# الوضع الحالي لتدريس وتطبيق أنظمة وتشريعات قوانين الجريمة الإلكترونية في المملكة العربية السعودية

**إعداد**

**اللواء د. حسن بن أحمد الشهري  د. صالح محمد العطيوي**

## مقدمـــــة

ساهمت الثورة التقنية وخصوصاً الابتكار في مجال الشبكة العالمية للمعلومات بإحداث تغييرات بطرق تأدية الأعمال لم بعهدها العالم من قبل في جميع القطاعات و تشمل القطاع الصحي والتعليمي والصناعي والتجاري والحكومي. و تكمن مميزات هذه الشبكة في تدعيم الأنشطة التي يقدمها كل قطاع وربط جميع فروعه لزيادة الكفاءة والفاعلية. ومن مميزاتها الإستراتيجية توفير منافذ الكترونية جديدة لتقديم المنتجات والخدمات بالإضافة لخدمة ما بعد البيع مما أدى إلى وزيادة درجة الرضا لدى عملاء هذه القطاعات من توفير للجهد والمال والوقت وإذابة المسافات وتعزيز العلاقة التجارية بواسطة التقنية الإلكترونية. وعلى الرغم من هذه المميزات إلا أن هناك تحديات تواجه تلك القطاعات خلال تدفق المعلومات داخل أو خارج المنظمة الذي قد يترتب عليه الاعتداء عليها إما بالسرقة أو الإطلاع أو التشويه أو الإتلاف. (Mellahi, Frynas and Finlay, 2005).

يقول ( Kalakata, 1998) أن سبب التحول المدهش الذي بدأ من عام ١٩٩٠ حتى وقتنا الحاضر تبني تقنية المعلومات في المنظمات مما ساهم في تعزيز عولمتها وانتشارها في مختلف دول العالم. ويؤكد ( Filos, 2005, Filos and Benahan, 2001 )أن الفضل في إيجاد المنظمات الافتراضية والتي لا تعترف بوجود الحدود بين دول العالم مصدره ثورة تقنية المعلومات والاتصال ( Information and communication Technology ). إن من سمات انتشار استخدام الشبكة العالمية للمعلومات نشوء المجتمعات الإلكترونية التي تعتمد في معاملاتها على هذا التطور في التقنية مما أدى إلى زيادة الاعتداء على الحقوق الفردية التي كفلتها الشرائع السماوية والتشريعات والأنظمة الأخرى. وهذا يؤكد حاجة الدول إلى سن الأنظمة والتشريعات التي توفر الحماية الكافية لتدفق المعلومات عبر الشبكة العالمية للمعلومات بين الدول أو بين المنظمات في الدولة الواحدة أو داخل المنظمة وفروعها.

**أهمية تقنية المعلومات للمنشأة**

تعتبر المعلومات من أهم المصادر للمنظمة الخاصة أو الحكومية وتمثل دم الحياة لتلك المنظمات، إن المعلومات الصحيحة تسهم في تقديم فرص المنافسة مع المنظمات الأخرى في هذا عصر. لا تقتصر أصول المنظمة على العناصر الملموسة فقط وإنما تشمل المعلومات التي تعتبر في الوقت الحاضر من أهم أصول المنظمة التي تمكنها من تبني استراتيجية معينة في الحاضر والمستقبل ( Elliott and Starkings, 1998 ). ويرى كل من ( **Elliott** and Starkings, 1998 ) أن نظم المعلومات الذي يتكون من مجموعة الأجزاء التقنية الموجودة في أنشطة المنظمة والتي تعمل على تخزين ومعالجة المعلومات تقدم خدمة عظيمة لصانعي القرارات. ويؤكد كل من (٢٠٠٣ Korpela, Mantea leper and Poulymenakou,) أهمية تقنية المعلومات والاتصال في عصر العولمة والتي تمكن المنشأة من الوصول إلى دول العالم لتقديم خدماتها ومنتجاتها و لم يكن لها القدرة على ذلك قبل عقد من الزمن.

ويبرز دور تقنية المعلومات والاتصال في تغيير استراتيجية المنشأة وإيجاد قاعدة أساسية للتجارة الإلكترونية التي تمكن المنظمة من البحث عن أسواق جديدة وتقديم خدمات ومنتجات جديدة للمستهلكين في مختلف أرجاء المعمورة، و تبرز أهمية دمج التقنية الحديثة في تخفيض تكلفة المنظمة وزيادة نموها وزيادة كفاءتها وفاعليتها ( Ada, 1999; Grpta and Sharma, 2004 ).

