# الجوانب الفنية والإجرائية اللازمة لتفعيل تطبيق قانون مكافحة جرائم تقنية المعلومات الكويتي رقم 63 لسنة 2015

د. فيصل فراج المطيري*

## الملخص:

يتناول هذا البحث بالدراسة والتحليل الجوانب الفنية والإجرائية لتفعيل تطبيق قانون مكافحة جرائم تقنية المعلومات الكويتي رقم 63 لسنة 2015، والذي جاء ليسد فراغاً تشريعياً، صنع نوعاً من الاضطراب والإرباك لدى القضاء ورجال تنفيذ القانون على حد سواء. وقد أكدت ذلك المذكرة التفسيرية للقانون التي أشارت إلى أن الاستخدام المتزايد للشبكات والأنشطة المعلوماتية أدى إلى كثير من المخاطر، إذ أفرز أنواعاً جديدة من الجرائم يطلق عليها «الجرائم المعلوماتية» كجرائم الاختلاس والتزوير والجرائم الماسة بالأخلاق والآداب وسرقة المعلومات واختراق النظم السرية.

وإذا كان من المؤكد أن القانون الإجرائي هو الذي ينقل القواعد الموضوعية لمكافحة الجرائم من حالة السكون إلى حالة الحركة وهي مرحلة التطبيق الفعلي أو التنفيذ العملي، فإن النصوص الإجرائية الجزائية التقليدية، متمثلة في قانون الإجراءات والمحاكمات الجزائية الكويتي رقم 17 لسنة 1960، لا تسعف لمواجهة الجرائم المستحدثة التي يتم ارتكابها باستخدام وسائل التقنية المتطورة، الأمر الذي يقتضي ضرورة مراجعة وتطوير هذه القواعد الإجرائية.

وفي ضوء ذلك فإن أهمية هذه الدراسة تكمن في السعي إلى وضع قواعد إجرائية خاصة تحاكي الواقع الافتراضي للجرائم الإلكترونية بعيداً عن القواعد التقليدية. ولذا فقد كان الهدف من هذه الدراسة هو تسليط الضوء على أن رجال الضبط القضائي والنيابة العامة والمحاكم يواجهون هذه الحرب الإلكترونية بأسلحة إجرائية تقليدية لا تنسجم مع الواقع الافتراضي.

وفي سبيل ذلك، فقد اتبعت الدراسة المنهج التحليلي المقارن بهدف معرفة النماذج الفنية والتجارب التي طرحتها بعض الدول مثل فلندا وسويسرا كنماذج يمكن النسج على منوالها والاستفادة من تجاربها.

* أستاذ القانون الجنائي المساعد، أكاديمية سعد العبدالله للعلوم الأمنية، الكويت.

وقد خلصت الدراسة إلى عدد من النتائج من بينها ضرورة اهتمام المشرِّع بتكامل النواحي الموضوعية مع النواحي الإجرائية، كما انتهت إلى عدد من التوصيات من أهمها إنشاء محكمة مختصة بالجرائم الإلكترونية.

**كلمات دالة:** نظام الحاسب الآلي، جريمة إلكترونية، تفتيش إلكتروني، مختبر جنائي إلكتروني، دليل إلكتروني.

## المقدمة:

عندما ينغمس الفرد في مزالق الواقع الافتراضي، فيتنقل بين جوانبه ليتلمس النعم والنقم، ويتجول بين صفحاته لينتقل إما إلى نقلة نوعية حضارية وإما إلى نقلة إلى الْهَاوِيَةُ وما أدراك ماهي؟. إن الأمر يتعلق بعوالم فوضوية لا تحكمها إدارة مركزية مهيمنة، فقد تَهْتِكُ السُّتر وتنحرف الأفكار، فتتجافي القيم الدينية، والأخلاقية، والعلمية، وتنصهر الحدود الفاصلة بين الأيديولوجيات التي تخاطب وجدان الإنسان، فينجرف إلى ما يسلبه إرادته أو يبعده عن هويته، وقد تُدمر شخصيته، فيبتعد عن الإبداع ويصير مهزوماً منفلتاً تتقاذفه أمواج الخنوع واليأس والقنوط ليقاسي ويلات الخليط العقائدي المشوه الذي تتصاعد وتيرته لممارسة التشدد أو التحلل ليجد نفسه أمام تركيبات فكرية متناقضة نسيجها الوصائية أو اليقظة المثالية أو السلبية الممزوجة بالتذمر والإهمال[1].

فبعض الأفراد يجهل معاني الخصوصية فلا يدرك خطورة ما يدلى به للشخصيات المجهولة فتغمره نشوة التطلع والفضول فيطرق المجهول، وقد لا يقدر عواقب الأمور[2]. فواقعية التجريم التي انتهجها المشرِّع لمكافحة جرائم تقنية المعلومات بمقتضى القانون رقم 63 لسنة 2015 تجاهلت خلق قواعد إجرائية خاصة تكافح الجريمة الافتراضية، وبالتالي فقد تم تحديث القواعد الموضوعية، ومكافحة الجرائم المستحدثة من دون تحديث للقواعد الإجرائية، وهو ما تركها للقواعد العامة التقليدية التي لا تنسجم مع الواقع الافتراضي.

لقد تبنى القانون سالف الذكر القواعد الموضوعية فيما يتعلق بالجرائم والعقوبات، وهي نصوص موضوعية مجردة تحدد الجريمة والعقوبة المقابلة لها، فيما ترك هذه القواعد الموضوعية المستحدثة خاضعة للقواعد الإجرائية التقليدية ممثلة في قانون الإجراءات والمحاكمات الجزائية رقم 17 لسنة 1960. وهنا تُطرح عدة تساؤلات من بينها: هل يمكن استجلاء قواعد إجرائية خاصة لكشف هذه الجرائم؟ خصوصاً فيما يتعلق بالمرحلة التمهيدية، وهي مرحلة التحريات وجمع الاستدلالات، والتي تتطلب إجراءات خاصة تختلف تماماً عن الإجراءات التقليدية لضبط الجناة، وذلك عن طريق أو بواسطة حيل

(1) د. على أسعد وطفة، الطفولة العربية والصراع على المصير في استراتيجية البناء الثقافي للطفل العربي، مجلة شؤون عربية، القاهرة، العدد 119، لسنة 2004، ص 79. د. محمد صديق محمد، الفضائيات والإنترنت مسؤولية مشتركة تجاه أطفالنا وشبابنا، مجلة التربية، الدوحة، السنة 37، العدد 164، مارس 2008، ص 49 وما بعدها.

(2) د. بدر عمر العمر، الإنترنت التربوي: ماذا يجب على الطفل معرفته، مجلة الطفولة العربية، الكويت، المجلد 3، العدد 12، السنة 2002، ص 122. د.علاء الدين يوسف العمري، المراهق والإنترنت: الفوائد والمخاطر، مجلة رسالة التربية، سلطنة عمان، العدد 6، ديسمبر 2004، ص 80 وما بعدها.

مشروعة وسلطات وصلاحيات تكتسبها الفئات المنوط بها كشف هذه الجرائم من خلال الولوج إلى أجهزة الحاسب الآلي، وهل يمكن استخلاص خصوصية أخرى أكثر عمقاً لحماية الأفراد من براثن العقل الإلكتروني المدمر؟، وذلك تحت مظلة واسعة للحماية تستوعب وضع عمليات الرصد والمتابعة، من خلال برامج إلكترونية دفاعية وهجومية مقننة تتيح طرق التعامل مع هذه الجرائم وضبط المجرمين بكل موضوعية ومهنية، مع الموازنة بين حقوق وحريات الأفراد وبين حق الدولة في العقاب وتغليب الجانب الأجدر بالرعاية والاهتمام حتى لا تدب الفوضى بالمجتمع ويعم الاضطراب في أرجائه، الأمر الذي يوثر في النهاية على وجود هذه الحقوق والحريات ذاتها[3]، وهو ما يقتضي وجود جوانب إجرائية خاصة تُمنح لرجال الشرطة في المرحلة التمهيدية عن طريق حيل إجرائية مشروعة. كما تنسحب هذه الجوانب الإجرائية إلى مرحلة التحقيق الابتدائي ومرحلة المحاكمة التي تتطلب إجراءات فنية أكثر تخصصاً وعمقاً.

**أولاً- الأهميـــة:**

تكمن أهمية هذا الموضوع الذي نحن بصدد بحثه في التالي:

1- إن من شأن وجود علاقة بين علم الاجتماع والعلوم القانونية المساعدة في وضع تصور نموذجي لمكافحة الإجرام الإلكتروني المرتبط بالأفراد نتيجة للتغيرات الرقمية والعولمة المستمرة وتداعياتها.

2- من المهم وجود فلسفة عامة للمعالجة الإجرائية الإلكترونية الفعالة من خلال وسائل الكشف الدفاعية والهجومية عن المجرمين وتبيان حالات انطباق هذا القانون وأغراضه وشروطه وضماناته وإجراءاته وهيئاته وخطوات استجلاء الدليل الفني والمادي في الواقع الافتراضي وحل مشاكل تنازع الاختصاص وأسس التعاون الدولي وعقوباته في حال الإخلال بأحكامه.

**ثانياً- الأهـــداف:**

إن الوصول لمسارات متنوعة واكتشاف الحلقات المفقودة في القوانين التي تكافح الإجرام الإلكتروني وتسعى لإيجاد شبكة حماية تكاملية بين النصوص والبيئة التي تطبق فيها، تستوجب تحقيق الأهداف التالية:

1- تهيئة البيئة المحلية لاستقبال النظم والبرامج والتقنيات التكنولوجية لكشف الجرائم الإلكترونية التي يتم ارتكابها ضد الأفراد وسبل التغيير في موجبات القواعد

(3) Russell G. Smith & Ray Chak-Chung Cheung & Laurie Yiu-Chung Lau: Cybercrime Risks and Responses: Eastern and Western Perspectives, Palgrave Macmillan in the UK is an imprint of Macmillan Publishers Limited, 2015, p.65.

