: دراسة الظواهر والتحكم في المواد النانوية الجزيئية بمقياس الجزيئات، أما تكنولوجيا النانو فقد عرفت بأنها: توصيف وتطبيق وتصميم الهياكل والأجهزة والأنظمة عن طريق التحكم في الشكل والحجم ومقياس متناهي الصغر. للمزيد حول الموضوع انظر للباحث: دور بقع الدم في اكتشاف وإثبات الجرائم من خلال تقنية النانو، المجلة العربية للدراسات الأمنية والتدريب، المجلد ٣٠، العدد٦١، صفر ١٤٣٦هـ، جامعة نايف العربية للعلوم الأمنية، الرياض، ص٥١-ص٥٤.

أهمية البحث:

يسعى الباحث لدراسة: الحماية الجزائية للأجهزة الطبية الحيوية المحوسبة لعدة أسباب منها:

١ - يعد هذا النوع من الدراسة من الموضوعات ذات الأهمية في الحياة العملية والتطبيقية لتوفير الحماية الجنائية لمن يستخدمون الأجهزة الطبية المحوسبة، وتحديداً حمايتهم من قرصنة هذه الأجهزة، وما ينتج عنها من آثار على سلامة وحياة المستخدم لها، وخاصة بعد دمج الأجهزة الطبية والشبكات والبرمجيات وأنظمة التشغيل، وهذا يعني أن سلامة الأجهزة الطبية قابلة للاختراق من قبل الجناة، مما ترتب على الانتقال من الأجهزة الطبية المستقلة إلى التكامل مع الشبكات والبرمجيات إلى خلق مشاكل للحماية الجزائية والتقنية لقطاع الرعاية الصحية.

٢ - أما عملياً، فإن الحاجة العلمية لمواكبة التحولات التقنية الطبية بالخصوص، تستلزم استنفار جميع المستويات التشريعية والقضائية والفقهية؛ والتجند لتخطي أزمة القصور التشريعي بشكل توافقي لمواكبة التقدم الطبي عبر ترسانة تشريعية لنصوص طبية تحدد المسؤوليات والالتزامات بدقة لجميع العاملين بالقطاع الصحي، وتجرم بعض الاعتداءات على الأجهزة الطبية المحوسبة التي تتطلب المساءلة الجزائية.

٣ - الإضافة العلمية التي يأمل الباحث أن تتحقق للباحثين والمختصين من خلال هذه الدراسة المتواضعة ليساهم وبشكل يتناسب مع أهمية انتهاك وقرصنة الأجهزة الطبية الحيوية المحوسبة للمرضى.

مشكلة الدراسة:

أوجد التطور التكنولوجي مستجدات تقنية لم تكن في الحسبان من بينها الأجهزة الطبية الحيوية المحوسبة والذي دعم استخدامها بولادة الشبكة الإلكترونية للمعلومات، وهذا طبعاً يستلزم حماية قانونية محضة خاصة في الجانب الجزائي حتى نكون أمام حماية أكثر شمولية للأجهزة الطبية الحيوية، فهذه الأخيرة على المستوى الواقعي تحمل في طياتها جملة من التعقيدات والإشكاليات.

فإلى أي حد تمكن المشرع الكويتي من توفير الحماية الجزائية للأجهزة الطبية الحيوية المحوسبة؟

وهذه الإشكالية المحورية تتفرع عنها مجموعة من التساؤلات الفرعية ذات صلة بالإشكالية الرئيسة، وهي كالتالي:

- ماهي الأجهزة الطبية الحيوية المحوسبة ؟
- ما هي التحديات الناتجة عن مخاطر الهجمات الإلكترونية على الأجهزة الطبية المحوسبة؟
- ما هو موقف التشريعات المقارنة من الأجهزة الطبية الحيوية المحوسبة؟
- ما هي صور الجرائم الواقعة عبر الأجهزة الطبية الحيوية المحوسبة؟

منهجية الدراسة:

سنعمد إلى مقاربة هذه الدراسة، بالاعتماد على المنهج التحليلي النقدي المقارن لعلنا نتوفق في الخروج بخلاصات أو مقترحات، تسهم ولو بقليل في استكناه الغموض الذي يكتنف مفهوم الأجهزة الطبية الحيوية المحوسبة، والذي تتأسس عليها المسؤولية الجزائية، مع الاستئناس ببعض الجرائم التي تشكل اعتداء على هذه التقنية الحديثة وتوجب العقوبة الجزائية المنصوص عليها في التشريع الكويتي.

خطة البحث:

بناءً على ما سبق من اشكاليات وتساؤلات، وعلى هذا الأساس فإننا سنتطرق إلى الأجهزة الطبية الحيوية المحوسبة والتحديات الناجمة عن استعمالها في مبحث أول، حتى يتسنى لنا معرفة مدى ملاءمة التشريعات العقابية الموجودة لها. وفي نفس السياق وجدنا أنه من اللازم التعرف على صور الجرائم الواقعة عبر الأجهزة الطبية الحيوية المحوسبة في مبحث ثان.

والذي لا شك فيه أن هذه الدراسة، تحتاج إلى دراسة معمقة ومستفيضة، وهذا ما لا سبيل إليه في بحث موجز، ولذا آثرت الإيجاز دون التفصيل في بعض الموضوعات العلمية الصرفة، دون الإخلال بالمعنى العام للدراسة.

المبحث الأول
الأجهزة الطبية الحيوية المحوسبة والتحديات الناجمة عن استعمالها

ظهر مصطلح الصحة الإلكترونية في السنوات القليلة الماضية حيث استخدم في وصف الاستخدام المزدوج للتقنيات الطبية والاتصالات الإلكترونية في القطاع الصحي، ويمكن تعريفها في المجال الطبي بأنها[٤]: «استخدام البيانات الإلكترونية المرسلة والمخزنة والتي يتم استرجاعها آلياً للاستخدامات الطبية» .

لذلك، نتناول في المبحث الأول الأجهزة الطبية الحيوية المحوسبة والتحديات الناجمة عن استعمالها، وسيشتمل على مطلبين: يعرض أولهما لماهية الأجهزة الطبية الحيوية المحوسبة، ويركز الثاني على التحديات الناتجة عن مخاطر الهجمات الإلكترونية على الأجهزة الطبية الحيوية المحوسبة.

المطلب الأول
ماهية الأجهزة الطبية الحيوية المحوسبة

لإعطاء ماهية الأجهزة الطبية المحوسبة أهميتها يجب الوقوف على مفهوم الأجهزة الطبية الحيوية المحوسبة. وذلك في الفرعين التاليين؛ نفرد الأول: لمفهوم الأجهزة الطبية المحوسبة ونخصص الثاني لدراسة: آليات عمل الأجهزة الطبية المحوسبة.

الفرع الأول: مفهوم الأجهزة الطبية المحوسبة.

على مدى السنوات القليلة الماضية، كان هناك ارتباك متزايد حول تعريف ما يشكل جهازاً طبياً، فالأجهزة الطبية أضحت تتكون من البرمجيات والأجهزة الإلكترونية، بما في ذلك اللاسلكية، حيث تكون مفيدة لأغراض الرعاية الصحية[٥]؛ لذلك يمكن تعريف الاتصالات الطبية بأنها: «توظيف تقنية المعلومات لإرسال الخدمات والمعلومات الطبية والصحية من موقع إلى آخر».

(٤) "What is e-health" Journal of Medical Internet Research, 3(2),April-June 2001. https://www.jmir.org/2001/2/e20/ (last visited on 2 Aug. 2019).

(٥) Marr, B. (2018). Why the internet of medical things (iomt) will start to transform healthcare in 2018. Retrieved from https://www.forbes.com/sites/bernardmarr/2018/06/25/why-the-internet-of-medical-thingsiomt-will-start-to-transform-healthcare-in-2018/#3ed660424a3c

ويعرف الجهاز الطبي بشكل عام بأنه[٦]: «أداة أو جهاز أو آلة أو زرع أو أي مادة أخرى مشابهة ذات صلة بما في ذلك جزء أو ملحق، مخصص للاستخدام في تشخيص المرض أو العلاج...».

بينما تعرف الأجهزة الطبية الحيوية المحوسبة، بأنها[٧]: «الأجهزة التي يتم إدخالها جزئياً أو كلياً في جسم الإنسان والإبقاء عليها فترة من الزمن»؛ ويمكن تعريفها، بأنها: أجهزة إلكترونية[٨] بها أجزاء عضوية تزرع داخل جسم الإنسان بهدف الحفاظ على حياته لوجود خلل في أحد أعضائه أو وظائفه الجسدية.

وتأسيساً على ما تقدم ذكره، نجد أن الأجهزة الطبية الحيوية المحوسبة، هي: عبارة عن تكنولوجيا يتم دمجها أو إلصاقها في جسم الإنسان والتي تساعده في القيام بوظائفه الجسدية والحيوية، وتتضمن غرسات طبية تزرع داخل جسم الإنسان، بالإضافة إلى أن هناك التطبيقات الطبية المحوسبة الخارجية، وكلا النوعين يهدفان لتوفير الدواء أو العلاج بشكل مستمر للمرضى المصابين بأمراض مزمنة مثل السكري، أمراض القلب...الخ.

ومن أشهر أمثلة الأجهزة الطبية الحيوية المحوسبة ناظمات نبض القلب الآلية أو نظيرتها المحوسبة[٩]؛ أما أشهر الأجهزة خارج الجسد فهي منظومة ضخ الأنسولين

(٦) Safe Medical Devices Act. U.S. Food and Drug Administration office(1990), http://www.fda.gov/cdrh/devadvice/312.html.. (last visited on 6 Dec. 2018).

(٧) Jonson JA,FDA Regulation of medical deviecesCnogressional research service, June 25, 2012,Available form: http://www.fas.org/sgp/misc. (last visited on 5 Dec. 2018).

(٨) تنص المادة (١) من قانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات الكويتي على تعريف إلكتروني بأنه: " كل ما يتصل بتكنولوجيا المعلومات وذو قدرات كهربائية أو رقمية أو مغناطيسية أو بصرية أو كهرومغناطيسية أو وسائل أخرى مشابهة سلكية كانت أو لاسلكية وما قد يُستحدث من تقنيات في هذا المجال."

(٩) وتعتبر أجهزة تنظيم ضربات القلب المعروفة (Pace Maker) منتشرة بكثرة في الرعاية الصحية لمرضى القلب، وتتمثل طريقة عملها: بتركيب الجهاز في صدر المريض وتوصيله بالقلب، ويجب أن يتم برمجته بنظام معين يتناسب مع حالة قلب المريض، ويتم هذا الأمر بشكل دوري وليس من المنطق أن يتم فتح صدر المريض في كل مرة؛ لذلك يتم الاتصال مع الجهاز لاسلكياً باستخدام موجات الراديو ويتم برمجته. للمزيد حول الموضوع انظر:
Medtronic. (2018). MYCARELINK SMART™U.S. Retrieved from http://www.medtronic.com/us-en/mobileapps/patient-caregiver/mycarelink-smart-us.html(last visited on 3 Dec. 2018).

والمكونة من مضخة أنسولين Insulin Pumps، والتي توفر الأنسولين لجسد مرضى السكري حسب أوامر جهاز التحكم، والذي يقوم بقياس مستوى السكر في الدم، قبل تحديد حاجة الجسم من الأنسولين وتوقيتها[١٠]، لضخ جرعات الأنسولين تلقائياً في الدم، وهناك أجهزة الصعق الكهربائي (Cardiac Difibrillator) التي تستخدم أيضاً لصعق القلب بشحنة كهربائية تلقائياً في حال توقفه[١١]، ويمكن اختراق وقرصنة هذه الأجهزة والتي قد تؤدي إلى وفاة أو إيذاء المريض.

الفرع الثاني: آليات عمل الأجهزة الطبية الحيوية المحوسبة

وبناءً على ما تقدم ذكره سابقاً، تؤدي الأجهزة الطبية الحيوية المحوسبة دوراً متنامياً في رعاية الملايين من المرضى وهي ليست بجديدة، ولا حتى التطبيقات الحاسوبية في هذه الأجهزة هي بجديدة[١٢]، ما هو جديد هو استخدام الشبكات اللاسلكية[١٣]، لنقل البيانات الحيوية أو ما يسمى بالقياسات عن بعد، التي ترسلها الأجهزة إلى أجزاء أخرى من الشبكة الصحية الشخصية، وينتهي بها الأمر في خادم متخصص للتطبيقات الصحية والذي يقوم بدوره بالتواصل مع الطبيب، مما يسهل معرفة حالة المريض ومدى نجاعة العلاج المعطى له والتدخل في حالة الطوارئ (عند فشل الجهاز في أداء مهمته مثلاً) بالتحكم أحياناً في عمل هذه الأجهزة عن بعد[١٤]،

(١٠) د. محمد سعيد غزال، قرصنة الأجهزة الطبية الملصقة والمزروعة بالمرضى، المجلة العربية الدولية للمعلوماتية، المجلد الخامس، العدد ٩، ٢٠١٧، ص٤١.

(١١) BioTel. (2018). wEvent: Event monitoring. Retrieved from https://www.myheartmonitor.com/device/wevent/ (last visited on 15 Dec. 2018).

(١٢) Maisel WH. Medical device regulation: an introduction for the practicing physician. Ann Intern Med. 2004;140:296–302.

(١٣) حيث جاء في مرسوم بقانون اتحادي لدولة الإمارات العربية المتحدة رقم (٣) لسنة ٢٠٠٣ في شأن تنظيم قطاع الاتصالات؛ حيث عرفت شبكة الاتصالات بأنها: «منظومة تحتوي على جهاز أو وسيلة اتصال أو أكثر، بهدف نقل أو بث أو تحويل أو استقبال أي من خدمات الاتصالات، وذلك بواسطة أي طاقة كهربائية أو مغناطيسية أو إلكترومغناطيسية أو إلكتروكيميائية أو إلكترو ميكانيكية وغير ذلك من وسائل الاتصال».