يذكر ( Chang , Tackson and Grover , 2003 ) الدور الذي قدمته تقنية المعلومات والاتصال في تغيير تأدية منشآت الأعمال للخدمات والمنتجات التي تقدمها، وذلك من خلال ما يعرف بالتجارة الإلكترونية. إن نجاح تلك التقنية مكنت المنشأة من ابتكار منافذ أخرى لتعزيز خدمات الزبائن وتقديم المنتجات والخدمات الرقمية. ويؤكد كل من (Iwwarden, Wicle , Ball and Millen , 2004 ) أن هناك نمواً متسارعاً وهائلاً في التجارة عبر الشبكة العالمية للمعلومات.

**أهمية الدراسة**

تعتبر المملكة من الدول التي تسعى الى دمج التقنية في جميع أعمالها سواء الحكومية أو الخاصة لما تتمتع به هذه التقنية من مرونة في الإستخدام وتقديم المعلومات في الوقت المناسب لمتخذي القرار، فإن الأمر يقتضي اصدار التشريعات اللازمة لحماية تلك المعلومات أثناء ابحارها داخل أو خارج المنظمة، ومدى المام العاملين في النظمة بتلك التشريعات، من خلال نتائج البحث سيتم تقديم التوصيات التي تدعم هذه الجوانب.

**الغرض من الدراسة**

إن الغرض من هذه الدراسة يكمن في مايلي:

١. معرفة مدى تدريس التشريعات والأنظمة المحلية والدولية الخاصة في الجريمة الإلكترونية في أقسام وكليات الجامعات في المملكة.

٢. معرفة مدى إلمام العاملين في القطاع الخاص والحكومي بتلك الأنظمة وتدرج عقوبة الجريمة الإلكترونية.

٣. استعراض أنظمة وتشريعات الجريمة الإلكترونية في دول العالم.

**مشكلة الدراسة**

بسبب الازدياد المستمر على دمج تقنية المعلومات في المنشآت العامة والخاصة، وتدفق المعلومات بين المنشآت وزيادة استخدام الشبكة العالمية للمعلومات والتي تعتبر العمود الفقري لهذه التقنية، هناك من المشاكل التي تواجه أو تحد من استخدامها والتي تكمن في مدى توفر الأنظمة والتشريعات التي تطبق في حالة الجريمة الإلكترونية، وإلمام العاملين بالأنظمة والتشريعات المحلية والدولية، وهل يتم تدريسها في كليات الشريعة والأنظمة بالمملكة.

## أسئلة الدراسة

١. هل يتم تدريس أنظمة وتشريعات خاصة بالجريمة الإلكترونية في كلية الشريعة في جامعة الإمام محمد بن سعود الإسلامية، وقسم الأنظمة في معهد الإدارة بالرياض؟ وهل أنواع الجرائم محددة في المنهج؟

٢. ما وجهة نظر عناصر العينة من القطاعين العام والخاص نحو سن أنظمة وتشريعات خاصة بالجريمة الكتروني في المملكة؟

٣. ما الحاجة لتدريس مادة خاصة في التشريعات والأنظمة الخاصة بالجريمة الإلكترونية في كليات الحاسب الآلي والمعلومات؟ ما أهمية تدريس مادة تقنية وأمن المعلومات في كليات الشريعة والقانون في المملكة؟

٤. هل يوجد لدى المنشآت أنظمة وتشريعات للجريمة الإلكترونية؟ وما مدى إلمام العاملين بالمنشآت بتلك الأنظمة والتشريعات؟

**صدق الإستبانة**

تم تصميم استبانتان الأولى موجهة إلى أعضاء هيئة التدريس والثانية موجهة إلى مديري تقنيات المعلومات بالقطاعين العام والخاص. كما قام الباحثان بعرضها على مجموعة من المحكمين في قسم وسائل وتكنولوجيا التعليم وكلية علوم الحاسب الآلي والأنظمة بجامعة الملك سعود بالرياض، للتأكد من صدق محتواهما بالنسبة لما تقيسه مفرداتها، و مدى وضوحها من الناحية اللغوية.

**الطريقة الإحصائية**

تم اختيار ر الطريقة الكمية في تحليل البيانات والتي تشمل الوسط الحسابي والانحراف المعياري. وتم اختيار العينة بطريقة عشوائية من أعضاء هيئة التدريس في كلية الشريعة بجامعة الإمام محمد بن سعود الإسلامية وقسم الأنظمة بمعهد الإدارة العامة بالرياض؛ ومديري تقنية المعلومات بالقطاعين العام والخاص على النحو الآتي:

جدول (١)

| | عدد الإستبانات الموزعة | عدد الإستبانات المستردة |
|---|---|---|
| كلية الشريعة بجامعة الإمام محمد بن سعود الإسلامية | ٣٠ | ٩ |
| قسم الأنظمة بمعهد الإدارة العامة بالرياض | ١٠ | ٤ |
| القطاع العام | ١٨ | ٩ |
| القطاع الخاص | ٢٥ | ٦ |

**حدود الدراسة**

سيتم تطبيق هذه الدراسة في المملكة وحدودها على النحو الآتي:

١. ستطبق في مدينة الرياض خلال الفترة من ١٤٢٧/11/١٠ – ١٤٢٧/١٢/١٥هـ.