بوضعها الراهن لتتلاءم مع مستحدثات العصر الرقمي ووسائل تفعيل النصوص وفض الإشكاليات التي تنشأ عن التطبيق حال وجوده من خلال مشروع قانون شامل كآلية متكاملة.

2- تحقيق العديد من الضمانات القانونية الإجرائية التي تراعي شرعية الدليل المستمد من الجريمة الإلكترونية، وتحديد هوية الأشخاص المتورطين فيها، في ظل تحقيق الموازنة مع الحقوق والحريات من النواحى القانونية والاجتماعية والأمنية والسياسية، من أجل توفير بيئة إلكترونية يتم ترويضها وتكييف الفرد ليتعامل معها بأمان. كما يتعين ترتيب هذه الضمانات مروراً بالاستحواذ والتحليل حتى التوثيق الفني للدليل ليكون أكثر فعالية[4].

**ثالثاً- خطة الدراسة:**

وعلى ضوء ذلك، فقد تم تقسيم هذا البحث إلى ثلاثة مباحث على النحو التالي:

المبحث الأول: مضمون الحيل الإجرائية المشروعة.

المبحث الثانى: محاولة تأصيلية لصياغة قواعد إجرائية إلكترونية.

المبحث الثالث: تهيئة البيئة المحلية لاستيعاب الجوانب الإجرائية الإلكترونية.

(4) د. عبدالرحمن محمد خليل أزهري، جمع وتوثيق وتحليل الأدلة الجنائية الرقمية بطرق أكثر فعالية، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية (ICACC)، كلية علوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية، الرياض، 2015، ص89.

# المبحث الأول
# مضمون الحيل الإجرائيـة المشروعـة

تقتضي معرفة الجانب الفني والإجرائي التطرق إلى الجانب الأكثر أهمية، وهي السلطة الممنوحة لرجال الضبط القضائي للكشف عن هذه الجرائم بطرق مستحدثة تتناغم مع واقعية التجريم الإلكتروني من خلال حيل إلكترونية مشروعة، وسوف نتناولها من خلال المطالب التالية:

## المطلب الأول
## ماهية الحيل الإجرائيـة المشروعـة

إن الحيل الإجرائية المشروعة هي عبارة عن: "مجموعة من الخطوات المترابطة والأدوات التي تهدف لمواكبة الإجرام الحديث وعلى وجه الخصوص لنوعية جرائم الحاسب الآلي لتتلافى بطء الإجراءات الجزائية في صورتها التقليدية"(5)، فهي بمثابة: "أسلحة إجرائية تكتيكية يتعين على السلطة المختصة بكشف الجرائم الإلكترونية منحها للقائم بضبط وإحضار ومعاينة وتفتيش محل الفعل المُجرَّم لتشمل حيلاً دفاعية هدفها المنع وأخرى هجومية هدفها المواجهة والكشف"(6). كما تتمثل هذه الحيل في صلاحيات وإمكانيات ضرورية لإظهار المكنونات الخفية داخل الجسم الإلكتروني المعقد المتشابك وتسهيل الخروج من الثغرات الوعرة من أجل استنباط الدليل الجنائي وسرعة التصرف الحكيم والحذق والمهارة في التحفظ على مادياته دون العبث بمفرداته. كما تهدف هذه الحيل إلى ابتكار أساليب جديدة لتحديد الأشخاص المتورطين في استغلال الأفراد وتقديمهم للعدالة. كما لا تهدف هذه الحيل المشروعة مطلقاً إلى خلق جريمة أو إنشاء حالة وهمية احتيالية تَتَصَيَّد أفعال الناس أو تهتك سترهم تمهيداً للإيقاع بهم في معاناة العقوبة وإيجاد حالة تنذر بخطر دون أن تكون مبنية على أساس واقعي.

(5) يقصد بالحيلة في اللغة: الحذق وجودة النظر والقدرة على التصرف في الأمور، فيقال عن شخص أنه واسع الحيلة أي بارع في الخروج من معضلاته ومشكلاته لسبب أنه عميق وحكيم في تدبر أموره، والعكس أن الرجل قد فقد كل حيلة أي احتار فيما يفعل لعجزه وعدم إمكانيته أو استطاعته الخروج من المأزق الملازم له. وقال تعالى في سورة النساء الآية 98: ﴿لَا يَسْتَطِيعُونَ حِيلَةً وَلَا يَهْتَدُونَ سَبِيلًا﴾ أي استنفذوا كل الوسائل والإمكانيات للوصول إلى هدفهم فلم يصلوا إليه. كما قد تستعمل كلمة حيلة في معاني المكر والخداع والدهاء يقال أحذر حيل الأعداء فكيدهم يأتي من كل حدب وصوب. كما قد تستعمل الحيلة في امتلاك الحبكة وتفادي الخديعة والمكيدة وهو المعنى الذي نرمي له. راجع: المعجم الوسيط، ط4، مجمع اللغة العربية، الإدارة العامة للمعجمات وإحياء التراث، 2004، باب الحيطة، ص 212.

(6) Wayne Graham, Beginning Facebook Game Apps Development: creat the next generation of facebook game and social media apps using html5 and java script, A press and friends of ED books, 2012, p.201.

إن هذه الحيل المشروعة قد تتنوع صورها وأنماطها، فتشمل برامج غاية في التقنية المتطورة ولها من الحداثة ما يجابه المحاذير الإجرامية وقد تتمثل في صلاحيات وإجراءات تقدمية وفنية، ونعرض ذلك من خلال الفروع التالية:

## الفرع الأول

## الحيل الإجرائية المشروعة كبرامج تقنية

وهي تهدف إلى استعمال البيانات وترجمتها في معلومات تتولاها أجهزة وبرامج غاية في الحداثة تتبع مصدر الخطر المعلوماتي ضد الأفراد، وتخترق مصدره لفك شفراته ومعضلاته الحصينة، وقد تعمل هذه البرامج على شرائح وشبكات مركزية تكون حائط صد دفاعي أو أجهزة لا مركزية للمراقبة تتحرك هجومياً عندما يتطابق النموذج الإجرامي مع التصور المعلوماتي للخطر المنبعث أو الضرر الذي يعرقل فكر وعقل ووجدان الفرد، وهناك برامج عالية الجودة تُطبَّق في بعض الدول لمتابعة مصدر الخطر ومعرفة الجناة، وسوف نتطرق بإيجاز إلى النموذجين الفلندي والسويسري في هذا الشأن:

**أولاً– النموذج الفنلندي** (The virus cinch connector)**:**

ونعرض لهذا النموذج من خلال استعراض الجوانب التالية:

**- آليات عمل الفايروس:**

ينتدب مجلس حماية البيانات الخبراء المتخصصين طبقاً للمادة (38) من القانون 523 لسنة 1999 بشأن البيانات الشخصية – ليضع تقنية أخرى تتكامل مع الفايروس هي تقنية (RFID)، وهذه التقنية تُعد قائدة أجهزة التتبع tracking system . فمن خلالها يتم تلقي الإشارات والترددات اللاسلكية التي تفيد في ترجمة المحتوى الإلكتروني ونطاقه وملحقاته، بل يمكن أن تعمل هذه التقنية على شرائح ذكية يمكن استخلاص الدلائل بواسطتها، فهي عبارة عن موجات لاسلكية تتعرف أوتوماتيكياً على مصدر الخطر فتتبعه من خلال أوعية ملحقة بهوائي ومجمعة وموحدة تنقل إشارات وخادماً مقترناً لفك الشفرات. ومن هنا يمكن القول أن الفايروس (cinch) يغل يد الجاني عن جريمته الإلكترونية، ثم تأتي تقنية (RFID) لتمثل الجانب التنفيذي والتفتيشي والاستخلاصي عن الدليل في حيز فضائي وعن بعد بحيث تتلافى عجز الضبط والمعاينة والتفتيش التقليدي طبقاً لقواعد الإجراءات العادية. كما يمكن استرجاع المعلومات والبيانات وتحليلها وتوثيقها حتى تتوازن مع شرعية الدليل وتتباعد عن محاولات الطمس والإتلاف من الجاني أو من رجال الضبط غير المؤهلين لاحتواء الدليل الفني. كما يمكن

الاعتماد على هذه الخاصية في مكافحة سوء استعمال الهواتف النقالة وتعزيز جودتها وتحصين البيانات من الاختراق طبقاً للقانون رقم (13لسنة 2003) بشأن رقابة الخدمات الإلكترونية [7].

**- كيفية التعامل مع البيانات الحساسة:**

أوجب قانون حماية البيانات رقم 523 لسنة 1999 على المدعي العام إشرافه على استخدام التقنيات في البحث عن جرائم إلكترونية ونص في المادة (9) على مبادىء يلتزم بها، فمنها الدقة والتجهيز والتحوط والخصوصية، كما عليه أن يثبت محتويات الملف وطبيعته واسمه وعنوانه ومحتواه طبقاً للمادة (10) وماهي البيانات التي يتم التحصل عليها من الفايروس أو تقنية (RFID) ويتم تدميرها على الفور أو العكس الاحتفاظ بها في أرشفة تراثية ترعاها السلطات. كما يجب طبقاً للمادة (43) أن يراعي حرمة المنازل وحظر التفتيش في محال أخرى غير المحددة في نطاق الإذن من مجلس إدارة وحماية البيانات مع تفعيل قواعد التشغيل ومعايير البحث والتقصي والتحري عن الدلائل.

**ثانياً- النموذج السويسري (Semantic Web):**

**- دلالات خاصية الويب:**

عبارة عن منهجية تتعامل مع المعلومات والبيانات في بيئة معرفية منظمة من خلال مسارين: أولهما، يجعل أدوات جمع وتصنيف وفهرسة واسترجاع ومعالجة البيانات والمعلومات تتم في نطاق بحثي وتفتيشي وفحصي يستند إلى ما تحمله من دلالات ومعان وليس على ما تحتويه من أحرف وألفاظ وكلمات كما هو الوضع الآن، وثانيهما، ترجمة المعلومات داخل أدوات التطبيقات والمتصفحات ببرمجيات مقترنة بإدارة بيانات عالمية تنفتح بلا حواجز لتنقل المعلومات ويتم عرضها على أي جهاز حاسوب مركزي مرصود لكشف الجرائم ضد الأشخاص والأموال. كما أنه يُمثِّل ثورة عالمية في معالجة البيانات فهو عبارة عن نصوص تشعبية صممت ليقرأها ويفهمها البشر لتتم عملية التحليل الاستنتاجي المستقبلي مما يجعل منها نسيجاً متكاملاً وتنسيقاً عالمياً مشتركاً لكشف خفايا وهويات محترفي الإجرام الإلكتروني [8].