(١٤) الإشارة إلى أن هذا النوع من الأجهزة الطبية تمت حوسبتها وشبكها لاسلكياً بهدف تحسين أدائها وزيادة الدقة في خياراتها، حيث تقوم البرمجيات الموجودة في الجهاز ببث إشارات تمثل البيانات الحيوية للقلب مثلاً، عادة على شكل تقرير برسومات بيانية يقرؤها الطبيب المختص للتأكد من صلاحية الجهاز وللتدخل وقت الحاجة بالتحكم في عمل الجهاز عن بعد. للمزيد انظر: د. محمد سعيد غزال، المرجع السابق، ص٤٥

وأعطى هذا التواصل عن بعد ميزة عظيمة وهي تمكين المريض من الحياة بشكل مشابه للشخص الطبيعي من حرية التنقل والذهاب للعمل وغيرها من النشاطات دون الحاجة لزيارة الطبيب بشكل متكرر أو البقاء في المستشفى لفترات طويلة[١٥].

ومن الناحية العملية، فإن التحكم بالأجهزة الطبية المزروعة يمكن أن يتم بواسطة معدات رقمية على نحو يؤدي إلى تعديل طريقة عمل الجهاز المزروع، مثلاً لجهة تغيير كمية الأنسولين التي يجب أن تحقنها مضخة مزروعة بالجسم في دم المصاب بداء السكري[١٦]...، ويستطيع القراصنة الاستفادة من برامج الترقية التي يتم إدخالها على المعدات المزروعة لتحسين أدائها، وذلك على نحو شبيه ببرامج الترقية الكمبيوترية المعهودة.

وكذلك، تمثل الشبكات اللاسلكية، مصدراً أكبر للمخاطر، نظراً لحجم عدد نقاط النفاذ إليها، وهي الشبكة التي يتم فيها استخدام موجات الراديو، هذا وقد نص قانون رقم ٣٧ لسنة ٢٠١٤ بإنشاء هيئة تنظيم الاتصالات وتقنية المعلومات الكويتي في المادة الأولى على تعريف الموجات الراديوية بأنها: «موجات كهرومغناطيسية ذات ترددات تزيد عن ثلاثة كيلو هيرتز تبث في الفضاء دون موجِّه اصطناعي». وذلك، لتبادل المعلومات بدلاً من الأسلاك أو الكوابل[١٧]، ويمكن استخدامها للربط بين الشبكات.

المطلب الثاني
التحديات الناتجة عن مخاطر الهجمات الإلكترونية على الأجهزة الطبية المحوسبة

الفرع الأول: مدى الحاجة إلى إقرار حماية للأجهزة الطبية الحيوية المحوسبة

رغم فوائد الأجهزة الطبية الحيوية المحوسبة غير المحدودة في تقديم الخدمات والرعاية الصحية للمرضى كما بينا سابقاً، إلا أن هذه الأجهزة معرضة في الوقت

(١٥) د. محمد سعيد غزال، مرجع سابق ، ٢٠١٧، ص٤١.

(١٦) Dario. (2018). Dario blood glucose monitoring system. Retrieved from https:// mydario.com/(last visited on 3 Dec. 2018).

(١٧) د. منى جبور ود. عزيز بربر، أمن الشبكات والإنترنت، الحلقة العلمية (الإنترنت والإرهاب) والمنعقد في جامعة نايف العربية للعلوم الأمنية – الرياض–خلال الفترة من ١٧–٢١ /١١/١٤٢٩هـ، الموافق ١٩–١١– ٢٠٠٨، ص٧.

ذاته بشكل كبير لمخاطر الهجمات الإلكترونية، مما يسبب مخاطر صحية للمرضى قد تصل إلى الوفاة، بسبب انقطاع العلاج أو زيادته عن الحد المقبول طبياً، فتعطل جهاز ناظم نبض القلب (بسبب هجوم متعمد عبر شبكات الاتصال) قد يؤدي لوفاة المريض بسبب ارتفاع ضغط الدم الناتج عن ازدياد معدل نبض القلب، وقس على ذلك أيضاً مضخة البنسلين التي يؤدي تعطلها إلى جلطات دماغية بسبب ازدياد معدل سكر الدم، أو الإغماء، وربما الموت في حالة نقص هذا المعدل عن الوضع الطبيعي[١٨]، وخاصة إن شبكات الاتصال[١٩]، هي الوسيط لتمكين الأطباء من التواصل عن بعد مع الأجهزة الحيوية الطبية، حيث يمكن نقل هذه المعلومات والبيانات مباشرة إلى الأطباء أو بشكل غير مباشر من خلال مزود طرف ثالث[٢٠]، في بعض الأحيان باستخدام أنظمة لاسلكية، للمساعدة في تشخيص وإدارة المشاكل الطبية المزمنة.

ومما تجدر الإشاره إليه في هذا الشأن أن قانون مكافحة جرائم تقنية المعلومات الكويتي رقم (٦٣) لعام ٢٠١٥ لم ينص على تعريف الوسيط في خدمة الإنترنت، مع أن له دوراً مهماً في إيصال المعلومات والبيانات أو توريدها أو حفظها، وهو يتحمل جزءاً من المسئولية الجزائية عن بعض الجرائم الإلكترونية الطبية.

وفي الوقت الحاضر، فإن تدفق المعلومات بين الأجهزة المزروعة ومقدمي الخدمات[٢١] هو في الغالب أحادي الاتجاه (من الجهاز إلى مزود الخدمة)، بيد أنه من الناحية النظرية يمكن بسهولة تعديل التكنولوجيات الحالية بحيث يمكن إجراء تفاعلات عن بعد بين مقدمي الخدمات والأجهزة الطبية (مثل إعادة برمجة مضخة الأنسولين أو جهاز تنظيم ضربات القلب).

---

(١٨) د. محمد سعيد غزال، قرصنة الأجهزة الطبية الملصقة والمزروعة بالمرضى، مرجع سابق، ص٤٣.

(١٩) تجدر الإشارة إلى أن المشرع الكويتي عرف في المادة الأولى من قانون رقم ٣٧ لسنة ٢٠١٤ بإنشاء هيئة تنظيم الاتصالات وتقنية المعلومات شبكة الاتصالات الخاصة بأنها: «منظومة اتصالات تشغل لمصلحة شخص واحد أو مجموعة واحدة من الأشخاص تجمعهم رابطة ملكية مشتركة لخدمة حاجاتهم الخاصة».

(٢٠) Hashmi, N., Myung, D., Gaynor, M., & Moulton, S. (2005). A sensor-based, web service-enabled, emergency medical response system. Paper presented at the Proceedings of the 2005 workshop on End-to-end, sense-and respond systems, applications and services.

(٢١) تعرف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠ مزود الخدمة بأنه: «أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها».

وقد أظهرت الدراسات[٢٢] مؤخراً إمكانية قرصنة مضخة الأنسولين من مرضى السكري عبر جهازه الطبي الخاص؛ فنقص الحماية القانونية يؤدي إلى تعرض الأجهزة الحيوية للاختراق والاعتداء على خصوصية المرضى[٢٣]، أضف إلى ذلك، إمكانية تعرض المرضى إلى الوفاة أو الإيذاء الجسدي عبر إدخال بيانات غير صحيحة أو التلاعب بها؛ مما يؤدي إلى تشخيص أو علاج خاطئ.

وهكذا، يسعى قراصنة الإنترنت في محاولاتٍ جديدة من نوعها إلى استهداف الأجهزة الطبية والمستشفيات[٢٤]، ويأتي هذا التحذير من هيئة الأغذية والعقاقير بالولايات المتحدة الأمريكية بعد أن شهد العام الحالي العديد من العيوب والمشكلات في الأجهزة الطبية المحوسبة؛ وأعلنت الهيئة أنه على الشركات المنتجة للأجهزة الطبية أن تتبع القواعد الإرشادية الجديدة التي أصدرتها الهيئة[٢٥]، وأن تكون متيقظة باستمرار لمواجهة أي تهديد للأجهزة الطبية عبر الإنترنت، فالمخاطر الإلكترونية عبر الإنترنت هي واقعية وفي تغير مستمر وأكثر مما سبق، وأن هذه التهديدات حقيقية، وهناك هجمات إلكترونية وتسلل تتعرض لها الأجهزة داخل المستشفيات، الأمر الذي يعرض سلامة المرضى للخطر.

---

(٢٢) Blackhat.com website.Accessed (last visited on 12 Dec. 2018). Available at:http://www.blackhat.com/html/bh-us-11/bh-us-11-briefings.html

(٢٣) HIPAA-Report2003. Summary of HIPAA Health Insurance Probabilityand Accountability Act. US Department of Health and Human Service, May 2003.

(٢٤) وتجدر الإشارة إلى قيام باحثين بدراسة مخاطر الأجهزة الطبية الحيوية، حيث توصلا إلى أن آلاف الأجهزة الطبية الحساسة، مثل أجهزة أشعة الرنين المغناطيسي، يمكن للجناة الوصول إليها عبر الإنترنت، وأشارا إلى أن نحو ٦٨ ألف جهاز طبي من مجموعة واسعة من الهيئات الصحية الأمريكية، قد تعرضت للاختراق بالفعل، وعرض الباحثان (سكوت إيرفن ومارك كولار) اللذان يعملان في مجال أمن الحواسيب، نتائج دراستهما في مؤتمر ديربيكون لمكافحة القرصنة ؛ وكشف الباحثان عن أنهما صنعا أجهزة طبية مزيفة، جذبت آلاف القراصنة ؛ واستخدم الباحثان محرك البحث شودان : وهو محرك بحث مخصص للأجهزة الطبية المتصلة بالإنترنت، للبحث عن البرمجيات المعرضة للقرصنة، في مجموعة واسعة من الشركات المزودة للخدمات الطبية، مثل إجراء الأشعة وعيادات الأطفال وغيرها، وقال الباحثان أنهما اكتشفا وجود آلاف حالات القصور والهجمات علي الأجهزة الطبية.
James Niccolai , 2015 ,Thousands of medical devices are vulnerable to hacking, security researchers sayThe security flaws put patients' health at risk.
https://www.csoonline.com/article/2987786

(٢٥) Tatham, M. (2018). Identity theft statistics. Retrieved from https://www.experian.com/blogs/ask-experian/iden tity-theft-statistics/(last visited on13 Dec. 2018).

وأظهرت العديد من الدراسات التي أجريت من قبل الباحثين[٢٦] نقاط الضعف لهذه الأجهزة مما يضر بتشغيلها الآمن، وتوافر سرية وسلامة البيانات المرتبطة بها، حيث سلطت هذه الدراسات الضوء على تحديات سلامة المرضى والأمن الإلكتروني مع التأكيد على طبيعة العلاقة بين التخصصات الطبية والتقنية والأمنية المطلوبة لتقييم المخاطر والمساهمة في حماية هذه الأجهزة، فاتصال الأجهزة الطرفية والتي يعرفها قانون هيئة تنظيم الاتصالات وتقنية المعلومات الكويتي في مادته الأولى على أنها: «أجهزة الاتصالات التي تستخدم من المستفيد من أجل إرسال اتصال أو استقباله أو تمريره أو إنهائه». وهي غير تقليدية مثل الأنسجة الطبية المتصلة بجهاز التحفيز الكهربائي، حيث ركزت البحوث حول الثغرات الأمنية على المرضى؛ وكشف الباحثون عن أن العديد من المنتجات الطبية، كأجهزة ضخ وحقن العقاقير، والأجهزة المنظمة لضربات القلب، قد تعرضت لهجمات من الإنترنت على أجهزة الرنين المغناطيسي وغيرها من الأجهزة الطبية الأخرى.

وكيف يمكن التحكم في مضخة الأنسولين المزروعة في جسده، وذلك بواسطة جهاز كمبيوتر محمول وبعض معدات التوصيل اللاسلكي، حيث يتم أولاً التقاط الإشارات اللاسلكية المرسلة إلى مضخة الأنسولين بواسطة الكمبيوتر، ومن ثم يجري تبديل البيانات التي ترسلها المضخة على النحو المطلوب من جانب الجاني، ويعاد إرسال البيانات المعدلة إلى المضخة التي تصبح تضخ مادة الأنسولين بكميات محددة بالاستناد إلى البيانات المعدلة[٢٧]، وليس إلى البيانات الصحيحة، ومن الواضح أن هذه البيانات الخاطئة يمكن أن تؤدي إلى قتل المريض، مع ضخ الكميات غير المناسبة لحالته الحقيقية... هذه التجربة يمكن القيام بها مع العديد من الأجهزة الطبية المزروعة الأخرى، حسب ما تؤكده وزارة الأمن الداخلي الأمريكي، وبصورة خاصة الأجهزة

(٢٦) Filkins, B. (2014). Health care cyberthreat report: Widespread compromises detected, compliance nightmare on horizon. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/healthcare-cyberthreat-report-widespread-compromises. (last visited on 18 Dec. 2018).
- Halperin D, Heydt-Benjamin TS, Ransford B, et al. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses; Paper presented at: Security and Privacy, 2008. SP 2008.IEEE Symposium; Oakland, California, USA. May 18–, 2008.

(٢٧) Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of things (IoT): A vision, architecturaltracking system on wrist devices. Paper presented at the Wireless Health.