٢. ستطبق على كل من: جامعة الإمام محمد بن سعود الإسلامية و معهد الإدارة العامة ومديري تقنية المعلومات في القطاع العام والخاص.

أدبيات الدراسة

**تعريف الجريمة الإلكترونية**

ويعرف الباب الثالث من المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية منتهك الحاسوب هو " الشخص الذي يخترق حاسوب محمي ( مشمول بالحماية ) دون أن يكون مصرح له بذلك " ( يونس صـ ٣٩٢ ) .

**العلاقة بين التقنية والأنظمة والتشريعات**

يؤكد ( Casey, 2000 ) أن الحاسب الآلي يستخدم كأداة لتأدية الأنشطة المختلفة، كما أن البنية التحتية للمجتمع في الوقت الحاضر مؤسسة على الحاسبات الآلية والشبكات المحلية والعالمية لتأدية جميع العمال، وعلى الرغم من ذلك لا يوجد الانتباه الكافي لتلك الأعمال التي يؤديها. وتعتبر تقنية المعلومات المحور الأساسي للأعمال البنكية، والجوانب الصحية ومحطات الطاقة . ومن الاستخدامات القردية لتشمل التعليم والتسلية وإدارة النواحي المالية للفرد ومن الممكن ربط الحاسب الشخصي بالشبكات المحلية أو العالمية للحصول على مميزات أخرى. وزيادة الإعتماد على التقنية مؤشر الى الزيادة في الجرائم الإلكترونية.

ويذكر أن الأشخاص المسؤولين عن تطبيق القانون يجب أن يغيروا من معارفهم ومهاراتهم نحو التغير في البيئة التقنية حتى يكون هناك توافق بين القوانين والبيئة الجديدة التي تعتمد على التقنية في أعمالها اليومية، إن الفهم القوي للأمور التقنية والتشرعية لتطوير تلك البيئة الغير مألوفة أصبح ضرورياً للتمكن من جمع الشواهد والبيانات المقبولة بواسطة المحكمة ( Casey, 2000 ).

يذكر ( Vallabhaneni, 1989 ) كلما بدأ اعتماد المنظمة على استخدام الحاسبات الشخصية في جميع أوجه أنشطتها بدأت زيادة فرصة نمو الجريمة الإلكترونية التي تشمل إساءة استخداما المعلومات والخداع والاحتيال للوصول للمعلومات هناك أشخاص يسعون إلى تدمير المعلومات بغرض اللهو والتسلية أو لأسباب أخرى كما سبق ذكرها.

**خاصية الجريمة الإلكترونية**

الجريمة الإلكترونية غير ملموسة بين الجرائم الأخرى الملموسة فإن الدليل الخارجي موجودة آثاره مثل السرقة والقتل ، أما لجريمة الإلكترونية لا يوجد أثراً ملموساً وإنما تتم من خلال الوصول إلى المعلومات، وإتلافها أو سرقتها ، ويذكر ( العريان ٢٠٠٤ ) " فالجرائم المعلوماتية لا عنف فيها ، ولا سفك دماء ولا آثار اقتحام لسرقة الأموال... فإن جرائم المعلوماتية لا هي جرائم فنية تتطلب تكتيك معين في مجال الحاسبات الآلية ، وهي جريمة هادئة لا تتطلب العنف ( ص ٥٣٠ ). في حقيقة الأمر أن الجريمة الإلكترونية مثل الجرائم الأخرى مثل السرقة والقتل العمد لأن الجريمة

الإلكترونية لا تكون بمحض الصدفة ولكن تحتاج إلى التخطيط والمعرفة الفنية باختراق الحواجز الأمنية وتدميرها والوصول إلى المعلومات والبيانات الخاصة بالمنشأة التي تمثل قوة اقتصادية لها وإتلافها ويؤدي إلى انهيارها أو الوقت لإصلاح الضرر وفقد جزء من الأرباح ، أو تحقيق خسائر عندما يكون هناك حماية إلكترونية للمعلومات التي تتدفق عبر الشبكة المحلية أو العالمية للمعلومات ، ومن ثم يتم الاعتداء عليها ، يعتبر مثل الاعتداء على أحد البنوك وسرقة الموجودات في الخزينة ، يذكر ( الصغير ، ١٩٩٢ ) أن الجريمة الإلكترونية لا يوجد لها حدود معينة بل يمكن إرتكابها من أي مكان في العالم ولا يحتاج المجرم إلى بذل الجهد والانتقال من مكان لآخر لتنفيذ جريمته بل يتمتع بكافة الأمان النفسي والراحة التامة عند تنفيذها .