(7) Act on Electronic Services and Communication in the Public Sector, 13/2003, Ministry of Justice, Finland.

(8) Liyang Yu: ( A Developer's Guide to the Semantic Web ) - Springer-Verlag Berlin Heidelberg 2011 – p.no 138. & Michael Schumacher and Heikki Helin: ( CASCOM: Intelligent Service Coordination in the Semantic Web ) – Birkhäuser – Berlin – 2008 – p.no 71. & John Domingue, Dieter Fensel: ( Handbook of semantic web technologies ) Vol (1) – Austria – 2011 – p.365.

- مؤشرات نجاحه:

عملت سويسرا على تطويره نظراً للإنجازات التي حققها في كشف الأرقام المجهولة في إحصائيات الجرائم، فأدخلت عليه إضافات جوهرية منها محرك استدلالي فرعي بداخله مدعوم بخرائط المفاهيم المعروفة بالأنطولوجيا ونظام مخطط العلاقات التنسيقية ما بين المعلومات كمدخلات والبيانات كمخرجات. ولمواكبة الطبيعة الديناميكية لحركة وتطور الإجرام في المجتمع، أصدرت قانوناً يوضح مضمون هذه الخاصية وكيف يمكن أن يتقارب من الأنظمة الشبيهة؟ وما هي آثاره ودلالاته في الإثبات الجنائي ومعايير نجاحه وأغراضه ومسؤوليات القائمين على استخدامه حال الإخلال ببنوده [9].

## الفرع الثاني

## الحيل الإجرائية كصلاحيات لرجال الضبط القضائي

تتمثل هذه الحيل الإجرائية الإلكترونية في الخطوات الفنية التي يمتلكها القائم بتحديد هوية الجاني، والتي يهدف من خلالها إلى استجلاء الدليل المادي من الحاسوب، وقد تشمل ترتيبات كشفية وتنقيبية وأدوات كمقومات لتحقيق الأمن المعلوماتي بهدف الخروج على تقليدية القواعد العامة الممنوحة لرجل الضبط القضائي في قانون رقم 17 لسنة 1960 بشأن قانون الإجراءات والمحاكمات الجزائية الكويتي الراسخة التي لا تتواكب مع مستجدات هذه الجرائم المستحدثة، فتتم مباغتة ومحاصرة المجرم المعلوماتي بمرونة في التعامل مع حيطته وذكائه، فالإجرام الذكي لابد وأن يواجه بصلاحيات ذكية طبقاً لقواعد إجرائية حديثة.

## المطلب الثاني

## أهمية الاستعانة بالحيل الإجرائية المشروعة

إن اللجوء إلى الحيل الإجرائية المشروعة في مجال مكافحة الجرائم الإلكترونية أصبح أمراً مستحقاً، خاصة في ضوء تجاهل القانون رقم 63 لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات الكويتي النص على تنظيم النواحي الإجرائية لتتلاءم مع واقعية التجريم، حيث إنه لم يتم تعديل النصوص الإجرائية لتصطبغ بلون المكافحة المتخصصة لهذا النوع من الإجرام الذي يُسمى بالإجرام الناعم، والذي أصبح يهدد فئات اجتماعية مختلفة وخاصة الأطفال والشباب منهم، إذ يحتاجون إلى حماية خاصة، في مواجهة المواقع الإلكترونية الإباحية وكذا التي تحض على تعاطي المخدرات والمسكرات، وتلك

(9) Jorge Cardoso: ( Semantic Web Services, Processes and applications: Semantic Web and beyond ,computing for human experience ) - Printed in the United States of Americ – springer – 2006 – p.189.

التي تخصص لبث الكراهية والعنصرية والعدوان ضد الدولة بالدعوة للجهاد ضدها ومناهضة سياستها (داعش على سبيل المثال) تمهيداً للتأثير السلبي على الفكر وزرع النوازع الانتقامية بتصنيع الأسلحة المميتة. هذا وقد اتخذت الحيل المشروعة صورة محركات البحث النوعية ومنها على سبيل المثال (yahooligans)، وهو محرك مخصص للأطفال فقط ويوجد به حائط صد يمنع الولوج إلى مصادر غير آمنة، فلا يُطلب منه الإدلاء بمعلومات عن شخصيته ولا تتم دعوته لتسجيل بياناته للاشتراك في غرف الدردشة [10]. هذا وقد هجرت الدول الطرق التقليدية في تحديد الجرائم وكشفها وهوية مرتكبيها، فتوارت آليات وقائية تقليدية مثل الجدار الناري والبرامج المضادة للفيروسات وسجلات المتابعة وتحديثات البرامج [11].

ويلاحظ أن صور الانحرافات التي تؤكد ضرورات الحيل تتمثل في:

**(أ) انحراف على شبكات التواصل الاجتماعي:**

من أهم واجبات الدولة المحافظة على النشء، وهم ثروة الوطن الحقيقية، لذلك فإن الحماية الموضوعية والإجرائية تكون بالنسبة لجميع الأفراد، لكنها تكون بشكل خاص بالنسبة للفئات الأولى بالرعاية، وقد تشدد المشرِّع في ذلك، حيث نص في المادة (11) من قانون مكافحة جرائم تقنية المعلومات على أن: «لا تقل عقوبة الحبس أو الغرامة التي يحكم بها عن نصف حدِّها الأقصى إذا اقترنت الجريمة بأي من الظروف (1 -...2 -.. 3 - التغرير بالقُصَّر ومن في حكمهم من ناقصي الأهلية أو استغلالهم.4 -..). لذلك تكمن الخطورة في اطِّلاع الطفل على أنماط متنوعة من الشخصيات الإنسانية، ويتواصل مع من يتجاوز عمره الحقيقي، فيستعجل جني ثمار المعرفة ويصطدم بواقع مرير مليء بالتناقضات، فيتربى على السطحية والفراغ المعلوماتي، ثم تتجاذبه أشكال الجريمة في صورة السب والقذف وغيرهما، فيعبر عن سلوكه بالانطواء وكراهية المجتمع ليمارس التخريب والإتلاف في الخفاء كرد فعل للكبت الداخلي والظلم المستمر، ثم يصبح فريسة سهلة لتستقطبه أنواء المجهول[12].

(10) د. هبة محمد إسماعيل، معايير لتقييم مواقع الأطفال على شبكة الإنترنت، المؤتمر التاسع للاتحاد العربي للمكتبات والمعلومات (الاستراتيجية العربية الموحدة للمعلومات في عصر الإنترنت)، تونس، أكتوبر 1999، ص 19. د. هاجر محمد علي حبة، أثر استخدام الإنترنت على الأطفال، مجلة التنمية البشرية، كلية التنمية البشرية، جامعة أم درمان الإسلامية، الخرطوم، العدد الأول، فبراير 2015، ص 193.

(11) Simone van der Hof and Bibi van den Berg, Minding Minors Wandering the Web: Regulating Online child safety, Information Technology and Law Series, Vol. 24, asser press, (springer), The Netherlands, 2014, p.58.

(12) د. إيمان عمر فوزي، حماية الأطفال على شبكة الإنترنت من أجل استخدام أكثر أمناً وأكثر متعة، مجلة مكتبات نت، القاهرة، المجلد (4) العدد (4/3)، أبريل 2003، ص 7.

**(ب) انحراف يتم بوسائط الميديا:**

لقد أصبح من السهل أن يحمل الطفل هاتفه النقال أو حاسوبه المحمول ليسافر بخياله الرحب إلى أبعاد سحيقة يتعلم من خلالها نسيان الزمان والمكان، ويتعلم الشجاعة الهوجاء ومناطحة الفكر. هذا وقد ظهرت برامج عديدة تلعب دور ولي أمر الطفل حال غيابه مثل برنامج (Kaspersky Safe Kids) ليراقب نشاطه الإلكتروني بفعالية مباشرة على أجهزة (iphone أو ipad)، وهو برنامج لا يمكن للطفل أن يحذفه أو يعطله أبداً [13].

(13) Tom Funk, Advanced Social Media Marketing: How to Lead, Launch and Manage a Successful Social Media Program, Worldwide by Springer Science, Business Media New York, 2013, p.207.

## المبحث الثانى
## محاولة تأصيلية لصياغة قواعد إجرائية إلكترونية

كما هو معلوم فإن قانون الإجراءات والمحاكمات الجزائية الكويتي ينقل القواعد الموضوعية في قانون الجزاء أو القوانين المكملة من حالة السكون إلى حالة الحركة، وهي مرحلة التطبيق الفعلي أو التنفيذ العملي حتي تقتضي الدولة حقها بالعقاب من خلال مراحل التحريات وجمع الاستدلالات مروراً بمرحلة التحقيق الابتدائي حتى مرحلة المحاكمة وإصدار الحكم النهائي، وعندما صدر القانون رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات تطرق للنصوص الموضوعية المستحدثة وترك الجوانب الإجرائية للقواعد العامة التقليدية، ومن خلال هذا المبحث سوف نقدم تصوراً عن الجانب الإجرائي، وذلك من خلال النقاط التالية:

### أولاً- الغرض من القانون الإجرائي:

يتمثل الغرض الرئيسي بالنسبة للقانون الإجرائي في هذا المجال في: «مكافحة جرائم التقنية الحديثة الموجهة ضد المصالح الخاصة والعامة، والتصدي للعقبات القانونية الإجرائية بصورتها التقليدية في مجال التحريات والتحقيقات والمحاكمات، واتخاذ السلطات كافة الترتيبات الوقائية من أجل ترتيب وتجميع وتصنيف وتسجيل المحتوى الفني والمادي من أجل استجلاء الدليل الإلكتروني في مجال الإثبات الجنائي، وهو ما يسمح بمتابعة حلقات مشروعية الدليل من خلال نشاط إجرائي سليم يصلح لبناء عقيدة ويقين القاضي الجزائي»[14].