من الجيل الجديد الأكثر تطوراً واعتماداً على التكنولوجيات الرقمية؛ والمعروف أن الأجهزة المحمولة من أجهزة كمبيوتر لوحية أو أجهزة هاتفية «ذكية» باتت رائجة جداً في الأوساط الطبية والإستشفائية[٢٨]، وذلك لتخزين البيانات الطبية أو لتبادل الاتصالات والبيانات مع المرضى أو الأقسام الاستشفائية، ما يعرض هذه الاتصالات للمخاطر نفسها التي تتعرض لها الاتصالات الكمبيوترية بصورة عامة.

الفرع الثاني: موقف التشريعات من الأجهزة الطبية الحيوية المحوسبة.

ان تطور المعلوماتية طوّر الإطار القانوني للتبادلات الإلكترونية، وتأتي الحماية القانونية للبيانات الصحية أساساً من النصوص العامة في القانون الداخلي والدولي، ومن المعايير الحقوقية التي وضعتها الدول وتدارستها المؤتمرات العالمية (تولوز ٢٠٠٦ مثلاً) لتنظيم النشاط الإلكتروني، ونستطيع أن نقدم لمحة مختصرة جداً عن التشريع في بعض الدول.

أولاً: موقف بعض التشريعات العربية

موقف المشرع الكويتي: نصت المادة (٣) من قانون مكافحة جرائم تقنية المعلومات الكويتي رقم (٦٣) لعام ٢٠١٥ على أنه: «يعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين كل من: .... ٣ - غير أو أتلف عمداً مستنداً إلكترونياً يتعلق بالفحوصات الطبية أو التشخيص الطبي أو العلاج الطبي أو الرعاية الطبية أو سهل للغير فعل ذلك أو مكنه منه، وذلك باستعمال الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات...».

وباستقراء هذا النص القانوني نجد وبدون شك أن المشرع الكويتي، لم ينص مباشرة على جريمة قرصنة الأجهزة الطبية المزروعة والملصقة على جسد المرضى (الأجهزة الطبية الحيوية)، رغم أهميتها القانونية والعملية لحمايتهم. وإن كانت تبدو أنها محمية بشكل كافٍ من المشرع الكويتي بالنسبة للسجلات الإلكترونية الطبية، إلا أنها تثير العديد من الصعوبات وخصوصاً ما يتعلق بالأمن الإلكتروني وحماية المرضى، لذلك يجب على المشرع ألا يكون قاصراً على تنظيم بعض الجرائم الإلكترونية دون الأخرى.

(٢٨) http://www.accemagazine.com/article.php(last visited on 3 Dec. 2018).

وكلنا أمل في المشرع الكويتي أن يأخذ بتجارب وتشريعات الدول التي نصت على الحماية الجزائية للأجهزة الطبية الحيوية، وخاصة المادة (٧) من قانون مكافحة جرائم تقنية المعلومات لدولة الإمارات، والتي تكفل تحقيق الفعالية المرجوة من قانون الجرائم الإلكترونية بالنظر لخصائص هذا النوع من الجرائم وخطورتها على حياة وسلامة أجسام الأفراد من الإيذاء.

لذلك، نجد بأن المشرع الاتحادي في دولة الإمارات العربية المتحدة قد نص على الجرائم المتصلة بالأجهزة الطبية المحوسبة - وحسناً فعل - وذلك، في منطوق المادة (٧) من قانون مكافحة جرائم تقنية المعلومات رقم (٥) لسنة ٢٠١٢ [٢٩] على أنه: «يعاقب بالسجن المؤقت كل من حصل أو استحوذ أو عدل أو أتلف أو أفشى بغير تصريح بيانات أي مستند إلكتروني أو معلومات إلكترونية عن طريق الشبكة المعلوماتية أو موقع إلكتروني أو نظام المعلومات الإلكتروني أو وسيلة تقنية معلومات، وكانت هذه البيانات أو المعلومات تتعلق بفحوصات طبية أو تشخيص طبي، أو علاج أو رعاية طبية أو سجلات طبية».

حقيقة، لم نجد أي نص صريح على تجريم الاعتداء على الأجهزة الطبية المحوسبة من حيث قرصنتها في التشريع الأردني، ولكنه نص في المادة (٤) من قانون رقم (٢٧) لعام (٢٠١٥) في شأن الجرائم الإلكترونية على أنه: «يعاقب كل من أدخل أو نشر أو استخدم قصداً برنامجاً عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ أو التقاط أو تمكين الآخرين من الاطلاع على بيانات أو معلومات أو إعاقة أو تشويش أو إيقاف أو تعطيل عمل نظام معلومات أو الوصول إليه أو تغيير موقع إلكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفة أو انتحال شخصية مالكه دون تصريح أو بما يجاوز أو يخالف التصريح بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (٢٠٠) مائتي دينار ولا تزيد على (١٠٠٠) ألف دينار».

(٢٩) وتجدر الإشارة إلى أن المشرِّع الاتحادي في دولة الإمارات قد نص في المادة (٢) من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢: (على تجريم صور الدخول إلى موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلومات، أو وسيلة تقنية معلومات، بهدف الإلغاء أو الحذف أو التدمير أو الإفشاء، أو الإتلاف أو التغيير أو النسخ أو النشر أو إعادة النشر لأيّ بيانات أو معلومات).

ثانياً: موقف بعض التشريعات الأجنبية

بداية، أطلقت الإدارة الأميركية في شباط ٢٠٠٥ مشروع خلق شبكة على مدى البلاد للسجلات الصحية الإلكترونية (EHR) في خلال عشر سنوات، وكذلك أطلقت إنكلترا عام ٢٠٠٢ برنامجاً وطنياً عشرياً يختص بتقنيات المعلومات في الحقل الطبي، كما أعلنت مايكروسوفت أخيراً خططها لموقع الـ Health Vault website وهو خدمة جديدة لتخزين وإدارة والحصول على معلومات المرضى الطبية[٣٠] ويعمل كخدمة مشفرة على الشبكة تقدم إمكانية جمع بيانات طبية من مصادر متعددة كشركات التأمين ومقدمي الخدمات الصحية ومن بعض الأجهزة الطبية (كأجهزة قياس ضغط الدم مثلا). وتنوي google أيضا تقديم خدمة مشابهة.

أ - موقف المشرع الأوروبي:

اعتمد الاتحاد الأوروبي[٣١] عام ١٩٨٥ مقاربة جديدة فيما يتعلق بالمعدات الطبية لتسهيل تداولها بين الدول الأعضاء، وصدرت توصيات عدة في هذا الصدد تتعلق بالشروط والمعايير الواجب توافرها في المعدات الطبية والتي على المُصنّع الالتزام بها كي تُصنّف على أنها من صنع الاتحاد الأوروبي، وأهم هذه الشروط تتعلق بسلامة المريض، أداء المعدات، أمان الاستخدام، المخاطر والمنافع، فصدرت التوصية رقم ٩٣/٤٢ المتعلقة بالشروط الأساسية في موضوعات الأمان والبيئة وحماية المستهلك، وقد تم تدعيم هذه التوصية بموجب التعديل ٢٠٠٧/٤٧، كما صدرت التوصية رقم ٩٠/٣٨٥ دعّمت بموجب التعديل عينه والمتضمنة المتطلبات الأساسية فيما يتعلق بالأجهزة المعدة للزرع في جسم الإنسان، والتوصية رقم ٩٨/٧٩ المتعلقة بالمعدات الطبية للتشخيص المخبري.

(٣٠) http.//www.healthvault.com. (last visited on 10 Dec. 2018).

(٣١) وتجدر الإشارة إلى أن هناك اتفاقيات ومعاهدات دولية لمكافحة الجريمة الإلكترونية منها: - اتفاقية الاتحاد الأوروبي الخاصة بحماية التعامل الإلكتروني مع البيانات الشخصية لسنة ١٩٨٩م.- الإتفاقية الأوروبية العالمية للجرائم السيبرانية لسنة ٢٠٠١م.– معاهدة المجلس الأوروبي للجرائم السيبرانية لسنة ٢٠٠٤م، والتي انضمت إليها الولايات المتحدة الأمريكية لعام ٢٠٠٦م. للمزيد انظر: د. جاسم محمد العنتلي، الجريمة والتكنولوجيا الحديثة (دراسة مقارنة)، مجلة العلوم الشرطية والقانونية، المجلد السادس، العدد الأول، يناير، ٢٠١٥، ص ١٥٥.

ب - موقف المشرع الأمريكي

في الولايات المتحدة الأمريكية من أهم القوانين التي سُنت لحماية المعلومات الصحية المحوسبة على المستوى العالمي قانون لضمان أمن (The Health Insurance Portability and Accountability Act of 1996 (HIPAA المعلومات الصحية، وهذا القانون يجبر المؤسسات الصحية (كبيرة كانت أو صغيرة) على حماية المعلومات الصحية للمرضى من الفقدان أو التلف أو اطلاع أشخاص غير مصرح لهم سواء كانت ورقية أو رقمية، وذلك بتحديد سياسات وإجراءات لأمن المعلومات؛ وعقوبة المخالف وتتضمن غرامة كحد أعلى ٢٥٠٠٠٠$ والسجن عشرة أعوام، والمعلومات الصحية التي تخضع لحماية هذا القانون المعلومات المرضية مثل التاريخ المرضي ونتائج التحاليل المعملية والأشعة التصويرية، ونتائج عينات الدم والأنسجة، ونتائج الفحص البدني، والمعلومات الخاصة بالأمراض والإصابات؛ بالإضافة إلى أنه منذ زمن بعيد يعرف التشريع الأمريكي قانوناً يحمي الخصوصية[٣٢].

وتتولى السلطات التنظيمية، مثل إدارة الغذاء والدواء الأمريكية (FDA)[٣٣]، مسئولية ضمان سلامة الأجهزة الطبية وفعاليتها وأمنها، وقد أقرت الهيئات الرقابية بخطورة المشكلة من خلال نشر توصيات لإدارة مخاطر الأمن الإلكتروني وحماية المعلومات الصحية للمرضى.

وكذلك نجد أن هناك قانوناً فدرالياً يضع معايير خصوصية المريض في ٥٠ ولاية The federal Health insurance portability and accountability Act (HIPAA)، ووضِع موضع التنفيذ بتاريخ ١٤ نيسان ٢٠٠٣ ويطبق على السجلات الطبية التي يحفظها ويديرها المجهزون والمؤسسات المختصة، والخطط الصحية والمقاصة الصحية إذا كانت وثائقها إلكترونية، وباختصار هو ينظم عملية جمع وإدارة

(٣٢) "dans la plupart des domaines ayant un lieu avec le commerce électronique, l'union européenne est en retard sur les U.S.A...dans le domaine de la protection de la vie privée,elle a des kilomètres d' avance ", Théo Hassler, Les Données personnelles et la protection des personnes, Les premières journées internationales de droit de commerce électronique, p114.

(٣٣) US Food Drug Administration .Content of Premarket Submissions for Management of Cybersecurity in Medical Devices.US Food and Drug Administration; 2014. Available from: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf(last visited on 23 Dec. 2018).

وبث المعلومات الطبية الممكننة وحق المريض في الدخول إلى سجلاته الخاصة، لكنه ليس شاملاً، وتبقى مساحة واسعة من الأنشطة بحاجة لتوجيهات تضمن الحماية[٣٤].

أما قانون إعادة إصلاح النظام الصحي الاميريكي للعام ٢٠٠٩ فقد أولى الملف الطبي الإلكتروني اهتماماً خاصاً، ونظم حماية معلوماته وطريقة استخدامه من سائر أطراف العلاقة الطبية، وأعطى المريض صلاحيات كثيرة كحقوق أساسية له، وإشراكه باتخاذ القرار وجعله محور العلاج، وأجبر جميع مستخدمي المعلومات الصحية على تبادلها إلكترونياً، ونظم حمايتها وطريقة استخدامها من سائر أطراف العلاقة الطبية وأعطى المريض صلاحيات كثيرة كحقوق أساسية له وإشراكه باتخاذ القرار وجعله محور العلاج.

ج – موقف المشرع الفرنسي

يحصي التشريع الفرنسي[٣٥] حوالي سبعة اعتداءات على هذا الحق، ويحيل ذلك إلى النصوص ٢٢٦–١٧ [٣٦] إلى ٢٢٦–٢٢ من قانون العقوبات الفرنسي الجديد الصادر سنة ١٩٩٢ والمعمول به منذ أول مارس ١٩٩٤ [٣٧]، وكذلك، قانون رقم ١٩٨٨/١٩ المعروف بقانون Godfrain والمتعلق بالغش ألمعلوماتي والجرائم الإلكترونية، حيث أوجد هذا القانون بعض الجرائم المختصة للوقاية من الاعتداءات

(٣٤) وتجدر الإشارة إلى أن أول قضية نظرت فيها وزارة العدل الأمريكية تطبيقا لـ HIPAA كانت سنة ٢٠٠٧ بدعوى سرقة سجلات طبية إلكترونية تتعلق بـ ١١٣٠ مريضاً في عيادة كليفلاند، حيث عمد أحد العاملين في المؤسسة إلى سرقة وبيع الملفات لمنظمة إجرامية حصلت بفعلها على ٧ ملايين دولار من التأمين المرضي Medicare.

للمزيد انظر: خليل خير الله، تنظيم الملف الطبي الإلكتروني وحماية بياناته في إطار تطوير القطاع الصحي والخدمات الصحية، مقال منشور على الموقع الإلكتروني:
https://www.lita-lb.org/images/publication/_.pdf
(last visited on 8 Dec. 2018)

(٣٥) وتجدر الإشارة إلى أن المشرِّع الفرنسي أصدر عدة قوانين لمعاقبة أنواع الاعتداءات على الأنظمة المعلوماتية ومنها: قانون المعلوماتية والحريات رقم ٧٨/١٧ في يناير ١٩٧٨ للمعالجة الإلكترونية للبيانات الاسمية، وقد خضع لبضعة تعديلات، بموجب القانون ٢٠٠٤/٨٠١.