### ثانياً- حالات التطبيق ونطاقه:

يجب أن تستوعب مجالات تطبيق القانون الإجرائي المقترح مخاطر هامة ثبت يقيناً تعرضها للضرر، فتمد لها يد العون لتشمل الآتي: «تتحرك الإجراءات الوقائية بما تمثله من حيل هجومية ودفاعية لمواجهة الحالات التالية: (أ) كافة الأفعال الإجرامية التي تتم في الواقع الافتراضي – بغض النظر عن وسيلة الاتصال المستخدمة في نطاقه. (ب) الوقاية من أفعال التهديد أو عقد العزم على التخريب وصولاً إلى هدف إرهابي يمس أمن وسلامة دولة الكويت. (ج) الاعتداء الجسيم على نظم المعلومات العامة في المؤسسات الحكومية والخاصة، مما يجعل الوصول إلى تحريات وتحقيقات قضائية فعالة وناجزة من الأمور المستحيلة لطمس الدليل الفني. (د) كما ينطبق هذا القانون في حالة المساعدة

(14) د. محمد عبيد سيف وعبدالناصر محمد محمود، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية: دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، 12 - 2007/11/14، ص 12.

القضائية الدولية المتبادلة بين الكويت وأي بلد آخر إقليمي أو دولي لكشف جريمة إلكترونية ارتكبت ضد المجني عليهم في الكويت».

**ثالثاً- ترتيب الإجراءات الكشفية للجرائم الإلكترونية:**

يجب أن يهدف هذا القانون إلى وضع تنسيق إجرائي فعال لضمان سرعة الحصول على دليل إلكتروني، فيجب أن يشمل ما يلي: «تتحرك الإجراءات الكشفية في هذا القانون بواسطة النائب العام أو من يُفوِّضه ليأمر السلطات المختصة بملاحقة من ثبت انتهاكه وخرقه لضوابط المادة (2) من هذا القانون ليتم الآتي: (أ) يجوز للسلطة المنوطة بضبط الجرائم المعلوماتية (الضبط القضائي) التحفظ والحجز والقبض والتفتيش بحثاً على الدليل الإلكتروني ولو عن بعد، وذلك بالدخول إلى أي منظومة معلوماتية إجرامية تنتهك الخصوصية وثبت من خلال متابعة حركة سيرها الافتراضي خروجها عن الطبيعي والمألوف من الأمور وبصفة خاصة ارتكاب جرائم ضد الطفل»[15].

**رابعاً- متابعة الإجراءات ضمن النطاق الداخلي والخارجي:**

وهي إشكالية لابد من تداركها، ومن خلال ذلك يتعين الحكم بجواز: "تمديد القواعد الإجرائية المنصوص عليها في الفقرة السابقة إذا كانت هناك أسباب جدية ومعقولة تؤكد أن المعطيات الإلكترونية المُخزَّنة تستقي مرجعيتها من منظومة رئيسية أخرى وأن ما ثبت كشفه وفحصه هو مجرد منظومة فرعية تابعة، الأمر الذي يستدعي ضرورة أخذ الإذن من السلطة المختصة (النيابة العامة) بالمتابعة ولو عن طريق التراسل الإلكتروني بإشارات أو كتابات نصية تفيد ضرورة استكمال إجراءات البحث والتحري، أما إذا اقتضى التمديد الخروج عن النطاق الجغرافي للإقليم الكويتي فيمكن الاعتماد على أسس المساعدة القضائية التبادلية بين الدول وبشرط المعاملة بالمثل". كما يجب انسجام بروتوكولات اتصالات الإنترنت مع هذه الحيل المشروعة حتى تتم الحماية الفعالة خصوصاً للأطفال كما قررت ذلك اتفاقية بودابست لحماية الأطفال من التعرض للمواد الخادشة للحياء[16]. كما يمكن بناء استراتيجية واضحة لها أهداف وآليات لحماية الأطفال من الإهمال وسوء المعاملة لتتكامل الحماية مع الإجراءات الموضوعية [17].

(15) Ammar Rayes and Samer Salam, Internet of Things - From Hype to Reality: The Road to Digitization, Springer International Publishing, AG, 2017, Library of Congress, USA, p. 198.

(16) د. سهير العطار، الجرائم المستحدثة ضد الأطفال عبر النظم المعلوماتية: تحليل نصوص اتفاقية بودابست للمواد الخادشة للحياء، المؤتمر الإقليمي للطفل العربي في ظل المتغيرات المعاصرة، القاهرة، يناير 2004، ص 294.

(17) د. قاسم الصراف، مؤتمر حماية الطفل من سؤ المعاملة والإهمال، مجلة الطفولة العربية، الكويت، المجلد 3 العدد 9، لسنة 2001، ص 126.

**خامساً- خطوات إظهار الدليل الفني:**

وهي تُعد أخطر نقطة على الإطلاق نظراً لمساسها بالحقوق والحريات والضمانات وأيضاً حجية الدليل الإلكتروني في مجال الإثبات الجنائي، لاسيما وأن المفتش التقليدي قد يصل إلى المحتوى الفني فيهدره ويتلعثم في استجلائه بعكس المتخصص الخبير المُزوَّد بالتقنيات والبرامج التي تغوص في عمق الدليل على اعتبار أن الدلائل الإلكترونية لا يجب أن تكون ظنية بل يقينية [18]. وعليه يتبلور الآتي: «للسلطات المنوط بها تنفيذ الإجراءات إثبات المعطيات الإجرامية المُخزَّنة من حيث النوع والطبيعة والماهية والآليات التي تباشرها، ولها في ذلك تتبع المعطيات الرئيسية والطرفية المستعملة في الاتصال الإلكترونى أو وسائل التواصل الاجتماعي والخدمات التكميلية لها. ويجب إثبات وقت التنفيذ وتاريخه كاملاً والمدة التي استغرقتها عملية الكشف عن مُكوِّنات المحتوى الإلكتروني عن بعد أو بوسيلة الضبط المادي بالحصر على الطبيعة لأدوات الجريمة. كما يتعيَّن إثبات صفة الجاني وعنوان الموقع الذي يستخدمه في الإيقاع بضحاياه ووسيلته وبرامجه التفاعلية الأخرى». هذا وقد غاب على المشرِّع في القانون رقم 63 لسنة 2015 أن يقدم تعريفاً واضحاً للدليل الإلكتروني، ومن جهتنا فإننا نعتقد بأنه يمكن تعريفه بأنه: «مجموعة من البيانات والمعلومات التي يمكن استخلاصها من جهاز حاسوب وبشكل يمكن قراءته وتحليله وذلك بالاستعانة بأشخاص لديهم من الخبرة والمهارة في اكتشاف بواطن هذه المعطيات بواسطة برامج وتطبيقات وتقنيات في كافة المجالات المادية والفنية التي يعتمد عليها القاضي الجزائي في بناء عقيدته»[19].

**سادساً- تقنين للحيل المشروعة الدفاعية والهجومية:**

يجب أن تتضمن القواعد الإجرائية منح شرعية قانونية لاستخدام هذه الحيل التي تستخدمها الدول لكشف الجرائم الإلكترونية، وذلك من خلال النص على أنه: "على السلطات المختصة بتطبيق هذا القانون كل في موقعه استعمال البرامج الحديثة عالية التقنية واستخدام ذلك في الحيل الإجرائية الهجومية والدفاعية لسرعة التدخل الحاسم لإثبات المحتوى الفني ودليله وماديات الجريمة ولمباغتة المجرم ومحاصرته بأفعاله المخلة بالنظام العام والآداب، كما لها وضع الترتيبات الإجرائية التي تتناغم مع سلطتها التقديرية من أجل تحقيق الأمن والاستقرار المعلوماتي. كما يجب أن لا تخل هذه الحيل أياً كانت صورتها ونمطها وتأثيرها على الحقوق والحريات المكفولة بموجب الدستور

(18) د. محمد محمود عمري، الإثبات الجزائي الإلكتروني في الجرائم المعلوماتية: دراسة مقارنة، مجلة العلوم القانونية والسياسية، الجمعية العلمية للبحوث والدراسات الاستراتيجية، بغداد، المجلد 12، العدد 2، لسنة 2016، ص 303.

(19) د. أسامة بن غانم العبيدي، الإثبات بالدليل الإلكتروني في الجرائم المعلوماتية، مجلة جامعة الملك سعود، كلية الحقوق والعلوم السياسية، الرياض، مجلد (25)، العدد (1)، يناير 2013، ص57 وما بعدها.

والقانون. ويُعد أي برنامج ينتهك الخصوصية أو يسعى إلى عرقلة الهدوء الذي تنعم به من قبيل الأفعال المجرمة طبقاً لقانون الجزاء الكويتي ويبطل أي دليل يستند إلى برنامج ينتهك الخصوصية للأفراد". كما يجب توعية الأفراد من خلال الإعلام الأمني بما تملكه الدولة من مقومات إلكترونية حديثة لردع كل من تُسوِّل له نفسه التلاعب أو الاحتيال في الفضاء الإلكتروني تفعيلاً لمقتضيات الأمن القانوني، وهو ما يسمح بإيجاد شراكات استراتيجية في التعاون الإعلامي كما فعلت عدة دول أوروبية ويمكن أن يتم تطبيقه في البلدان العربية على اعتبار أنه يُحسِّن من النظام العام الإجرائي [20].

**سابعاً- إنشاء محكمة مختصة للجرائم الإلكترونية:**

يُعد مقترح إنشاء محكمة مختصة للجرائم الإلكترونية أمراً مهماً وضرورياً من أجل تشجيع التخصص النوعي لملاحقة ومكافحة هذا النوع من الجرائم المتزايد والمتلاحق. ومن شأن هذه المحكمة التي تتمتع بالاستقلالية والفاعلية تطبيق القواعد الإجرائية بمهنية وفنية في عملها لاستخلاص الدليل من ثنايا المجهول الإلكتروني بالنظر لعجز القواعد الإجرائية التقليدية عن مواكبة التطور المتنامي. وفي ضوء ذلك، يجب أن تنشأ محكمة نوعية مختصة على غرار محكمة الأحداث التي تم إنشاؤها بالقانون رقم 111 لسنة 2015، ويكون نص إنشائها مشابهاً لذلك، حيث: "تنشأ محكمة متخصصة لمكافحة الجرائم الإلكترونية بكافة صورها وأنماطها، يرأسها قاض ويعاونه أربعة من الخبراء الفنيين، يختارهم الوزير المختص، ويمكن أن تستعين المحكمة بمن تندبه لتحقيق أغراضها. وتهدف المحكمة إلى تحقيق التكامل الموضوعي والإجرائي لحماية المجتمع من مخاطر العالم الافتراضي". ونعتقد بأنه إذا لم يكن إنشاء المحكمة متاحاً، فإنه يجب على أقل تقدير استحداث دائرة جزائية في المحكمة الكلية خاصة بالجرائم الإلكترونية، وذلك لتحقيق التوافق والحماية الإجرائية [21].

**ثامناً- فض إشكالية الاختصاص في حال التنازع:**

يجب تبني استراتيجية دولية تتفق عليها الدول عموماً تضمن الملاحقة للجرائم التقنية، بحيث توضح أسس تحدي الاختصاص القضائي والتعاون الدولي بشأن محاكمة المتهمين بارتكاب هذه الفئة من الجرائم، على أن: «تختص المحاكم الكويتية على اختلاف درجاتها بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والرقمنة، فإذا ارتكب الجاني أنماطها خارج إقليم دولة الكويت قاصداً تعطيل مؤسساتها أو التعرض

(20) George Christou, Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy, Palgrave Macmillan in the UK is an imprint of Macmillan Publishers Limited, 2016, p.164.

(21) Pompeu Casanovas & Ugo Pagallo & Giovanni Sartor & Gianmaria Ajani, Approaches to the Complexity of Legal Systems: Complex Systems , the Semantic Web, Argumentation and Dialogue, Springer-Verlag Berlin Heidelberg, 2010, p.113.

للمصالح العامة والخاصة»، وبذلك ينهي الجدل الفقهي الحديث فيما يتعلق بما إذا كان القضاء الكويتي مختصاً أم لا إذا كان الجاني خارج الإقليم الكويتي وارتكب فعلاً يُشكِّل جريمة وفق قانون الجزاء أو القوانين المُكمِّلة على سبيل المثال (قانون الوحدة الوطنية) أو عن طريق الإنترنت بأن تعرض لأحد مكونات الشعب الكويتي سواء طائفياً أو اجتماعياً، وهذا المكون قد يكون داخل الكويت أو خارجها.

**تاسعاً- البطلان كجزاء إجرائي:**

يجب أن يتضمن القانون شق الجزاء ليتكامل مع شق التكليف الوارد فيه لضمان الالتزام الطوعي والتلقائي له وتبيان الآثار الجوهرية في حالة مخالفة أحكامه، وذلك بالنص على أنه: «يبطل كل إجراء تتخذه السلطات المنوطة بتنفيذ أحكام هذا القانون، فلا يعتد به كدليل له حجية قانونية أمام القاضي إذا أخل بأحد الركائز والضمانات الجوهرية التي ينص عليها الدستور لاسيما الحق في الخصوصية والأمن والبراءة والسلام الاجتماعي. ومع عدم الإخلال بأي عقوبات أشد قد ترد في أي قانون متى شكلت هذه الأفعال المرتكبة جريمة جزائية أو تأديبية أو حتى التعويض المدني».

**عاشراً- عقوبة جزائية على خرق مبدأ السرية:**

لقد تجاهلت القواعد الموضوعية الواردة في المادة (15) من القانون رقم 63 لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات أي عقوبات على من يخرق قدسية وسرية العمل الإجرائي لضمان فاعليته، فالموظفون الذين يحددهم قرار الوزير المختص بمنح صفة الضبطية القضائية قد يتجاوزون وينحرفون عن مسار العمل القويم فيدلون بمعلومات فما جزاؤهم في هذه الحالة؟ وما حدود واجباتهم وصلاحياتهم ومسؤولياتهم حال ارتكابهم جريمة إفشاء للسر أو طمس للدليل وإخفائه؟. ولذلك فإنه يجب معالجة هذا الوضع بصياغة تتماشى مع خصوصية وسرية المهنة من خلال النص على أنه: «يحظر تماماً إفشاء أسرار عمليات وإجراءات الضبط والتفتيش الإلكتروني بواسطة رجال الضبط القضائي أو من الخبراء أو أي موظف يندب لتحقيق غرض الكشف عن الجرائم، ويعاقب بعقوبة الحبس لمدة ثلاث سنوات وبغرامة لا تتجاوز 20 ألف دينار أو بأحدى هاتين العقوبتين».

ونلاحظ أن هناك عقوبة لذات الفكرة الوقائية تلقفها المشرِّع البحريني لتجريم هذه الأفعال في قانون رقم 60 لسنة 2014 بشأن مكافحة الجرائم الإلكترونية، حيث أورد حظراً على كل من يسند إليه عمل من النيابة العامة بجمع أو حفظ الدليل المعلوماتي ويكشف عنه دون مُسوِّغ قانوني بحيث يفتش مكنونات السر وبواطنه أو الانتفاع به بأي طريق وذلك بالنص في المادة (18) على عقوبة الحبس لمدة سنة وبالغرامة التي لا تجاوز ثلاثة آلاف دينار أو بإحدى هاتين العقوبتين.

## المبحث الثالث

## تهيئة البيئة المحلية لاستيعاب المعالجة الإجرائية الإلكترونية

تحتاج البلاد إلى نقلة نوعية في فلسفة مكافحة الجرائم الإلكترونية تنطلق في مسارات متنوعة لتشمل الأمني والقانوني والاجتماعي والسياسي، وهنا يجب أن نتخلى عن التمسك بالطرق التقليدية الإجرائية التي تشوه الدليل وتفتقد الفعالية وتطوي وتهدر الحقوق والحريات والضمانات وتقتحم الخصوصية. ونرى ضرورة التوسع في فهم بعض النصوص التشريعية لكي تستوعب موجهات ودعائم وركائز هذه المعالجة الإجرائية مع تكامل بعض القوانين والأجهزة بوضعها الحالي ومنها إدارة مكافحة الجرائم الإلكترونية التابعة للإدارة العامة للمباحث الجنائية، وهيئة الاتصالات وتقنية المعلومات، وذلك من خلال القانون رقم 37 لسنة 2014، وأيضا القانون رقم 9 لسنة 2001 بشأن إساءة استعمال أجهزة الاتصالات الهاتفية والتنصت، وكذلك قانون رقم 61 لسنة 2015 في شأن تنظيم وتركيب كاميرات وأجهزة المراقبة الأمنية، وقبل كل ذلك تعديل نظرة القاضي الجزائي للدليل الإلكتروني. وفي ضوء ذلك، فإننا سنقسم هذا المبحث إلى المطالب التالية:

### المطلب الأول

### ضرورة التحول القضائي لفهم متطلبات الدليل الرقمي

ينطلق هذا التحول من تغيير في منظومة العدالة وما يكتنفها من أطر تشريعية على المستوى الجزائي والتكميلي له وهي تشمل الآتي:

**أولاً- إنشاء مختبر جنائي متخصص رقمي تابع لوزارة العدل أو للإدارة العامة للأدلة الجنائية:**

من شأن هذا المختبر أن يساعد القاضي الجزائي على استلهام بوادر الدليل، فتكون لهذه المعمل صلاحيات تحليل وتوثيق وحماية الدليل من التلف والتغيير، فيمكن عمل نسخة احتياطية من الأصل واسترجاع المعلومات من خلالها، ويكون تابعاً لوزارة العدل أو تابعاً للإدارة العامة للأدلة الجنائية التابعة لوزارة الداخلية، وتصبح إدارة من إداراتها. وتجدر الإشارة في هذا المجال إلى أن هناك مختبراً حالياً ولكنه ليس مختبراً بالمعنى الدقيق، إذ يوجد به فقط تفريغ الأجهزة الإلكترونية فقط من محتواها. كما نود التأكيد في هذا السياق إلى أنه يمكن الاستعانة بشركات القطاع الخاص من أجل إنشاء هذا المختبر. (انظر حكم محكمة الاستئناف العليا رقم 2015/52 الصادر في جلسة 2017/1/19). ويقع

على القاضي الجزائي واجب استخلاص ثبوتية الدلائل ويقينها حتى يُرجِّح حجيتها أو يهدرها فلا يترك الأمر لذات القواعد الإجرائية في قالبها التقليدي، بل يمكن خلق خصوصيات قضائية من السوابق المتواترة التي يكتسبها القاضي من خبرات هذا المختبر الجنائي المتفرد في طابعه الرقمي.

**ثانياً- التكامل الشخصي للدلائل الرقمية:**

يقوم هذا الدور على محاور ترتيبات وتنسيقات منتظمة تبدأ خيوطها الأولى عند رجل الشرطة المعلوماتي والمحقق المعلوماتي والخبير المعلوماتي لتنتهي عند القاضي المعلوماتي من أجل إيجاد تخصص وتميز يواكبان مستجدات العصر. فلا يجب أن ينفرط عقد هذه السلسلة، بحيث إذا فقدت حلقاتها قد لا تنتج آثارها. فهذه المنظومة تجسد واقعية تهيئة البيئة لاستيعاب نظم وتقنيات تحدد الهويات وتتغلب على غموض الحوادث كما هو التشكيل في فريق (CIRT)[22]. والقاضي الحصيف يسعى إلى توسيع مداركه وتنمية تخصصه، فيتكون لديه قدرات وعلاقات ترابطية بمشغلي الحاسب وخبراء البرامج ومديري النظم المعلوماتية ومحللي البيانات ومهندسي الصيانة من أجل ابتكار خطة هادفة يمضي في خطواتها ليستجلي الدليل الفني، فيُراجع ويُمحِّص ويبدي الملاحظات ويؤكد شرعية الإجراءات، فإن بُنيت على دلائل مختلقة أو وهمية انهارت عقيدته وبنى أحكامه على الشك الذي قد يُفسر لصالح المتهم، وهنا تتراجع آليات وسبل المكافحة كلما توارت الأفكار خلف جدران النمطية التقليدية في الإجراءات العادية التي لابد من أن يعزف عنها القاضي حتى تتهيأ البيئة المحلية لاستيعاب تقنيات معقدة.