(٣٦) تم تعديل المادة ٢٢٦ فقرة ١٧ بموجب المرسوم رقم ٢٠١٨-١١٢٥ المؤرخ ١٢ ديسمبر ٢٠١٨.
https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte (last visited on 18 Aug. 2019)

(٣٧) https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte (last visited on 18 Aug. 2019)

على أنظمة المعالجة الآلية للبيانات، والذي أصبح بعد تعديل قانون العقوبات الفرنسي لعام ١٩٩٤، تحت رقم المادة (٣٢٣ فقرة ٣)؛ والمتعلق بتجريم الاعتداء على العناصر غير المادية أي المعلومات والبرامج، بحيث يجرم إدخال بيانات بطريق الغش لنظام المعالجة الآلية أو محو البيانات أو تعديلها، وجعل عقوبة هذا الفعل مشددة وهي الحبس ثلاث سنوات وغرامة ٣ ملايين يورو، من دون أن يحدد شروطاً تتعلق بطبيعة المعلومات محل الإتلاف بل ترك النص عاماً ليتسع لأنواعها كافة.

وفي نفس السياق، تناول المرسوم رقم ٩٦٠-٢٠٠٧ تاريخ ١٥ أيار ٢٠٠٧ [٣٨] تدابير ومعايير سرية المعلومات الطبية المحفوظة إلكترونياً أو المنقولة عبر الطرق الإلكترونية، ونص قانون المعلوماتية والحريات[٣٩] في مادته ٣٨ و ٣٩ على حق الدخول إلى المعطيات الطبية الشخصية وحق اعتراض المريض على تبادل المعلومات الخاصة به لأسباب قانونية، ونصت المادة ١١١٠ -٤ بند ٣ من قانون الصحة العامة الفرنسي لعام ٢٠٠٢ [٤٠] على أن المريض الموجود بعناية الفريق الطبي، في مؤسسة صحية، تكون المعلومات التي تخصه وبإرادته، بعهدة مجموع الفريق، وكذلك إذا تعلق الأمر بمجموعة معالجين في عيادة أو مركز طبي، وتنص هذه المادة على دور القضاء والهيئة الوطنية للمعلوماتية والحريات CNIL في التدابير المتعلقة بضمان سرية المعلومات الطبية وعقوبات مخالفتها.

ويبقى رضا المريض مطلوباً قانوناً وبشكل صريح عند تخزين المعلومات واستدعائها بحسب المادة ١١١١-٨ بند ١ من قانون الصحة العامة آنف الذكر، ومن ثوابت اللجنة الوطنية للمعلوماتية والحريات CNIL أن اقتسام معلومات المريض الطبية عبر الإنترنت لغاية تنسيق المعالجة مشروط بموافقته الصريحة المسبقة.

مثلما أن الغرفة الجزائية لمحكمة النقض الفرنسية عرضت عليها كثير من حالات الاعتداء المرتبطة بحوادث الدفع، لكن رغم ذلك فإن القرارات المتخذة بشأن

(٣٨) Décret n° 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le code de la santé publique (dispositions réglementaires).

(٣٩) Loi informatique et libertés codifiée par la loi n°2004-801 du 6 aout 2004 pour l'harmonization avec la directive européenne.

(٤٠) Code de la Santé Publique, dernière modification : 1 juillet 2014.

هذه الاعتداءات تعد جد نادرة[٤١]؛ وتعتبر التوصية الأوروبية رقم ٤٤/٩٥ المصادرة بـ ١٩٩٥/١٠/٢٤ الخاص بحماية الأفراد من جمع المعلومات ذات الطابع الشخصي والمتعلقة بحماية البيانات الاسمية والشخصية والحياة الخاصة المصدر الذي استند إليه المشرع الفرنسي في تفعيل القواعد الضابطة أو الحامية لهذه الحقوق[٤٢].

المبحث الثاني
صور الجرائم الواقعة عبر الأجهزة الطبية الحيوية المحوسبة

كما هو الأمر عليه بالنسبة إلى جميع النشاطات الإنسانية، فإن تكنولوجيا المعلومات والاتصالات دخلت عالم الطب والعلاجات من الباب العريض، وذلك ليس لتشغيل أجهزة التشخيص والمعالجة فحسب، وإنما كذلك، بالنسبة إلى التقنيات التي يتم زرعها في أجساد المرضى لتشغيل بعض الوظائف الحيوية، من قبل آلات تنظيم نبضات القلب أو مضخات مادة الأنسولين، وغيرها أيضاً. ويعتمد الجيل الجديد من هذه المعدات المزروعة في الأجسام على التكنولوجيا المعلوماتية بصورة متزايدة، مما يؤدي إلى تحسين أدائها كثيراً، ولكن الأمر أوجد أيضاً خطراً مستجداً يتمثل بتعريضها - أي تعريض الأجهزة المزروعة - إلى خطر تعرضها لهجمات القراصنة المعلوماتيين (كما بينا سابقاً)، وكذلك إلى خطر اعتداء القراصنة على المرضى عن طريق التحكم بالأجهزة على نحو يجعلها تعمل بطريقة معاكسة لما ينبغي أن يكون عليه العلاج الطبي المناسب.

المطلب الأول
الجرائم الواقعة على الأجهزة الطبية الحيوية المحوسبة

على نحو متزايد، تعتبر الرعاية الصحية هدفاً رئيساً للهجمات الإلكترونية، وقد صدر تقرير معهد سانس مؤخراً يفيد بأن ٩٤٪ من منظمات ومؤسسات الرعاية الصحية كانت ضحية لهجوم إلكتروني، ويشمل ذلك هجمات على الأجهزة الطبية

(٤١) Cass.crim, 25oct,1995, Bernard R et Gie – Cass.crim, 19dec, 1995, M, R Et CPIT, ibid, P29.

(٤٢) Marie –Pierre, fenoll-trousseau, gerardhaas, op.cit, p30.

والبنية التحتية[٤٣]، وإن الانتشار السريع للأجهزة الطبية القادرة على تخزين ونقل المعلومات الطبية للمرضى والإمكانية النظرية لإعادة برمجة الأجهزة الطبية المزروعة عن بعد تثير مخاوف مهمة تتعلق بالأمن والخصوصية والسلامة[٤٤].

الفرع الأول: جرائم الإضرار بالبيانات الطبية الحيوية المحوسبة.

ساعد توافر تقنية اللاسلكي مع تطبيقات الأجهزة الطبية الملصقة بجسد المريض أو المزروعة داخل جسده، والمستخدمة في تنظيم علاج الأمراض المزمنة، إمكانية قرصنة هذه الأجهزة، فأضحى خطر أختراقها يتعدى المخاطر المألوفة ليصبح خطراً على السلامة الجسدية للمريض[٤٥]، فقرصنة أجهزة التقنية الميكروبولوجيه (ناظمات نبض القلب وتقنية ضخ الأنسولين...الخ) قد يؤدي إلى جريمة قتل بحق المستخدم؛ لإمكانية التعديل والتلاعب على برمجياتها، ومن ثم التحكم فيهاعن بعد، بواسطة أجهزة بسيطة ومتوفرة، بالإضافة إلى أن كثيراً من الأخطاء قد تحصل بسبب الإهمال أو عدم المعرفة من قبل الفنيين المشغلين للأجهزة الطبية[٤٦]؛ وذلك من خلال

(٤٣) SANS Institute . Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon. Filkins B: 2014. [Accessed June 18, 2018].Available from: http://www.sans.org/reading-room/whitepapers/firewalls/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735.

(٤٤) MaiselWH, Kohno T. Improving the security and privacy of implantable medical devices. N Engl J Med. 2010;362:1164–1166.

(٤٥) Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. Crime .Prevention Studies, 16, 41–96.

(٤٦) فكثير من الأخطاء تحصل بسبب الإهمال من قبل الفنيين المشغلين للأجهزة الطبية، وأفضل مثال على ذلك هو ما حصل من جراء استخدام جهاز (ثيراك ٢٥) Therac ٢٥ في أواسط ثمانينات القرن الماضي، وهو جهاز طبي محوسب كان يستخدم في علاج مرضى السرطان بواسطة الأشعة وبشكل آلي، فقد تسبب استخدام الجهاز في عدة مستشفيات في أمريكا بوفاة ستة مرضى وإصابة العديد منهم بجروح ومشاكل صحية ؛ وكما حصل في قضية ثيراك ٢٥؛ حيث كان للأجهزة المزروعة نصيبها من حوادث الوفاة وإصابات أخرى بسبب الأعطال الفنية في الأجهزة نفسها . فمن النصف مليون مريض الذين حصلوا على جهاز ICD مزروع خلال الفترة بين عام ١٩٩٧-٢٠٠٣ تم تسجيل ٢١٢ حالة وفاة بسبب فشل خمسة أنواع من هذه الأجهزة حسب سجلات إدارة الغذاء والدواء الفدرالية FDA في أمريكا، وأحد هذه السجلات يشير إلى حدوث تماس كهربائي في الجهاز أدى لوفاة شاب عمره (٢٢) سنة. للمزيد انظر: Sara E. Dyson, Esq.Medical Device Software & Products Liabilit: An-Overview (Part I), September 15, 2017 https://www.medtechintelligence.com/feature_article/medical-device-software-products-liability-overview-part/2/

تغيير إعدادات الأجهزة الطبية، مما يترتب عليه خلل في عملية التشخيص والعلاج للمرضى، وهناك مئات الأجهزة الطبية القابلة للتطبيقات التي تجمع بيانات المستخدمين وترسلها إلى الطبيب عبر الإنترنت أو تخزنها بالخوادم والخدمات السحابية، فماذا لو نجح الجناة في اختراقها والاستيلاء عليها لبيعها أو تشفيرها بهدف ارتكاب الابتزاز بحق المشفى أو بحق المرضى أيضاً ؟

لذلك، هناك العديد من الجرائم التي تقترف عبر الإنترنت أو شبكة الاتصالات يكون الهدف منها هو المعلومة ذاتها، ويتمثل هذا الهدف إما بالحصول على المعلومات المحفوظة أو المنقولة، أو تغييرها، أو حذفها وإلغائها نهائياً، والدافع من وراء ذلك قد يكون بقصد التنافس أو الابتزاز أو تحقيق مكاسب أو الحصول على مزايا ومكاسب اقتصادية[٤٧].

أولاً: جريمة الاعتراض أو التشويش على موجات الأجهزة الطبية

تنص المادة (٧٥) من قانون رقم ٣٧ لسنة ٢٠١٤ على إنشاء هيئة تنظيم الاتصالات وتقنية المعلومات الكويتي وجاء بمقتضاها أن: «أ - كل من قام متعمداً بأي إجراء لاعتراض موجات راديوية مخصصة للغير أو بالتشويش عليها أو بقطعها، يعاقب بالحبس مدة لا تزيد على سنتين وبغرامة لا تزيد على عشرين ألف دينار ولا تقل عن ألفي دينار أو بإحدى هاتين العقوبتين. ب - كل من قام متعمداً باستخدام موجات راديوية باستثناء الموجات الراديوية التي لا تحتاج إلى تراخيص يعاقب بالحبس مدة لا تزيد على سنة وبغرامة لا تزيد على عشرة آلاف دينار ولا تقل عن ألفي دينار أو بإحدى هاتين العقوبتين، وللمحكمة مضاعفة العقوبة إذا كان استخدام الترددات لأغراض تجارية. وفي جميع الأحوال تقضي المحكمة بمصادرة الأجهزة المستخدمة».

وكذلك، جاء بمنطوق المادة (٧٥) من قانون إنشاء هيئة تنظيم الاتصالات وتقنية المعلومات الكويتي[٤٨] النص على أن: «أ- كل من قام متعمداً بأي إجراء لاعتراض موجات راديوية مخصصة للغير أو بالتشويش عليها أو بقطعها، يعاقب بالحبس مدة

(٤٧) د. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت (دراسة مقارنة)، دار النهضة العربية، ٢٠٠٩، ص ٥٧.

(٤٨) ونجد نص المادة (٨٠) من قانون الاتصالات الأردني رقم (١٣) لسنة ١٩٩٥ وتعديلاته على أن: «كل من قام متعمداً باعتراض موجات مخصصة للغير أو بالتشويش عليها أو باستخدام موجات كهرومغناطيسية بدون ترخيص يعاقب بالحبس مدة لا تزيد على ستة أشهر أو بالغرامة لا تقل عن ٥٠ ديناراً ولا تزيد على ٢٠٠ دينار أو بكلتا العقوبتين».

لا تزيد على سنتين وبغرامة لا تزيد على عشرين ألف دينار ولا تقل عن ألفي دينار أو بإحدى هاتين العقوبتين. ب- كل من قام متعمداً باستخدام موجات راديوية باستثناء الموجات الراديوية التي لا تحتاج إلى تراخيص يعاقب بالحبس مدة لا تزيد على سنة وبغرامة لا تزيد على عشرة آلاف دينار ولا تقل عن ألفي دينار أو بإحدى هاتين العقوبتين، وللمحكمة مضاعفة العقوبة إذا كان استخدام الترددات لأغراض تجارية، وفي جميع الأحوال تقضي المحكمة بمصادرة الأجهزة المستخدمة».