## المطلب الثاني

## إدارة مكافحة الجرائم الإلكترونية

حدد القرار الوزاري اختصاصات الإدارة المذكورة أعلاه بحيث لا يقتصر دورها على الإشراف ووضع الخطط اللازمة لكشف الجرائم الإلكترونية ومتابعة التعديات على حقوق الملكية الفكرية وتشويه وإتلاف المعلومات والقرصنة والاحتيال، بل يشمل دورها توفير المستلزمات الفنية للبرمجيات والأجهزة عالية التقنية التي تحول دون استدراج المواطنين عموماً والأطفال خصوصاً في سلسلة الإجرام الإلكتروني. ونظراً لأنها تتبع المباحث الجنائية بوزارة الداخلية فإنه يظهر عليها التأثر الشديد بالاعتماد على الطرق التقليدية الواردة في قانون المحاكمات الجزائية الكويتي رقم 17لسنة 1960 بما يشمله

(22) د. حسام الدين مصطفي علي، فريق الاستجابة لحوادث الكمبيوتر (CIRT) Team Response Incident Computer مؤتمر أمن المعلومات والحكومة الإلكترونية، المنظمة العربية للتنمية الإدارية، كوالالمبور، أبريل 2009، ص 5.

من ضبط للأشياء المنصوص عليها في المواد من (90 إلى 97) ومعاينة وتفتيش وقبض، وقد لا تتواكب هذه الإجراءات مع طبيعة الجريمة الإلكترونية وصفة مرتكبها نظراً لتمتعه بالحيلة والذكاء [23].

لذلك نرى أن تخصص مبالغ من ميزانية وزارة الداخلية لتغطية مصروفات شراء البرامج التفاعلية واستيرادها من الخارج، بحيث يتم متابعة تحديثها والتدريب على استخدامها من قبل الخبراء والفنيين المتخصصين والمؤهلين من رجال الضبطية القضائية، بحيث يتم الإلمام الكامل بوسائل هذه البرامج تمهيداً لاستخدامها في الأغراض المخصصة لها أصلاً وفي مقدمتها حماية الأفراد من براثن الانقياد للعوالم الافتراضية الفتاكة. كما لا يجب أن تستخدم هذه البرامج في انتهاك الخصوصية أو عرقلة ممارسة الحقوق والحريات لاسيما التعبير عن الرأي والفكر، بحيث لا يمكن أن نعالج جريمة انتهاك الخصوصيات والانحراف في محاذير التواصل الاجتماعي بجريمة أخرى أشد قسوة وهي كبت الحرية والتمادي في وأد الفكر الحر المستنير بفزاعة وهمية تعطل القانون.

كما يجب على هذه الإدارة أن تستلهم دورها في كافة المراحل (الاستدلال والتحقيق والمحاكمة) بكتابة تقارير فنية عن الآليات المستخدمة في ضبط الجريمة محل الاتهام وقدرتها على استجلاء الدليل واستنباط معطياته من خلال وسائل الكشف والفحص والحيل المقترنة بذلك. كما يتعين عليها متابعة آليات العمل في المختبر الجنائي التابع للإدارة العامة للمباحث الجنائية بوزارة الداخلية لتصوير المشتبه فيهم والانتقال إلى بؤرة الأحداث لإثبات صورة حية نابضة يستلهم منها القاضي الجزائي عقيدته في إرساء العدالة. كما يجب أن تخضع الأدلة لمبدأ اليقينية وجواز المناقشة الشفوية والحصول عليها بطريق شرعية [24].

هذا وقد وسَّعت بعض الدول من النماذج الخاصة لإدارة مكافحة الجرائم الإلكترونية وصنفت نشاطها ضمن إدارات مكافحة الاعتداء على الأمن القومي، ومنها فرنسا وسويسرا وبلجيكا، وهذه الدول تسمي الإدارات لديها بالمجلس القومي لحماية البيانات، ومنحته من الخصوصية والاستقلالية (الفنية والمالية والإدارية) بما يسمح له بأن يكافح بفعالية كافة صور الاعتداءات على البيانات، كما أن هناك أقساماً فرعية داخل المجلس الرئيسي تسعى إلى وضع حماية خاصة للطفل وإحاطته برعاية خاصة من مزالق

(23) د. محمود فتوح سعدات، خصائص الجرائم المعلوماتية وصفات مرتكبيها في ظل مجتمع المعلومات، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية (ICACC)، كلية علوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية، الرياض، 2015، ص34.

(24) د. راشد بن حمد البلوشي، الدليل في الجريمة المعلوماتية، مجلة الحقوق للعلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، القاهرة، العدد1، لسنة 2008، ص 27.

الانحراف في الواقع الافتراضي. ومن جهتنا فإننا ندعو إلى تبني إنشاء قسم خاص لحماية الطفل في إدارة مكافحة الجرائم الإلكترونية يكون أكثر نجاعة في الحماية وأكثر تخصصاً [25].

## المطلب الثالث

## التشريعات القانونية ذات العلاقة

هناك محاولات تشريعية سابقة على القانون رقم 63 لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات وهي:

### أولاً- قانون إساءة استعمال أجهزة الاتصالات الهاتفية والتنصت:

تبنى المشرع هذا القانون بعد حدوث طفرة التراسل عبر تقنية البلوتوث ونشر الصور والمقاطع المصورة في بداية الألفية الثانية، وأيضاً يجابه هذا القانون رقم 9 لسنة 2001 إساءة استعمال الاتصالات الهاتفية واستعمال أجهزة التنصت في غير الحالات القانونية، ونرى ضرورة تكامل المادة (2) من هذا القانون والتي تبين مضمون حظر التداول بالبيع والشراء وحالات الاستعمال بواسطة جهة رسمية مختصة منوط بها الحيازة بواسطة إذن مسبق من النيابة العامة طبقاً لقانون المحاكمات الجزائية رقم (17) لسنة 1960، مع تفعيل شبكة معلوماتية حمائية تضمن عدم اختراق الخصوصية، فيجب على الأجهزة التي يناط بها كشف الدليل الإلكتروني أن لا تستخدم وسيلة للتنصت تنتهك الحقوق والحريات. كما ندعو إلى تشديد العقوبة الواردة بالمادة (2) لتصبح ثلاث سنوات وغرامة 20 ألف دينار بدلاً من العقوبة في صورتها الراهنة وهي الحبس لمدة لا تجاوز سنة وغرامة لا تجاوز ألف دينار أو بإحدى هاتين العقوبتين كلما وظّف الجاني انتهاك الخصوصية في التنصت على أجهزة الاتصالات على اعتبار أن العقوبة في صورتها الراهنة ليست محققة للردع العام والخاص لاسيما وأن الجريمة المرتكبة على جانب كبير من الخطورة.

### ثانياً- قانون رقم 61 لسنة 2015 في شأن تنظيم وتركيب كاميرات وأجهزة المراقبة الأمنية:

أشارت المذكرة الإيضاحية للقانون أعلاه إلى أنه: نظراً لما للتدابير الأمنية الوقائية من أثر فعال في الحدِّ من وقوع الجريمة وسرعة الكشف عن مرتكبيها وحفاظاً على سلامة

(25) A.T.Wood and Harrper nimal jayaratna ,Methodologies for Developing and Managing Emerging technology based information systems) - Methodologies 1998, Sixth International Conference on Information Systems Methodologies - Springer-Verlag London 1999 – p.102.

المنشات، لذلك فتهيئة البيئة المحلية لاستقبال المعالجة الإجرائية من منطلقات هذا القانون، وهي تهدف إلى إحداث نوع من الترابط والتكامل بين كاميرات المراقبة التي تحددها السلطة المختصة (وزارة الداخلية) مع جهاز حاسوب رقمي رسمي حكومي منوط به فحص وتحديد هوية وصورة ومكان الأشخاص المتورطين في ارتكاب جرائم ضد الأفراد، بحيث يطابق ملامح وهيئة المنحرف الإلكتروني الذي يتواجد في بؤرة الأحداث لتلتقطه الكاميرات وتفصح عن هويته بكل بساطة تميهداً لتقديمه للسلطات، وهو تكامل فني يشبه تطبيق آلية ماندريك الأمريكية (وهي تتكون من دوائر تلفزيونية ممغنطة ومغلفة مرتبطة بكاميرات خفية توضع في الشوارع والميادين وكافة مناطق التنقلات لرصد أي شخص والتي تقوم بإرسال صور إلى جهاز حاسب آلي رقمي لملاحقة المجرمين على الشبكة الافتراضية، ولهذا فإن تهيئة البيئة يحتاج التي حسن توظيف واستخدام الجوانب الرئيسية في هذه المعادلة، وهي تتمثل في: تخصيص مساحة من البث التليفزيوني، ونصب كاميرات ممغنطة خفية في الشوارع والأماكن العامة تتولى التقاط صور ومتابعة تحركات وخط سير الشخص المشتبه به، وارتباط الكاميرات بإشارات البث وبحاسوب إلكتروني مرصود لتحديد أماكن المجرم، وتطابق الصورة محل البث مع الصورة المخزنة في الحاسب العملاق ليتم مراقبة الشخص المتورط تمهيداً للقبض عليه وتقديمه للمحاكمة العادلة.

## ثالثاً– قانون إنشاء هيئة الاتصالات وتقنية المعلومات رقم (37) لسنة 2014:

أشارت المذكرة التفسيرية لهذا القانون بأنه: "نظراً للتطور السريع الذي يشهده قطاع الاتصالات وتكنولوجيا المعلومات عالمياً والحاجة الماسة إلى تنظيم هذين القطاعين، لذلك باتت الحاجة ملحة إلى صدور قانون بتنظيم الاتصالات وتقنية المعلومات"، ومن خلال هذا القانون تمت إضافة مواد نوعية تتضمن ضرورة فحص القواعد الفنية والمواصفات القياسية لضمان جودة الاتصالات ومنع تأثير التشويش على الترددات الطيفية في البر والبحر والجو، لاسيما وأن ازدياد الهواتف الذكية في الأسواق لا يحكمه تنظيم كامل. كما يجب أن تتبنى الهيئة إعداد برامج توعية لنشر الوعي التقني بمحاذير إساءة استعمال الهواتف ووسائل الاحتيال والتلصص وانتهاك الخصوصية، وسبل تعقب الأشخاص دائمي القرصنة على الحسابات الشخصية للأفراد في شبكة التواصل الاجتماعي. كما يجب أن تتلقى الشكاوى من المواطنين وتعمل على إزالة العقبات الإلكترونية التي يواجهونها عند استخدام الكمبيوتر عموماً وتبيان حالات تعرضهم للخطر والضرر [26].

(26) د. أشرف عبدالعزيز يوسف، المواد الإباحية للأطفال جريمة معلوماتية، مجلة الطفولة والتنمية، القاهرة، العدد 20، المجلد (5)، سبتمبر 2013، ص109.

## الخاتمــة:

من خلال ما سبق مناقشته في البحث، يتبيَّن لنا أنه يمكن استخدام أدوات تقنية تساعد في تحديد شخصية الأفراد المتورطين في الجرائم الإلكترونية، كما يتبيَّن لنا أن البيئة المحلية صالحة لاستقبال هذا النظام إذا تم تعديل بعض أحكام القوانين الحالية، وأن هذه الصلاحية يمكن أن تؤتي ثمارها إذا ما تعززت ببعض التوصيات في المجالات القانونية والأمنية والسياسية.

وعليه، فقد توصلنا في هذا البحث إلى مجموعة من النتائج والتوصيات للحد من مخاطر الجرائم المعلوماتية، نعرض لها على النحو التالي:

### أولاً- النتائــج:

1- إن اعتماد الحيل الإجرائية المشروعة أصبح اليوم إجراءً ضرورياً لتحديد هوية المجرم الإلكتروني واصطياده في العوالم الافتراضية وملاءمتها في البيئة المحلية إذا انطلقت من مفهوم محدد لتشمل: "مجموعة من الخطوات المترابطة والأدوات التي تهدف لمواكبة الإجرام الحديث وعلى وجه الخصوص نوعية جرائم الحاسب الآلي لتتلافى مساوئ الإجراءات الجزائية في صورتها التقليدية"، فهي عبارة عن: "أسلحة إجرائية تكتيكية يتعين على السلطة المختصة بكشف الجرائم الإلكترونية منحها للقائم بضبط وإحضار ومعاينة وتفتيش محل الفعل المُجرَّم لتشمل حيلاً دفاعية هدفها المنع وأخرى هجومية هدفها المواجهة والكشف".

2- ثبت يقيناً أن تهيئة البيئة المحلية لاستيعاب المعالجة الإجرائية يتم في عدة محاور منها القضائي، وذلك بضرورة هجر المفهوم التقليدي لنمط الإجراءات الجزائية وإحلال سياسات وقائية ناجعة لها القدرة على استنباط الدليل الرقمي بإنشاء مختبر جنائي متخصص في الرقمنة، كما أن من الضرورات توسيع دائرة الاختصاص في إدارة مكافحة الجرائم الإلكترونية كما فعلت بعض البلدان الأوروبية مع تعديل في أحكام بعض القوانين الموضوعية كقانون إساءة استعمال أجهزة الاتصالات الهاتفية، وقانون كاميرات المراقبة، وقانون إنشاء هيئة الاتصالات وتقنية المعلومات.

3- ضرورة تحقيق العديد من الضمانات الحمائية في المجال الإجرائي التي تضفي شرعية على الدليل المستمد من الجريمة الإلكترونية، وتحديد هوية الأشخاص المتورطين فيها وعدم التغول على الحقوق والحريات، وتأهيل الأطفال ليتعاملوا مع العولمة المعلوماتية بأمان. ويتعين ترتيب هذه الضمانات بدءًا بتحصيلها والاستحواذ عليها ومروراً بالتحليل وانتهاءً بالتوثيق الفني للدليل ليكون أكثر فعالية. كما تتأكد ضرورة اهتمام المشرع بتكامل النواحي الموضوعية مع النواحي الإجرائية ليكون

هناك انسجام بين القواعد، فتظهر فعالية وكفاءة الحماية. وبالإضافة إلى ذلك، فقد ثبتت مخاطر إهمال معالجة الأمور الإجرائية ومعضلات تركها للقواعد العامة وأهمية وضع خصوصية إجرائية للجرائم الإلكترونية.

## 1- ثانياً- التوصيات:

**في ضوء نتائج البحث المبينة أعلاه، فإننا نوصي بما يلي:**

1- ضرورة أن يتبنى المشرع التجريم في واقعية واضحة لا لبس فيها أو غموض أو تجريم أنماط مطاطة من أنواع السلوك في مجال الجرائم الإلكترونية حتى لا تتخبط أسس الحماية الموضوعية وينتج بالتبعية تنافر بين أسس الحماية الإجرائية ومراعاة المنظور المستقبلي في التجريم لاسيما وأن هذه الأفعال سريعة التطور بشكل متلاحق[27].

2- ضرورة وضع قانون إجرائي متخصص لمكافحة الجرائم الإلكترونية والتخلي عن الجوانب التقليدية التي تمنحها النصوص الإجرائية بوضعها الراهن في قانون المحاكمات الجزائية الكويتي رقم (17) لسنة 1960، وذلك بعدما ثبت عدم فعالية وسائل التحري وجمع الاستدلالات والتحقيق والمحاكمة في استنباط دليل إلكتروني واضح المعالم، أو يحقق التوازن بين الحقوق والحريات وشرعية الدليل الإجرائي وفعاليته. كما يجب الأخذ في الاعتبار ضرورة أن يتضمن القانون الإجرائي المقترح أهدافه وحالاته وشروطه وضماناته، وإنشاء محكمة نوعية مختصة بنظر هذه الجرائم، وإجراءات استجلاء الدليل الفني وحجيته في الإثبات وتقنين واضح لمجموعة من الحيل الإجرائية المشروعة التي تستعين بها السلطة المختصة لتحديد هوية الجناة في الجرائم الإلكترونية عموماً وضد الأطفال بشكل خاص، وتحديد الاختصاص والتنازع فيه، والعقوبات التى تتقرر كلما انتهكت أحكامه سواء بالبطلان أو بالجزاءات الأخرى في أي قانون جزائي مكمل.

3- نوصي بضرورة تبني إنشاء مختبر جنائي متكامل فنياً لاستجلاء الدليل الإلكتروني والدعوة إلى إنشاء هذا المختبر المتخصص في مكافحة الجرائم الإلكترونية تُستخدم فيه بالفعل التقنيات الحديثة بما في ذلك البرامج والتطبيقات الجديدة[28].

4- تقديم ووضع بعض الضمانات الإجرائية الوظيفية لمن يتولون الكشف عن هوية المجرم الإلكتروني تتمثل في عدم الملاحقة القضائية إذا انصاع في حدود الأمر من

(27) د. عادل يوسف عبدالنبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مجلة مركز دراسات الكوفة، العراق، العدد 2، لسنة 2011، ص127.

(28) د. عبدالحليم بن بادرة، إجراءات البحث والتحري عن الجريمة المعلوماتية: الخصوصية والإشكالات، مجلة الحقوق والعلوم الإنسانية، جامعة زيان بن عاشور، الجزائر، العدد 23، مايو 2015، ص 97 وما بعدها.

رئيسه المباشر واعتقد بحسن نية (كسبب من أسباب الإباحة كما هو منصوص عليه في قانون الجزاء في المادة رقم (37))، أن هذا الأمر يكتسب الشرعية ما يمكنه من التنفيذ على الوجه الأكمل، مع تحديد نطاق المسؤولية في حال الإخلال بالعملية الإجرائية إذا كان الخطأ جسيماً لا يمكن تداركه.

5- على السلطة المختصة دعم البرمجيات المتخصصة في الحماية بحيث تتكامل مع إنشاء مواقع إلكترونية تعليمية وثقافية عربية جذابة تشجع الأطفال بشكل خاص على الاطلاع على معالمها فلا ينجرفون إلى ثقافات غربية مستوردة قد يصطدمون معها. كما ينبغي عدم تحميل أي برامج ذات دلالات غامضة تنتهك الخصوصية والسلامة من أجل تأمين نظام متكامل يحمي البيانات والمعلومات ويضمن نسخها احتياطياً حتى تكون بمأمن من أي اختراق مستقبلي[29].

6- تخصيص ميزانية ودعم مالي للكشف عن هذه الجرائم، تتوجه أوجه الصرف فيها لشراء برامج تفاعلية تضمن تنفيذ الحيل الإجرائية المشروعة داخل المؤسسات الحكومية والخاصة وخارجها ومواجهة الكوارث المعلوماتية لاسيما عند تنفيذ الخطط العادية والاستثنائية. كما يتعين أن يتم الصرف منها في تحفيز الكوادر الفنية ذات الخبرة في اقتفاء أثر الدليل الإلكتروني، وتدريبهم وتوظيفهم في أماكن التشغيل مع منحهم مكافآت مالية ومعنوية كلما نجحوا في فك شفرات التعقيدات الإلكترونية.

7- يجب على رجال الضبط القضائي أثناء التفتيش عن الدليل الإلكتروني التزام نطاقه فلا يتم تجاوز ذلك أو اختراق ضوابطه. ويمكن أن يتحدد هذا النطاق بالمكونات المادية والتي تشمل المزود الآلي والمضيف والملحقات التقنية والقطع الصلبة والبرمجيات والشبكات السلكية وكذلك الشبكة العنكبوتية وملحقاتها من مواقع وملفات ومجلدات مخزَّنة بشكل مستقل[30]. وأيضا يقع على رجال الضبط القضائي واجب الإسراع في الإنجاز حتى لا يتعرض الدليل للتلف والتدمير من الجاني. كما يجب التأكد من نظافة سلة المهملات لاسترجاع المعلومات بطريقة فنية سليمة حتى تتم آليات عمل الحيل الإجرائية بطريقة سليمة[31].