وتأسيساً على ماتقدم، يقصد بالموجات اللاسلكية تلك «الموجات الكهرومغناطيسية التي تستخدم في الاتصالات اللاسلكية، تدخل جنحة اعتراض الموجات اللاسلكية بغير حق أو التشويش عليها من ضمن جرائم الضرر؛ حيث يتكون ركنها المادى من نشاط إجرامى ونتيجة ويربطهما علاقة سببية. ويشتمل السلوك الجرمي من خلال النص آنف الذكر على صورتين يقع بهما النشاط الجرمي.

الصورة الأولى: الاعتراض، ويعرف بأنه منع المسار الذي يجب أن تسير عليه الموجات اللاسلكية لنقل صوت أو صورة بين مرسل ومستقبل، وهناك من عرفه بأنه[٤٩]: «الحيلولة بين الشيء وبين بلوغ هدفه، فالاعتراض يمثل إعاقة للاتصالات يمنع وصولها إلى المرسل إليه».

وهكذا، فإن اعتراض الموجات اللاسلكية يعني قيام شخص أو أكثر أو أية جهة خاصة أو عامة بالدخول عنوة أو دون استصدارها إذناً من السلطة القضائية المختصة وفى غير الحالات المصرح بها قانوناً لحيز التردد أو مجال الموجات اللاسلكية للأجهزة الطبية الحيوية لتعطيل إرسال أو استقبال الموجات الكهرومغناطيسية المستخدمة في الاتصالات اللاسلكية الطبية؛ لتقف حائلاً بين وصول الرسالة أو الاتصالات من المرسِل (الجهاز الطبي أو الطبيب مثلاً) إلى المرسَل إليه المشترك أو المستخدم لشبكة الاتصالات (الطبيب، أو مزود الخدمة الطبية) مما يحقق ضرراً يتمثل في حجب الخدمة عن المشترك في الشبكة وعدم استفادته من خدماتها. وتصاب الشركة أو الجهة المسئولة عن خدمات الاتصالات بأضرار مادية وأدبية يتعين تعويضها عنها.

أما بالنسبة للصورة الثانية فتتمثل بالتشويش؛ حيث يعرف بأنه: «إدخال بعض

(٤٩) الدكتور/ إبراهيم حامد طنطاوى: أحكام التجريم والعقاب في قانون تنظيم الاتصالات، دار النهضة العربية، ٢٠٠٣، بند رقم ٢٥٣، ص٢٠٩..

الذبذبات على الموجة اللاسلكية يكونٍ من شأنها تشويه الصوت أو الصورة المنقولة عبر هذه الموجات»؛ ويقصد به أيضا[٥٠] «عدم نقاء الرسالة في صورتها أو وضوحها في صورتها نتيجة وجود أصوات متداخلة فيها أو ذبذبات تؤدي إلى عدم تبينها»، وللاعتراض مفهوم يختلف عن مضمون التشويش حيث يمنع ارتكاب المتهم للأول وصول الرسالة أو الاتصال، في حين لا يترتب على التشويش نفس النتيجة بل تصل الرسالة ولكن مشوهة غير واضحة.

ومما يلاحظ أن قانون مكافحة جرائم تقنية المعلومات الكويتي رقم (٦٣) لسنة ٢٠١٥ لم ينص على (التداخل) وهو فعل يختلف عن الدخول غير المشروع، ويختلف أيضاً عن الالتقاط، وهو يتعلق بمحاولة الجاني اعتراض الموجات والإشارات بقصد الإطلاع على محتواها، أو بقصد التشويش[٥١].

بينما نجد أن المجلس الأوروبي قد أوصى بضرورة إفراد نص خاص لاعتراض أنظمة المعلوماتية، يتم بموجبه تجريم كل اعتراض لاتصال يتم من أو إلى أو داخل أنظمة المعلوماتية عبر شبكات الاتصالات[٥٢]. وقد تبنت عدة تشريعات[٥٣] هذا النهج وجرمت فعل الاعتراض بنصوص خاصة، ومنها: قانون العقوبات الكندي لعام ١٩٨٥ [٥٤] في نص المادة ٣٤٢ والتي جاء بمقتضاها أن: «كل شخص يسعى باستخدام وسائط

(٥٠) الدكتور/ إبراهيم حامد طنطاوي: أحكام التجريم والعقاب في قانون تنظيم الاتصالات، مرجع سابق، ص٢٠٩.

(٥١) د. بوقرين عبدالحليم، قانون مكافحة جرائم تقنية المعلومات الكويتي (دراسة مقارنة) ، مجلة كلية القانون الكويتية العالمية ،ع٤، السنة الخامسة، العدد التسلسي٢٠- ديسمبر ٢٠١٧ ، ص٢٩٢.

(٥٢) "Unauthorised interception ; the interception made without right by technical means, of comunication to, from and within computer system or network",Russell G.Smith, Peter Grabosky, Gregor Urbas ,Cyber Criminals on Trial, Cambridge University Press,2004, p 100..

(٥٣) جرمت المادة (٨) من القانون البرتغالي رقم ١٠٩ لسنة ١٩٩١ الخاص بجرائم المعلوماتية اعتراض عمليات الاتصال التي تقوم على نقل المعلومات داخل أنظمة الحاسبات الآلية وشبكات المعلومات باستخدام وسائل تقنية، كما نصت المادة (٢) من ذات القانون على تعريف فعل الاعتراض بأنه : «كل نشاط يهدف إلى الوصول لمعلومات تتظمنها أنظمة المعالجة الآلية للمعطيات باستخدام أجهزة كهرومغناطيسية سمعية، وميكانيكية، وغيرها». انظر الموقع الإلكتروني:
https://hudoc.echr.coe.int/eng (last visited on 18 Aug. 2019).

(٥٤) انظر الموقع الإلكتروني:
Criminal Code of Canada - Laws.justice.gc.ca(last visited on 18 Aug. 2019).

مغناطيسية، صوتية، أو ميكانيكية أو أي أداة أخرى لوقف أو اعتراض أو التسبب باعتراض بصورة مباشرة أو غير مباشرة أي وظيفة لنظام المعلوماتية».

أما بالنسبة للنتيجة الإجرامية، تعد جريمة اعتراض أو التشويش على الأجهزة الطبية من جرائم الضرر فيلزم لتوافر ركنها المادى إتيان المتهم للنشاط وترتب نتيجة عليه تتمثل في عدم وصول الرسالة أو الصورة أو الاتصال (فى حالة الاعتراض)، أو وصولها مشوهة غير واضحة فى حالة التشويش، ويترتب أضراراً تلحق بالمشفى وكذا الجهاز والمرضى المستخدمين له.

وتعد جريمة أعتراض أو التشويش على الشبكة اللاسلكية الطبية من الجرائم العمدية، ويتكون ركنها المعنوي من القصد الجنائي العام بعنصرية العلم والإرادة؛ فيجب أن يعلم المتهم بأنه يقوم باعتراض موجات لاسلكية أو التشويش عليها دون سند من القانون، كما يلزم أن تتجه إرادته إلى تحقيق النتيجة المتمثلة في منع وصول الرسالة أو الاتصال في حالة الاعتراض، وتشويه الرسالة أو الاتصالات في حالة التشويش.

ثانياً : جريمة قرصنة المعلومات(٥٥)

القرصنة المعلوماتية هي عبارة عن: «نسخ البرامج على نحو غير مشروع أو الحصول دون وجه حق على معلومات مخزنة في ذاكرة الحاسوب بطريقة مباشرة أو غير مباشرة»، فإن الأمر الذي يظهر بوضوح أن هذه الأفعال الإجرامية أصبحت تشكل خطراً جدياً يهدد قطاع الرعاية الصحية؛ وكذلك، الحصول على برامج للحاسوب بطريقة غير شرعية، واستنساخها، أو الحصول على معلومات سرية حول طريقة إنشائها، يعد عملاً مجرماً قانوناً بغض النظر عن النقاشات الفقهية حول مدى اعتبارها شيئاً مادياً أو معنوياً أو خدمة(٥٦)، وفي ظل بعض ظروف الشبكة اللاسلكية

(٥٥) د. محمد شتا، الحماية الجنائية لبرامج الحاسب الآلي، ط١، دار الجامعة الجديدة للنشر، القاهرة، ٢٠٠١، ص٩١.

(٥٦) قد تظهر هذه الفكرة بسيطة، لكنها في الواقع تثير العديد من التساؤلات. فلوقوع جريمة السرقة، لابد أن يكون الشيء المسروق مملوكاً لشخص ما وأن يكون ذا طبيعة مادية. فما مدى انطباق هذه المسألة على برامج الحاسوب، للقول بوقوع جريمة السرقة عليها؟ يمكن أن نجيب -دون الدخول في تفاصيل جرائم السرقة- بأن الجدل الفقهي حول مدى اعتبار برامج الحاسوب شيئاً مادياً أو خدمة، قد توصل إلى أن "ما هو مادي في برامج الحاسوب هو دعامتها المادية، أما البرامج في =

يمكن أن يحدث خطأ في الاتصال، مما يجمد شاشة وحدة الكمبيوتر، مما يترتب عليه تأخير العلاج، وقد يؤدي ذلك إلى إصابة خطيرة أو الوفاة[٥٧] وذلك لعدم توفر الرعاية الصحية بسبب اختراق الحاسب الآلي، أو زرع فيروس بالكمبيوتر في مختبر قسطرة القلب مما يتطلب نقل المرضى إلى مسشفى مختلف.

ومن جانب آخر فإن نمو الأنظمة المتصلة بالشبكة السلكية واللاسلكية يجلب المخاطر المصاحبة لانتهاكات الأمن ألمعلوماتي والمخاوف بشأن سلامة الأجهزة الطبية وفعاليتها، على وجه الخصوص، فقضايا سلامة المرضى- الإصابات أو الوفاة -المتعلقة بالثغرات الأمنية للجهاز الطبي الشبكي هي مصدر قلق بالغ للمختصين، ويمكن أيضاً تعرض استخدام الأجهزة الطبية للخطر بسبب مهاجمة أجزاء أخرى من شبكة المؤسسة الصحية المحوسبة.

ويعد هذا النوع من الجرائم الإلكترونية أشدها خطراً وتأثيراً على قطاع الرعاية الصحية عامة، وصحة المريض خاصة، ويشمل هذا النوع من الإجرام كل أنشطة تتضمن تعديل أو محو أو سرقة أو إتلاف أو تعطيل العمل للمعلومات والبيانات الموجودة إلكترونياً، أو محاولة الدخول بطريقة غير مشروعة على أجهزة الحاسب الآلي المتصلة بشبكة الإنترنت أو غير المتصلة بشبكة المعلومات.

وعليه: فإن سياسة المشرع في مجال الجرائم الإلكترونية مثل خرق أمن الكمبيوتر أو سرقة البيانات أو إساءة استخدامها وإدخال الشيفرات الخبيثة، لن تغطي عادة التهديدات التي تلحق الأذى البدني بأي شخص، ولا أي إصابة جسدية ناتجة عن تأثير البرامج الضارة عبر اختراق الأجهزة الطبية المحوسبة.

فاستخدام الاتصالات والشبكات المعلوماتية في الولوج إلى قاعدة البيانات للمرضى، والحصول على معلومات غير مصرح بها أو إمكانية السيطرة على تلك الأجهزة الطبية المزروعة أو الملصقة على جسد المريض، والقيام بالتعديل أو محو

= ذاتها فأعمال فكرية صرفه. ولا يمكن بذلك، تصور وقوع جريمة سرقة على شيء معنوي: العمل الفكري المدمج داخل دعامته المادية". فحين وقوع عملية السرقة، فإنها تقع على دعامة البرنامج (قرص مرن، أو قرص ليزر...)، أي لا وجود لاعتداء مادي مباشر على القيم غير المادية المخزنة، مما يحذو إلى القول، بأن المعلوميات غيرت بشكل كبير مفهوم التجريم، بأن أبانت عن العديد من الجرائم.

(٥٧) FDA/CDRH Enforcement Report for Baxter Colleague Single Channel Volumetric Infusion Pumps. last visited on 8 Dec. 2018).. Available at: http://www.fda.gov/Safety/Recalls/EnforcementReports/ucm234282.htm.

أو سرقة أو إتلاف أو تعطيل عمل نظم المعلومات، فإن تلك الأنشطة ضد أجهزة الرعاية الصحية، تتم من خلال أفراد أو محترفين، والذين يقومون بهذه الأنشطة غير المشروعة بهدف الاستفادة المادية أو المعنوية من المعلومات والبيانات، أو لغاية الإضرار بمستخدمي هذه الأجهزة الطبية الحيوية.

الفرع الثاني: جريمة نشر فيروسات داخل الأجهزة الطبية المحوسبة

من أخطر التعديات على الأجهزة الطبية الحيوية، العدوى عن طريق الفيروسات والبرمجيات الخبيثة التي تتسبب في إتلاف برمجة الأجهزة الطبية، أو تدمير برامجها، أو إتلاف البيانات والأجهزة الطبية الخاصة بالمرضى(٥٨).

وجاء بمقتضى نص المادة (٢) من قانون مكافحة جرائم تقنية المعلومات الكويتي أنه: «يعاقب بالحبس مدة لا تجاوز ستة أشهر وبغرامة لا تقل عن خمسمائة دينار ولا تجاوز ألفي دينار أو بإحدى هاتين العقوبتين، كل من ارتكب دخولاً غير مشروع إلى جهاز حاسب آلي أو إلى نظامه أو إلى نظام معالجة إلكترونية للبيانات أو إلى نظام إلكتروني مؤتمت أو إلى شبكة معلوماتية.

فإذا ترتب على هذا الدخول إلغاء أو حذف أو إتلاف أو تدمير أو إفشاء أو تغيير أو إعادة نشر بيانات أو معلومات، فتكون العقوبة الحبس مدة لا تجاوز سنتين والغرامة التي لا تقل عن ألفي دينار ولا تجاوز خمسة آلاف دينار أو بإحدى هاتين العقوبتين.