---

(29) عبدالمطلب أحمد د. السماني، الحماية الأمنية من الأخطار المحتملة على شبكة الحاسب الآلي: دراسة مسحية تحليلية في مدينة الرياض، المجلة العربية للدراسات الأمنية والتدريب، المجلد 28، العدد 56، لسنة 2012، ص247.

(30) د. عادل عبدالله خميس العمري، التفتيش في الجرائم المعلوماتية، مجلة الفكر الشرطي، مركز بحوث الشرطة، الشارقة، الإمارات، المجلد 22، العدد 86، يوليو 2013 ، ص261.

(31) Babak Akhgar & Ben Brewster, Combating Cybercrime and Cyber terrorism Challenges: Trends and Priorities, Advanced Sciences and Technologies for Security Applications, Springer International Publishing Switzerland, 2016, p.131.

## المراجع:

### أولاً- باللغة العربية:


- د. أسامة بن غانم العبيدي، الإثبات بالدليل الإلكتروني في الجرائم المعلوماتية، مجلة جامعة الملك سعود، كلية الحقوق العلوم السياسية، الرياض، مجلد 25، العدد1، يناير 2013.
- د. أشرف عبدالعزيز يوسف، المواد الإباحية للأطفال جريمة معلوماتية، مجلة الطفولة والتنمية، القاهرة، العدد 20، المجلد 5، سبتمبر 2013.
- د. إيمان عمر فوزي، حماية الأطفال على شبكة الإنترنت من أجل استخدام أكثر أمناً وأكثر متعة، مجلة مكتبات نت، القاهرة، المجلد 4، العدد 3/4، أبريل 2003.
- د. بدر عمر العمر، الإنترنت التربوي: ماذا يجب على الطفل معرفته، مجلة الطفولة العربية، الكويت، المجلد 3، العدد 12، لسنة 2002.
- د. هاجر محمد علي حبة: أثر استخدام الإنترنت على الأطفال، مجلة التنمية البشرية، كلية التنمية البشرية، جامعة أم درمان الإسلامية، السودان، العدد 1، فبراير 2015.
- د. هبة محمد إسماعيل، معايير لتقييم مواقع الأطفال على شبكة الإنترنت، المؤتمر التاسع للاتحاد العربى للمكتبات والمعلومات (الاستراتيجية العربية الموحدة للمعلومات في عصر الإنترنت)، تونس، أكتوبر 1999.
- د. حسام الدين مصطفى علي، فريق الاستجابة لحوادث الكمبيوتر (CIRT) Team (Response Incident Computer، مؤتمر أمن المعلومات والحكومة الإلكترونية، المنظمة العربية للتنمية الإدارية، كوالالمبور، أبريل 2009.
- د. محمد عبيد سيف وعبدالناصر محمد محمود، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية: دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، 12-2007/11/14.
- د. محمد صديق محمد، الفضائيات والإنترنت مسؤولية مشتركة تجاه أطفالنا وشبابنا، مجلة التربية، دولة قطر، السنة 37، العدد 164، مارس 2008.
- د. محمد محمود عمري، الإثبات الجزائي الإلكترونى في الجرائم المعلوماتية: دراسة مقارنة، مجلة العلوم القانونية والسياسية، الجمعية العلمية للبحوث والدراسات الإستراتيجية، العراق، المجلد 12، العدد 2، لسنة 2016.
- د. محمود فتوح سعدات، خصائص الجرائم المعلوماتية وصفات مرتكبيها في ظل مجتمع المعلومات، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية (ICACC)، كلية

علوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية، الرياض،2015.

- المعجم الوسيط، ط4، مجمع اللغة العربية، الإدارة العامة للمعجمات وإحياء التراث، 2004، باب الحيطة.

- د. سهير العطار، الجرائم المستحدثة ضد الأطفال عبر النظم المعلوماتية: تحليل نصوص اتفاقية بودابست للمواد الخادشة للحياء، المؤتمر الإقليمي للطفل العربي في ظل المتغيرات المعاصرة، القاهرة، يناير 2004.

- د. عبدالرحمن محمد خليل أزهري، جمع وتوثيق وتحليل الأدلة الجنائية الرقمية بطرق أكثر فعالية، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية (ICACC)، كلية علوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية، الرياض، 2015.

- د. عبدالمطلب أحمد السماني، الحماية الأمنية من الأخطار المحتملة على شبكة الحاسب الآلي: دراسة مسحية تحليلية في مدينة الرياض، المجلة العربية للدراسات الأمنية والتدريب، المجلد 28، العدد 56، لسنة 2012.

- د. عادل يوسف عبدالنبى الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مجلة مركز دراسات الكوفة، العراق، العدد 2، لسنة 2011.

- د. عادل عبدالله خميس العمري، التفتيش في الجرائم المعلوماتية، مجلة الفكر الشرطي، مركز بحوث الشرطة، الشارقة، الإمارات، المجلد 22، العدد 86، يوليو 2013.

- د. علي أسعد وطفة، الطفولة العربية والصراع على المصير في استراتيجية البناء الثقافي للطفل العربي، مجلة شؤون عربية، القاهرة، العدد 119، لسنة 2004.

- د. علاء الدين يوسف العمري: المراهق والإنترنت: الفوائد والمخاطر، مجلة رسالة التربية، سلطنة عمان، العدد 6، ديسمبر 2004.

- د. عبدالحليم بن بادرة: إجراءات البحث والتحري عن الجريمة المعلوماتية: الخصوصية والإشكالات، مجلة الحقوق والعلوم الإنسانية، جامعة زيان بن عاشور، الجلفة، الجزائر، العدد 23، مايو 2015.

- د. قاسم الصراف، مؤتمر حماية الطفل من سوء المعاملة والإهمال: دولة البحرين، مجلة الطفولة العربية، الكويت، المجلد 3، العدد 9، لسنة 2001.

- د. راشد بن حمد البلوشي، الدليل في الجريمة المعلوماتية، مجلة الحقوق للعلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، القاهرة، العدد1، لسنة 2008.

## ثانياً– باللغة الأجنبية:


- A.T.Wood and Harrper Nimal Jayaratna: Methodologies for Developing and Managing Emerging Technology Based Information systems, Methodologies 1998، Sixth International Conference on Information Systems Methodologies, Springer-Verlag, London, 1999.
- Ammar Rayes and Samer Salam: Internet of Things - From Hype to Reality: The Road to Digitization, Springer International Publishing AG 2017, Library of Congress, USA.
- Babak Akhgar and Ben Brewster, Combatting Cybercrime and Cyberterrorism Challenges: Trends and Priorities, Advanced Sciences and Technologies for Security Applications, Springer International Publishing, Switzerland, 2016.
- George Christou, Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy, Macmillan Publishers Limited, 2016.
- John Domingue and Dieter Fensel, Handbook of semantic web technologies, Vol.1, Austria, 2011.
- Jorge Cardoso, Semantic Web Services - Processes and Applications: Semantic Web and Beyond Computing for Human Experience, Springer, USA, 2006.
- Liyang Yu: A Developer's Guide to the Semantic Web, Springer-Verlag Berlin Heidelberg, 2011.
- Luciano Floridi, Protection of Information and the Right to Privacy: A New Equilibrium?, Springer International Publishing, Switzerland, 2014.
- Michael Schumacher and Heikki Helin, Cascom: Intelligent Service Coordination in the Semantic Web, Birkhäuser, Berlin, 2008.
- Pompeu Casanovas and Ugo Pagallo and Giovanni Sartor and Gianmaria Ajani: Approaches to the Complexity of Legal Systems: Complex Systems - the Semantic Web- Argumentation and Dialogue, Springer-Verlag, Berlin Heidelberg, 2010.
- Russell G. Smith and Ray Chak-Chung Cheung and Laurie Yiu-Chung Lau: Cybercrime Risks and Responses: Eastern and Western Perspectives,

Macmillan Publishers Limited, UK, 2015.

- Saba Bebawi and Diana Bossio: Social Media and the Politics of Reportage - The 'Arab Spring', Palgrave Macmillan in the US is a division of St Martin's Press LLC، - 2014.
- Simone van der Hof and Bibi van den Berg, Minding Minors Wandering the Web- Regulating Online child safety, Information Technology and Law Series, Vol. 24, Springer, The Netherlands, 2014.
- Tom funk, Advanced Social Media Marketing: How to Lead, Launch and Manage a Successful Social Media Program Worldwide, Springer Science Business Media, New York, 2013.
- Wayne Graham, Beginning Facebook Game Apps Development: Create the Next Generation of Facebook Game and Social Media Apps Using html5 and Java Script, ED books, 2012.

## المحتوى:


| الموضوع | الصفحة |
|---|---|
| الملخص | 89 |
| المقدمة | 91 |
| المبحث الأول– مضمون الحيل الإجرائية المشروعة | 94 |
| المطلب الأول– ماهية الحيل الإجرائية المشروعة | 94 |
| الفرع الأول– الحيل الإجرائية المشروعة كبرامج تقنية | 95 |
| الفرع الثاني– الحيل الإجرائية كصلاحيات لرجل الضبط القضائي | 97 |
| المطلب الثاني– أهمية الاستعانة بالحيل الإجرائية المشروعة | 97 |
| المبحث الثاني– محاولة تأصيلية لصياغة قواعد إجرائية إلكترونية | 100 |
| المبحث الثالث– تهيئة البيئة المحلية لاستيعاب المعالجة الإجرائية الإلكترونية | 105 |
| المطلب الأول– ضرورة التحول القضائي لفهم متطلبات الدليل الرقمي | 105 |
| المطلب الثاني– إدارة مكافحة الجرائم الإلكترونية | 106 |
| المطلب الثالث– التشريعات القانونية ذات العلاقة | 108 |
| الخاتمة | 110 |
| المراجع | 113 |