فإذا كانت تلك البيانات أو المعلومات شخصية فتكون العقوبة الحبس مدة لا تجاوز ثلاث سنوات والغرامة التي لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين.

ويعاقب بالحبس مدة لا تجاوز خمس سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرين ألف دينار أو بإحدى هاتين العقوبتين، كل من ارتكب أياً من الجرائم المنصوص عليها أعلاه أو سهل ذلك للغير، وكان ذلك أثناء أو بسبب تأدية وظيفته».

(٥٨) انظر الموقع الإلكتروني:
Information révélée par Graham CLULEY, consultanten technologie chez Sophoshttp://informatique.zebulon. (last visited on 12 Dec. 2018).

ولما كان المشرع الكويتي قد نص في المادة (٢) من قانون مكافحة جرائم تقنية المعلومات على تجريم صور الولوج إلى موقع إلكتروني، أو نظام معلومات، أو وسيلة تقنية معلومات، أو نظام معلومات إلكتروني، بهدف الحذف أو الإلغاء أو الإضافة أو تدمير أو إتلاف أو إفشاء أو حجب أو تعديل أو تغيير أو نقل أو التقاط لأي بيانات أو معلومات؛ ومما يلاحظ أن الجناة قد لا يدخلون إلى البرامج والمواقع الافتراضية، وإنما يعملون على إرسال الفيروسات من خلال الشبكة الافتراضية.

ويلاحظ من خلال الفقرة الثانية من المادة (٢) آنفة الذكر أن المشرع الكويتي قد ذهب إلى تشديد العقوبة إذا نتج على فعل الدخول إلغاء أو حذف أو إتلاف أو تدمير أو إفشاء أو تغيير أو إعادة نشر بيانات أو معلومات.

بالإضافة إلى أن الولوج إلى النظام المعلوماتي قد لا يترتب عليه إلغاء أو الحذف أو التدمير أو الإفشاء أو الإتلاف أو التغيير لأي بيانات أو معلومات فقط، وإنما قد يترتب عليه تعديل في البيانات المخزنة آلياً، أو أضعاف أداء هذا النظام، وهذا ما عالجه قانون إساءة استخدام الحاسب الآلي الإنجليزي لعام ١٩٩٠ [٥٩] وقد نص بالمادة الثانية منه على تجريم الدخول غير المشروع متى توافر لدى الفاعل قصد جنائي خاص ، يتمثل في نية اقتراف جريمة أخرى لاحقة على فعل الدخول، فإلى جانب المادة الأولى التي تجرم الدخول غير المشروع ، فإن المادة الثانية جرمت الدخول غير المشروع الذي يقترن بقصد ارتكاب جريمة أخرى أو تسهيل اقتراف جريمة أخرى، وقد جاءت هذه المادة لتعالج تلك الحالات التي يرتكب فيها الدخول غير المشروع لنظام الحاسب الآلي بنية أرتكاب جريمة أخرى كالسرقة أو الابتزاز أو الاحتيال ، الا أن هذه الواقعة لم تتم[٦٠]، كما أنه لا يمكن العقاب عليها بوصف الشروع؛ نظراً لعدم إتيان الفاعل

(٥٩) للمزيد حول الموضوع انظر: د. سامي الرواشدة ود. أحمد الهياجنة، مكافحة الجريمة المعلوماتية بالتجريم والعقاب: القانون الإنجليزي نموذجاً، المجلة الأردنية في القانون والعلوم السياسية، المجلد ١د، ع ٣، ٢٠٠٩.

– د. عبد الإله النوايسة و د. ممدوح العدوان، جرائم التجسس الإلكتروني في التشريع الأردني (دراسة تحليلية)، مجلة دراسات علوم الشريعة والقانون، مجلد ٤٦، ع١، ملحق ١، ٢٠١٩، ص ٤٧١ وما بعدها.

(٦٠) Piragoof (Donald.k), computer crimes and other crimes against information in Canada ,I.R.P.L1993,VOI , P314.

عملاً يعد بدءاً بالتفيذ[٦١]، لذلك فإن هذه المادة تسد نقصاً في التشريع في مثل هذه الحالات[٦٢]، ولذا فهي تعاقب على الدخول بنية اقتراف جريمة أخرى.

وتأسيساً على ما تقدم بيانه، يتعين على المشرع الكويتي التوسع في نطاق التجريم ليتضمن إرسال أي بيانات حاسوبية تحتوي على فيروسات ضارة، أو تعديل البيانات الواردة في النظام، أو إضعاف أداء هذا النظام، فالفيروسات تعمل على إتلاف البيانات والمعلومات الموجودة على قاعدة البيانات للأجهزة الطبية، وقد تعمل على تعطيل عمل الأجهزة والإقلال من كفاءتها وسرعتها أو إصابتها بالشلل التام؛ وقد يتمكن الجناة من الولوج بسهولة إلى الأجهزة الطبية المحوسبة والعبث بالبيانات أو نقل أو محو ما هو هام منها للمريض وخاصة سجلاته الطبية.

كما وإن العديد من المراكز الطبية والمستشفيات سبق وأن تعرضت للهجمات الإلكترونية التي نفذها القراصنة في السنوات القليلة الماضية (كما بينا سابقاً)، مما أدى إلى تشفير بيانات أنظمة التشغيل الخاصة بأجهزة هذه المستشفيات، ومن ثم اقتراف جريمة الابتزاز من قبل القراصنة لدفع مبالغ مالية كبيرة لإعادة الأنظمة التشغيلية لتلك الأجهزة لحالتها السابقة، وفي بعض الحالات اضطرت بعض

(٦١) د. أيمن عبد الله فكري، الجرائم المعلوماتية: دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد، الرياض، ط١، ٢٠١٤، ص ٣٢١.

(٦٢) ومما تجدر الإشارة إليه أن المشرع الانجليزي كفل حماية البيانات من الاعتداء عليها، أو إساءة استخدامها بإصداره لقانون إساءة استخدام الحاسب الآلي لعام ١٩٩٠، فجرم من خلال المادة الأولى منه فعل الدخول غير المشروع إلى أي برنامج أو بيانات موضوعة في أي حاسب آلي، مع جعله يؤدي أية وظيفة لتحقيق الدخول، كما عاقب على أي دخول يقصد به تدبير غير مشروع ، إذا توافر للجاني العلم بعدم مشروعية الدخول، وقت تغييره لوظيفة الحاسب الآلي، أو إذا اتجهت نيته للاعتداء على تفاصيل أي برامج أو بيانات في أي حاسب آلي محدد أو غير محدد، وقد جرم في المادة الثالثة فعل الدخول إذا كانت الغاية منه تعمد تعديل محتوى أي كمبيوتر، فيعاقب على إتلاف عمل الحاسب الآلي أو إعاقة الدخول لأي برنامج أو بيانات موضوعة في أي كمبيوتر أو إتلاف عمل أي برنامج أو صحة أي بيانات، و يعاقب الجاني متى اتجهت نيته بصورة مباشرة الى أي كمبيوتر للشخص أو برنامج خاص أو بيانات من نوع خاص أو تعديل من نوع خاص، مَنْ توافرت لديه المعرفة السابقة، والمتمثلة بأي تعديل يقصده الجاني كي يتسبب بفعله غير المشروع، استناداً لنص المادة الثالثة من قانون إساءة استخدام الحاسب الآلي لعام ١٩٩٠ والتي جاء فيها على أنه يعد مرتكباً لجريمة الإتلاف المعلوماتي: «كل من يقوم بعمل من شأنه إحداث تغييرات غير مصرح بها في محتوى أي حاسب آلي متى توافر العلم والإرادة وقت قيامه بهذا الفعل». انظر الموقع الإلكتروني:
https://www.legislation.gov.uk/ukpga/1990/18/contents (last visited on 20 Aug. 2019).

المستشفيات لإلغاء عمليات جراحية بسبب برامج خبيثة تعرضت لها أنظمة تشغيل حواسيب غرف العمليات.

ووراء كل هجوم إلكتروني تقريباً كان هدفه الاستيلاء على أموال المرضى والقطاع الصحي، وبالرغم من ذلك -ونظراً لإمكانية الاتصال بمجموعة كبيرة من الأجهزة الطبية - فإن اختراق الأجهزة يمكن أن يؤدي إلى عواقب أكثر خطورة من فقدان المال؛ فماذا عن صحة الإنسان وحياته؟

نجد أن المشرع الكندي قد أضاف فقرة جديدة للمادة ٣٨٧ من قانون العقوبات لعام ١٩٨٥ [٦٣] حيث خصصها المشرع لجريمة الإتلاف المعلوماتي، وتواجه هذه الفقرة المضافة محو البيانات بطريق العمد ودون وجود مسوغ قانوني أو عذر بالآتي: إتلاف أو تشويه البيانات أو جعل البيانات بلا معنى أو بدون فائدة أو بلا تأثير أو فعالية، أو إعاقة أو مقاطعة الاستخدام المشروع للبيانات أو التدخل في هذا الاستخدام. كما أضيفت على المادة ٤٣٠ من قانون العقوبات الكندي فقرة أخرى تنص على معاقبة: «كل من يقوم بعمل أو يمتنع عن عمل متى ترتب على هذا السلوك أضرار جسيمة تتعلق بحياة الأفراد». وبعد هذا التنصيص من النصوص القليلة التي اهتمت صراحة بالآثار المترتبة على إتلاف أو إعادة النظام المعلوماتي إذا كان يتعلق بحياة الأفراد بالمستشفيات[٦٤].

وترتيباً على ما تم ذكره، فإن المعدات الطبية الذكية عرضة للاختراق، فهي معدة للحفاظ على صحة الأفراد، ولكن يمكن أن تُستخدم لأغراض معاكسة في الحقيقة، فقد سبق وأن هاجم مجرمو الإنترنت المستشفيات مراراً وتكراراً باستخدام حصان طروادة "Trojans" وغيره من البرمجيات الخبيثة الشائعة[٦٥].

---

(٦٣) انظر موقع الإلكتروني:
Criminal Code of Canada - Laws.justice.gc.ca (last visited on 18 Aug. 2019)

(٦٤) Piragoof (Donald.k), computer crimes and other crimes against information in Canada ,I.R.P.L1993,VOI , P208.

(٦٥) فعلى سبيل المثال: في السنوات الماضية، أصاب العديد من فيروسات الفدية المراكز الطبية في الولايات الأمريكية، منها «المركز الطبي بهوليوود» وفي لوس أنجلوس. وقد دفع مستشفى لوس أنجلوس مبلغاً قدره ١٧،٠٠٠ دولار مقابل استعادة تسجيلاته، ولكن عندما حاول «مستشفى كانساس للقلب» أن يفعل الشيء نفسه، رفض الجناة استرجاع الملفات بل طالبوهم في المقابل بالمزيد من المال؛ من هنا، لا يمكن الاعتماد على الواجبات الأخلاقية من أجل إيقاف المجرمين. انظر الموقع الإلكتروني: https://me.kaspersky.com/blog/vulnerable-medical-equipment/3857/

المطلب الثاني
جريمة انتهاك حق الخصوصية للمريض عبر الأجهزة الحيوية المحوسبة

تتزايد مخاطر التقنيات الحديثة على حق الخصوصية، وكثيرة هي الابتكارات التكنولوجية التي أصبحت اليوم تفيد الفرد في تنقلاته، ومن جانب أخر أضحت هذه التطورات ترصد أعماله وحركاته، وتجمع البيانات الشخصية حوله وتخزنها وتعالجها بواسطة الوسائل المعلوماتية كالسجلات الطبية، ورقابة قواعد البيانات، وهي جميعها تؤلف تهديداً مباشراً وجديداً على الحياة الخاصة [٦٦].

وتعتبر العديد من القضايا الأخلاقية والمجتمعية مرتبطة بالتقنية الحديثة، حيث يذهب البعض بالقول إن التكنولوجيا الحديثة محايدة وليس لها مخاطر على الخصوصية، بينما يذهب آخرون إلى القول بأن التطورات التقنية المعاصرة لها تأثير على حق الإنسان في خصوصيته؛ فتأثير التكنولوجيا الطبية المحوسبة على حق الخصوصية، وخاصة بارتباطها بالانترنت وتكنولوجيا النانو الحيوية، فهذه التقنيات المعاصرة لها ثلاث متناقضات من متطلبات الأمن والشفافية والخصوصية.

والكثير من الفقهاء يخشون من انتهاكات حق الخصوصية بسبب الاستخدام الواسع للتكنولوجيات غير المرئية، والتي يمكن أن تنتهك خصوصية الأفراد مع أجهزة الأستشعار عن بعد الطبية، والتي سوف تجعل كل ما لدينا وحياتنا الخاصة في متناول العامة إذا ما تم انتهاكها من قبل الجناة.

فليس هناك علاقة مطلقة بين التطور التكنولوجي وانتهاك الحقوق الشخصية للأفراد، ولكن هناك العديد من الفرص لانتهاك حق الخصوصية لأفراد المجتمع، فالجميع له الحق في الحفاظ والسيطرة على معلوماته الشخصية عامة، ومعلوماته الشخصية الحيوية والطبية خاصة؛ ولفهم الطبيعة الحديثة لانتهاكات حق الخصوصية والتي تتبع تطور تكنولوجيا الاستشعار عن بعد عامة، والتقنيات الحيوية غير المرئية خاصة.

وذلك عن طريق زرع نانو الأجهزة التي تسيطر عليها رقائق في جسم الإنسان، فبعض هذه الأجهزة يمكن أن تقدم الأدوية أو مساعدة مرضى الزهايمر الذين يعانون

(٦٦) د. أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، ط٣، دار النهضة العربية، ١٩٩٤، ص ٤٨.

من صعوبة الإدراك، وبالإضافة إلى إمكانية زرع أجهزة الاستشعار النانوية في دماغ المريض، والتي تعمل على إرسال إشارات عصبية من مناطق الدماغ، وبمساعدة هذه التقنيات الطبية سيتم تسجيل البيانات والمعلومات للمريض.

ومن خلال تقنيات الاستشعار عن بعد يمكن مراقبة المريض من الداخل من خلال زرع أجهزة طبية نانوية داخل جسم المريض، حيث أضحى بالإمكان مراقبة أجسام المرضى عن طريق التكنولوجيا الحيوية بشكل مخفي غير مرئي.

ولاريب أن كلاً من البيانات والمعلومات المستخلصة التي يتم جمعها بواسطة الأجهزة الطبية النانوية وأجهزة الاستشعار عن بعد من الأفراد، يمكن أن تؤدي إلى انتهاك خصوصيتهم بسبب سوء استخدام هذه البيانات والمعلومات والتي يتم الاستعانة بأجهزة الحاسب الآلي لحفظها وتخزينها وتحليل الكمية الهائلة منها[٦٧]؛ فهذه التكنولوجيا الحيوية الطبية مرتبطة بتكنولوجيا الاتصال والمعلوماتية، لذا تعتبر جزءاً من الحوسبة المعلوماتية، لأنها تشمل الحاسب الآلي للتعامل مع بيانات الأفراد مستخدمي الأجهزة الطبية الملصقة أو المزروعة داخل أجسادهم.

إذاً، فلابد من حماية سجلات المرضى[٦٨]، حيث إنها والمعلومات الحساسة تصبح أكثر عرضة لمخاطر الهجمات الإلكترونية التي قد تجعلها تقع في أيدي الأشخاص الخطأ[٦٩]، الذين بدورهم قد يهددون أمن المستشفى ومرافق الرعاية الصحية –كما بينا سابقاً– إذ إنه في حالة تمكن القراصنة من قفل أو تشفير السجلات الصحية للمرضى الذين هم في حاجة إلى الرعاية الصحية بشكل عاجل،

(٦٧) Wellington, K. (2013). Cyberattacks on medical devices and hospital networks: Legal gaps and regulatory solutions. Santa Clara High Technical LJ, 30, 139.

(٦٨) يعرف السجل الطبي الإلكتروني بأنه: وثيقة قانونية طبية تحتوي على معلومات إلكترونية للمريض وهو يسهل العمل لأعضاء فريق الرعاية الصحية؛ حيث تبقى هذه المعلومات سرية ويتضمن سجل المعلومات تفاصيل تعريف وتحديد المريض والمعالج، ومعلومات طبية حول العلاج الطبي الذي حصل عليه المريض، تاريخ المريض الطبي كما هو مبين في السجل، وتشخيص الوضع الحالي وتعليمات العلاج.
Norcal (2008) Mutual Insurance Company , Medical Records Management Practice Management, San Francisco, www.norcalmutual.com.

(٦٩) Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. Crime Prevention Studies, 16, 41–96.

فإن ذلك يعني بأن حياتهم معرضة لخطر[٧٠]؛ وتطبيقاً لذلك نص المشرع الاتحادي في دولة الإمارات العربية المتحدة على الجرائم المتصلة بالأجهزة الطبية المحوسبة، وذلك في المادة (٧) من قانون مكافحة جرائم تقنية المعلومات رقم (٥) لسنة ٢٠١٢ [٧١] على أنه: «يعاقب بالسجن المؤقت كل من حصل أو استحوذ أو عدَّل أو أتلف أو أفشى بغير تصريح بيانات أي مستند إلكتروني أو معلومات إلكترونية عن طريق الشبكة المعلوماتية أو موقع إلكتروني أو نظام المعلومات الإلكتروني أو وسيلة تقنية معلومات، وكانت هذه البيانات أو المعلومات تتعلق بفحوصات طبية أو تشخيص طبي، أو علاج أو رعاية طبية أو سجلات طبية».

وجاء النص على هذه الجريمة في الفقرة الثانية من المادة ٢٢٦– ١٨ من قانون العقوبات الفرنسي[٧٢] على أنه: «يعاقب كل من يقوم بجمع معلومات خفية أو بصورة غير مشروعة أو معالجة بيانات اسمية تتعلق بشخص طبيعي على الرغم من اعتراضه، وكان الاعتراض يقوم على أسباب مشروعة بالحبس لمدة خمس سنوات وغرامة ٣٠٠,٠٠٠ يورو».

يلاحظ أن الفقرة الثانية من المادة ٢٢٦-١٨ عقوبات فرنسي، قد تضمنت صوراً للركن المادي، حيث يتحقق الركن المادي للجريمة إذا تمت المعالجة الآلية

(٧٠) Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., . . . Maisel, W. H. (2008). Pacemakers and implantable cardiac defibrillators:
Software radio attacks and zero-power defenses. Paper presented at the Security and Privacy, 2008. SP 2008. IEEE Symposium on.

(٧١) وتجدر الإشارة إلى أن المشرِّع الاتحادي في دولة الإمارات قد نص في المادة (٢) من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢: (على تجريم صور الدخول إلى موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلومات، أو وسيلة تقنية معلومات، بهدف الإلغاء أو الحذف أو التدمير أو الإفشاء، أو الإتلاف أو التغيير أو النسخ أو النشر أو إعادة النشر لأيّ بيانات أو معلومات)، فإن راغبي نشر الفيروسات قد لا يدخلون إلى تلك المواقع ويكتفون بإرسال تلك الفيروسات عبرالإنترنت فقط، كما أن الدخول إلى النظام لا يترتب عليه الإلغاء أو الحذف أو التدمير أو الإفشاء أو الإتلاف أوالتغيير أو النسخ أو النشر أو إعادة النشر لأي بيانات أو معلومات فقط، وإنما قد ينجم عنه تعديل في البيانات المخزنة آلياً، أو ضعف أداء هذا النظام.

(٧٢) تم التعديل بموجب القانون رقم ٢٠٠٤–٨٠١ المؤرخ ٦ أغسطس ٢٠٠٤. انظر الموقع الإلكتروني: https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle

للبيانات لغير الأغراض الطبيّة، أو إذا لم يخطر أصحاب الشأن بحقهم في الإطلاع والتصحيح والاعتراض- و لو التزم بالغرض من المعالجة - أو قام بالمعالجة بالرغم من اعتراض صاحب الشأن وعدم وجود موافقة صريحة من الأخير، أما الركن المعنوي لهذه الجريمة فهو القصد الجنائي، أي إرادة ارتكاب الجريمة على ما عرفها القانون (م٦٣) عقوبات أردني، ويتحقق القصد الجنائي العام عندما يعلم الجاني بأركان الجريمة وعناصر هذه الأركان.

كما أورد المشرع الفرنسي في المادة (٢٢٦/ ٢٢) من قانون العقوبات الجديد لعام ١٩٩٤، تجريم كل فعل يرتكبه شخص من شأنه إفشاء بيانات شخصية، بمناسبة تسجيل أو فهرسة أو نقل أو أي شكل من إشكال معالجة البيانات الشخصية، التي يترتب على كشفها الاعتداء على حرمة حياة المريض الخاصة عبر هذه المعلومات دون تصريح بذلك من صاحب الشأن للغير الذي لا توجد له أية صفة في تلقي هذه المعلومات؛ أما إذا وقع هذا الاعتداء بطريقة الإهمال فتكون العقوبة هي الغرامة خمسين ألف يورو ولا تقام الدعوى إلا بشكوى المجني عليه».

الخاتمة

لا يسعنا في نهاية هذه الدراسة المتواضعة إلا أن نؤكد على أن الحماية الجزائية للأجهزة الطبية الحيوية المحوسبة، باتت تفرض نفسها أكثر من أي وقت مضى، وخاصة تنامي الحس الحقوقي وثقافة حقوق الإنسان عامة وحقوق المرضى خاصة.

فلقد أفرزت العقود الأخيرة ثورة من نوع آخر متعلقة بوسائل الاتصال والمعلومات، نتيجة التطور الذي تجسد أساساً في انتشار أجهزة حاسب آلي ذات مستوى عالٍ ومتطورة بشكل مستمر، وبرامج متقدمة، وشبكات اتصال قرَّبت ملايين البشر بعضهم من بعض، وأتاحت فرصاً جديدة للإطلاع على المعلومات وتبادلها، وحتى تشخيص وعلاج المرضى عبر شبكة الاتصال والإنترنت.

ويستعين الاطباء في استخدامهم للتكنولوجيا الحديثة بأجهزة وتقنيات تتجدد دوما كي تلائم أحدث المعايير التي تضعها التشريعات العالمية أو الوطنية وتسمح، ليس بإدارة وتحليل المعطيات الصحية فقط، بل بإدارة كل ما يتعلق بالقطاع الصحي: من الاستشفاء حتى الدفع والضمان ومواعيد الزيارات والإحصاءات والمؤتمرات

والتواصل مع الأطباء والمساعدة على أخذ القرار والتزويد بالمعلومات والأبحاث ونقل البيانات واسترجاعها عبر الإنترنت بشكل آمن.... إلخ، وفي هذا الكثير من الفعالية وكسب الوقت والاقتصاد في المال والجهد.

وهكذا، أدى التطور السريع لتقنيات الإعلام والاتصال وتنوع شبكات الربط بطبيعة الحال إلى توسع ميادين استعمال هذه التقنيات إن على المستوى الثقافي أو الاقتصادي أو الاجتماعي أو الطبي...الخ، فالتوسع في استعمال هذه التقنيات ترتب عليه تزايد في أرقام الإجرام المرتكب بواسطتها، وهو ما يصطلح عليه بالجرائم الإلكترونية أو الجرائم المعلوماتية[٧٣]، الأمر الذي أثر على حقوق الأفراد وحرياتهم؛ حيث وفرت الأنظمة المعلوماتية وسيلة جديدة في أيدي مجرمي المعلوماتية تسهل ارتكاب العديد من الجرائم.

ومن أهم النتائج التي خلصت اليها الدراسة:

١ - مع تزايد مستعملي الأجهزة الطبية الحيوية المحوسبة، بات من الضروري مراعاة الثغرات الأمنية في هذه الأخيرة. بالإضافة إلى ذلك، تتزايد قيمة المعلومات الطبية للمريض المنقولة عبر هذه الأجهزة أيضًا بشكل كبير، وتشمل نقاط الضعف لهذه الأجهزة من خلال الوصول إلى المعلومات الطبية الخاصة للمريض، وكذلك التلاعب بالبيانات مما قد يؤدي إلى زيادة جرعات مميتة من الأنسولين دون موافقة المريض، والتحكم عن بعد بهذه التقنيات الحيوية.

٢ - تبين لنا من خلال هذا العرض أن الطبيعة السريعة والمتطورة لتهديدات الأمن السيبراني تعني أن مدى وطبيعة التحديات الأمنية المحتملة للأجهزة الطبية الشبكية، إلى حد ما، غير معروفة. وسيتعين على هذه النظم أن تكون لديها عمليات وإجراءات تعالج التهديدات الإجرامية، وتوقع وتقييم المخاطر المحتمل أن تتعرض لها الأجهزة الطبية، التأكد من قابلية الأجهزة المنتجة للتحديث لسد أي ثغرات قد تكتشف مستقبلاً ؛ ولا بد للشركات المصنعة لهذه الأجهزة الأخذ بعين الاعتبار الجانب التقني والأمني لسلامة الأجهزة الطبية المنتجة طوال دورة

(٧٣) د. سومية عكور، الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، الملتقى العلمي، كلية العلوم الإستراتيجية، الأردن، خلال الفترة مابين ٧-٩ /١١/ ١٤٣٥هـ، الموافق ٢-٢٠١٤/٩/٤م، ص١.

حياة المنتج بأكملها، سواء كانت تلك الأجهزة ثابتة في المستشفيات، أو تلك التي يرتديها المرضى؛ ويتعين على الشركات المنتجة للأجهزة الطبية المحوسبة الانتباه لأشياء هامة منها: المراقبة الدائمة للتهديدات واستقصاء الثغرات التي قد توجد في تشفير أنظمة تشغيل الأجهزة الطبية.

٣ - تبين لنا من خلال هذه الدراسة أن قانون مكافحة جرائم تقنية المعلومات الكويتي رقم (٦٣) لسنة ٢٠١٥ لم ينص على (التداخل)، وهو فعل يختلف عن الدخول غير المشروع، ويختلف أيضاً عن الالتقاط، وهو يتعلق بمحاولة الجاني اعتراض الموجات والإشارات بقصد الاطلاع على محتواها، أو بقصد التشويش.

٤ - سعينا من خلال هذه الدراسة أن نسهم ولو بنصيب، في تفعيل نوع من الخطاب التوافقي من أجل التأسيس لقواعد تشريعية تلائم بين معادلة الحماية الجزائية للأجهزة الطبية الحيوية المحوسبة من القرصنة وتحقيق مصلحة المريض، لذلك سنعمد إلى بسط بعض التوصيات، وكلنا أمل أن تثير نوعاً من الاهتمام، وهي ما سنورده كالآتي:

- **أولاً:** لا يمكن الجزم بان الرصيد التشريعي الكويتي في هذا الصدد كاف لمكافحة كل صور الجرائم المعلوماتية، بل لابد من تكملته، بحيث يشمل جرائم أخرى لم تشملها المبادرات التشريعية الجديدة، مثل قرصنة الأجهزة الطبية الحيوية. وبما أن ظاهرة الإجرام ألمعلوماتي جديدة ومتجددة، لأن قطاع تكنولوجيات المعلوماتية والاتصالات في تطور مستمر، فهذا يعني أنه يمكن أن تظهر مستقبلاً أنواع أخرى من الجرائم المعلوماتية، مما يجعل المشرع الكويتي ملزماً بمواكبة التطورات المتلاحقة عبر سن تشريعات جديدة أو تعديل أخرى.

- **ثانياً:** يتعين إفراد نصوص جنائية خاصة بالمسؤولية الجزائية للتقنيات الطبية الحيوية المحوسبة بالنظر إلى تطور وتنامي هذه المسؤولية، بموازاة مع تصاعد وتيرة قرصنة هذه الأخيرة، فلم تغدُ الحالة هذه –القواعد والنصوص الجزائية العامة– بقوالبها الجامدة منسجمة مع واقع هذه المسؤولية ومواكبة لمستجداتها، فالمشرع مطالب بتنظيم بعض القوانين الطبية ذات الطبيعة التقنية في العلوم الحديثة كالأجهزة الطبية المزروعة أو الملصقة على جسم المريض... حتى لا يظل في

منأى عن مسايرة الركب الدولي في المجال الطبي، وحتى لا يقف القضاء عاجزاً عن مساءلة الجاني -الطبيب- عن كل فعل أو امتناع في هذا الباب، ووسيلته غياب النص المجرم «لا جريمة ولا عقوبة إلا بنص».

- **ثالثاً:** بحث إمكانية الانضمام لاتفاقية بودابست لعام ٢٠٠١ بشأن الإجرام المعلوماتي، بعد تطوير البنية التكنولوجية والأمنية والقضائية حتى يمكن تطبيق بنود هذه الاتفاقية الدولية، وضرورة أن تتضمن تشريعات مكافحة الجرائم الإلكترونية كافة صور السلوك غير المشروعة، وخاصة جرائم الاعتداء على الأجهزة الطبية الحيوية المحوسبة، والتي يستخدم فيها الإنترنت أو الشبكات اللاسلكية.
- **رابعاً:** إن تأمين الشبكات والأجهزة الطبية قد أصبح أولوية قصوى بالنسبة لقطاع الرعاية الصحية، ويتعيَّن على القطاع الصحي اليوم أكثر من أي وقت مضى ضمان سرية بيانات المرضى بنفس مستوى الرعاية الصحية المقدمة إليهم.
- **خامساً:** لا بد من التوسع في نطاق التجريم في المادة (٢) من قانون مكافحة جرائم تقنية المعلومات الكويتي ليتضمن النص إرسال أي بيانات حاسوبية تحوي فيروسات ضارة، أو تعديل البيانات الواردة في النظـــام، أو إضعـــاف أداء هذا النظام.

المراجع:

أولاً: المراجع العربية.

- د. أسامة عبد الله قايد، الحماية الجزائية للحياة الخاصة وبنوك المعلومات، ط٣، دار النهضة العربية، ١٩٩٤.
- د. أيمن عبد الله فكري، الجرائم المعلوماتية: دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد، الرياض، ط١، ٢٠١٤، ص ٣٢١.
- د. بوقرين عبد الحليم، قانون مكافحة جرائم تقنية المعلومات الكويتي (دراسة مقارنة)، مجلة كلية القانون الكويتية العالمية، ع٤، السنة الخامسة، العدد التسلسلي ٢٠- ديسمبر ٢٠١٧.
- د. جاسم محمد العنتلي، الجريمة والتكنولوجيا الحديثة (دراسة مقارنة)، مجلة العلوم الشرطية والقانونية، المجلد السادس، العدد الأول، يناير، ٢٠١٥.

- د. حسين بن سعيد الغافري، السياسة الجزائية في مواجهة جرائم الإنترنت (دراسة مقارنة)، دار النهضة العربية، ٢٠٠٩.
- د. عبد الإله النوايسة و د. ممدوح العدوان ، جرائم التجسس الإلكتروني في التشريع الأردني (دراسة تحليلية)، مجلة دراسات علوم الشريعة والقانون، مجلد ٤٦، ع١، ملحق ١، ٢٠١٩ .
- د. سامي الرواشدة ود. أحمد الهياجنة، مكافحة الجريمة المعلوماتية بالتجريم والعقاب: القانون الإنجليزي نموذجاً، المجلة الأردنية في القانون والعلوم السياسية، المجل د١، ع ٣، ٢٠٠٩.
- د. سوميه عكور، الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، الملتقى العلمي، كلية العلوم الاستراتيجية، الأردن، خلال الفترة ما بين ٧-٩ /١١/ ١٤٣٥هـ، الموافق ٢-٤/٩/٢٠١٤م.
- د. محمد سعيد غزال، قرصنة الأجهزة الطبية الملصقة والمزروعة بالمرضى، المجلة العربية الدولية للمعلوماتية، المجلد الخامس، العدد ٩، ٢٠١٧.
- د. محمد شتا، الحماية الجزائية لبرامج الحاسب الآلي، ط١، دار الجامعة الجديدة للنشر، القاهرة، ٢٠٠١، ص٩١.
- د. منى جبور ود. عزيز بربر، أمن الشبكات والإنترنت، الحلقة العلمية (الإنترنت والإرهاب) والمنعقد خلال الفترة من ١٧-٢١ /١١/١٤٢٩هـ، الموافق ١٩-١١- ٢٠٠٨.

القوانين والأنظمة:

- قانون مكافحة جرائم تقنية المعلومات الكويتي رقم (٦٣) لعام ٢٠١٥.
- قانون رقم ٣٧ لسنة ٢٠١٤ بإنشاء هيئة تنظيم الاتصالات وتقنية المعلومات الكويتي.
- قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم (٥) لسنة ٢٠١٢.
- قانون الاتصالات الأردني رقم (١٣) لسنة ١٩٩٥ وتعديلاته
- مرسوم بقانون اتحادي لدولة الإمارات العربية المتحدة رقم (٣) لسنة ٢٠٠٣ في شأن تنظيم قطاع الاتصالات.

المرجع الاجنبية:

- BioTel. (2018). wEvent: Event monitoring. Retrieved from https://www.myheartmonitor.com/device/wevent/.
- Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. Crime Prevention Studies, 16, 41–96.
- Dario. (2018). Dario blood glucose monitoring system. Retrieved from https://mydario.com/.
- Defend, B., Morgan, W., . . . Maisel, W. H. (2008). Pacemakers and implantable cardiac defibrillators:
- Dimitrov, D. V. (2016). Medical internet of things and bigdata in ealthcare. Healthcare Informatics Research,22(3),156–163. doi:10.4258/hir.2016.22.3.156
- FDA/CDRH Enforcement Report for Baxter Colleague Single Channel Volumetric Infusion Pumps. 2012. Available at: http://www.fda.gov/Safety/Recalls/EnforcementReports/ucm234282.htm
- Filkins, B. (2014). Health care cyberthreat report: Widespread compromises detected, compliance nightmare on horizon. Retrieved from https://www.sans.org/reading-oom/whitepapers/analyst/healthcare-cyberthreat-report-widespread-compromises.
- Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of things (IoT): A vision, architecturaltracking system on wrist devices. Paper presented at the Wireless Health.
- Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S.,
- Software radio attacks and zero-power defenses. Paper presented at the Security and Privacy, 2008. SP 2008. IEEE Symposium on.
- Hashmi, N., Myung, D., Gaynor, M., & Moulton, S. (2005). A sensor-based, web service-enabled, emergency medical response sys-

tem. Paper presented at the Proceedings of the 2005 workshop on End-to-end, sense-and respond systems, applications and services.

- Halperin D, Heydt-Benjamin TS, Ransford B, et al. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses; Paper presented at: Security and Privacy, 2008. SP 2008.IEEE Symposium; Oakland, California, USA. May 18–22, 2008.
- HIPAA-Report2003. Summary of HIPAA Health Insurance Probabilityand Accountability Act. US Department of Health and Human Service,May 2003.
- Jonson JA,FDA Regulation of medical deviecesCnogressional research service, June 25, 2018,Available form: http://www.fas.org/sgp/misc.
- MaiselWH, Kohno T. Improving the security and privacy of implantable medical devices. N Engl J Med. 2010; 362:1164–1166.
- Maisel WH. Medical device regulation: an introduction for the practicing physician. Ann Intern Med. 2004;140:296–302.
- Marr, B. (2018). Why the internet of medical things (iomt) will start to transform healthcare in 2018. Retrieved from
- Medtronic. (2018). MYCARELINK SMART™U.S. Retrieved from http://www.medtronic.com/us-en/mobileapps/patient-caregiver/mycarelink-smart-us.html
- Norcal (2008) Mutual Insurance Company , Medical Records Management Practice Management, San Francisco, www.norcalmutual.com
- SANS Institute. Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon.
- Safe Medical Devices Act.http://www.fda.gov/cdrh/devadvice/312.html

- Tatham, M. (2018). Identity theft statistics. Retrieved from https://www.experian.com/blogs/ask-experian/identity-theft-statistics/
- US Food Drug Administration.Content of Premarket Submissions for Management of Cybersecurity in Medical Devices.US Food and Drug Administration; 2014. Available from: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf.
- Wellington, K. (2013). Cyberattacks on medical devices and hospital networks: Legal gaps and regulatory solutions. Santa Clara High Technical LJ, 30, 139.
- Zoll PM. Resuscitation of the heart inventricular standstill by external electric stimulation ,Neug1 J MED.
- Décret n° 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le code de la santé publique (dispositions réglementaires).
- "dans la plupart des domaines ayant un lieu avec le commerce électronique, l'union européenne est en retard sur les U.S.A..dans le domaine de la protection de la vie privée,elle a des kilomètres d' avance", Théo Hassler, Les Données personnelles et la protection des personnes, Les premières journées internationales de droit de commerce électronique, p114.
- Loi informatique et libertés codifiée par la loi nº2004-801 du 6 aout 2004 pour l'harmonization avec la directive européenne
- Marie -pierre, fenoll-trousseau ,gerardhaas , Internet et protection des donnés personnelles ,litec ,paris 2000, P 27.
- Code de la Santé Publique, dernière modification : 1 juillet 201429

- مواقع الإنترنت

- htt://blog.bit9.com-
- htt://www.accemagazine.com/article.php?
- https://www.smartflowcompliance.com/smartflow-anti-piracy-conference Information révélée par Graham CLULEY, consultant en technologie chez Sophoshttp://informatique.zebulon.
- https://www.forbes.com/sites/bernardmarr/2018/06/25/why-the-internet-of-medical-thingsiomt-will-start-to-transform-healthcare-in-2018/#3ed660424a3c
- Norcal (2008) Mutual Insurance Company , Medical Records Management Practice Management, San Francisco, www.norcalmutual.com

Criminal Protection of Digital Biomedical Devices in the Light of the Kuwaiti Combating Information Technology Crimes Law

Dr. Omar Musbih*

Abstract:

Objectives: This study aims to discuss the subject through the piracy acts directed to biomedical devices, in an attempt to show some forms of crimes related to medical devices that have been planted in patients' bodies. "Microbiological techniques". **Methodology**: this study is based on a comparative critical analytical approach. **Results**: The most important results of the study can be summarized as follows: 1- The increase of the patient's medical information transmitted through digital medical devices increases the possibility of access to the patient's private medical information, and the possibility of manipulation. 2: because of the nature of advanced cyber threats, regulations concerned should include certain procedures able to face such criminal threats. 3. The Kuwaiti law of combating information technology crimes did not adopt the term (overlapping) which is different from the acts of (illegal entry) and (capturing). **Recommendations**: The need to include criminal provisions on criminal responsibility in the Kuwaiti law of combating information technology crimes. This is in view of the development and growth of this responsibility to be in parallel with the escalation of the piracy of information technology, in addition to the view that the existing general rules of criminal responsibility are no longer in their rigid forms able to face the new threats.

* College of Law, Sultan Qaboos University - Oman.
Email: Musbih2003@yahoo.com

- Submitted: 29/12/2018, Accepted: 27/10/2019.

To Cite P. 349

الدكتور عمر عبد المجيد مصبح، حاصل على الدكتوراه في القانون الجنائي، كلية الحقوق بجامعة عين شمس، جمهورية مصر العربية، عام ٢٠١٠، يعمل حالياً بكلية الحقوق - جامعة السلطان قابوس - سلطنة عمان. الاهتمامات البحثية: الأدلة الجنائية المستحدثة، القانون الجنائي والعصر الرقمي، تقنية النانو والقانون الجنائي، القانون الجنائي للأعمال.

الإيميل: Musbih2003@yahoo.com

للاستشهاد:

مصبح، عمر. (٢٠٢٣). الحماية الجزائية للأجهزة الطبية الحيوية المحوسبة في ضوء قانون مكافحة جرائم تقنية المعلومات الكويتي. *مجلة الحقوق*، *٤٧*(٤)، ٣٠٧ - ٣٤٩.

To Cite:

Musbih, Omer.(2023). Criminal Protection Digital Biomedical Devices in the Light of the Kuwaiti Combating Information Technology Crimes Law. *Journal of Law, 47*(4), 307 - 349.

JOURNAL OF LAW

A Refereed Academic Quarterly, Published by the Academic Publication Council - University of Kuwait

Criminal Protection of Digital Biomedical Devices in the Light of the Kuwaiti Combating Information Technology Crimes Law.

Dr. Omar Musbih

جامعة الكويت
KUWAIT UNIVERSITY

ISSN: 1029 - 6069

No. 4 - Vol. 47

Jamada II 1445 - December 2023