يذكر( العريان ، ٢٠٠٤م ) " أن الشخص الذي يرتكب الفعل غير المشروع ويعتدي فيه على حق من حقوق الغير بالمعنى الواسع ، يعد في نظر القانون مجرماً ويتعرض للعقاب إذا ما اقترف جريمته " ( صـ ٦١٠ ، ٢٠٠٤ ) . ويذكر كل من ( Carter and Katz , 1996 ) أن الشواهد الرقمية ( Digital Evidence) تشتمل أي بيانات رقمية التي تؤكد وقوع الجريمة أو تقديم رابط بين الجريمة والضحية أو بين الجريمة ومرتكبوها. ويوضح ( Casey 2000 ) أن البيانات الرقمية تشمل النّص والصور والصوت والفيديو.

**أنواع الجرائم الإلكترونية**

يذكر ( Casey, 2000 ) أن جرائم الحاسب الآلي والشبكة العالمية للمعلومات تنوعت وشملت الآتي : الخلافة والفسق وإغراء القصر على أداء أعمال الجريمة والتحرشات والانتهاكات والتحايل والتجسس والتخريب والتدمير وتشويه سمعة الآخرين ( ص . ٥ ). إن الجرائم الإلكترونية تهدف إلى الإساءة للبيانات والمعلومات الموجودة على الشبكة العالمية للمعلومات والخاصة بشركة معينة ، ومن أنواع تلك الإساءة الإلكترونية محو المعلومات أو تغييرها أو تبديلها أو إلغائها أو تعديل مسارها( الشوابكه ، ٢٠٠٤ ). إن العمل الإجرامي استفاد من تقنيات الاتصال والمعلومات الحديثة وبصورة سريعة.

أشار ( Castells, 1996, 1998 ) أن هناك مجموعة المؤثرات على الاقتصاد العالمي في الوقت الحالي ومن أهمها تقنية المعلومات والاتصال التي لها الأثر الكبير في نمو ربحية المنشآت الناتجة من إتاحة الفرص لها للتواجد في الأسواق العالمية . ومع زيادة النمو في تبني تلك التقنية في جميع الأنشطة التجارية وغيرها مما أدى هذا التطور السريع في تلك التقنية وزيادة استخدامها من جميع منظمات المجتمع إلى خلق ونمو نوع آخر جديد من الجرائم الذي يعرف بالجرائم الإلكترونية. كما يذكر( Castells, 1998 ) أن تقنية المعلومات والاتصال أدت إلى خلق المناخ والبيئة المناسبة للمنشآت العالمية لمزاولة أنشطتها، وما حققته من تجاوز للحدود الدولية والتنظيمات الخاصة بالدول وتقليص التحكم الفردي، وهذا التقدم أوجد مناخاً ملائماً لنشوء شبكة من الجرائم الإلكترونية الدولية المنظمة والعابرة للقارات .

ويؤكد كل من ( Thomas and Loader, 2000 ) أن الترابط العالمي الذي تحقق بواسطة الإنترنت سهّل عملية نمو أنشطة المجرمين عبر حدود الدول لمزاولة الأعمال الغير مشروعة، وعملت على إمكانية تنظيم الجريمة الإلكترونية واستخدام أساليب محكمة وتقنية وتطوير الشبكات الإجرامية مثل المخدرات وغسيل الأموال.

ويذكر ( Gallagher , 1998 ) مساعد مدير التحقيقات الفيدرالية الأمريكية ( FBI) ذكر أن الشبكة العالمية للمعلومات تبيح أنواعاً من الجرائم الغير منتهية مثل الخداع والتحايل والقرصنة التي لها التأثير على أداء المنشآت .

وأشار ( Thomas and Loader, 2000 ) أن التهديدات الحقيقية للمنظمات التجارية تأتي من قبل تجسس الشركات الصناعية ، وتقدم تقنية المعلومات والاتصال فرصة جديدة للقراصنة للحصول على المعلومات الخاصة بتطوير المنتجات واستراتيجيات التسويق والجوانب التجارية الأخرى التي تتمتع بالسرية ومن ثم بيعها للمنافسين . ويؤكد ( Thomas and Loader, 2000) أن القوانين تنظر للمجرم الذي نادراً ما يستخدم تقنية المعلومات والاتصال ليس بأقل من المجرم الذي يستخدم هذه التقنية الحديثة لتنفيذ جرائمه وأورد مثالاً يذكر فيه أن اللذين يستخدمون الحاسب الآلي وشبكة المعلومات العالمية للإعتداء على الآخرين لا تختلف نهائياً على الاعتداء على الآخرين باستخدام الهاتف وجهاً لوجه أثناء المحادثة ، ويؤكد أن استخدام البريد الإلكتروني أو الشبكة العالمية للمعلومات للاعتداء على الآخرين من سب أ و مس العرض واستخدام الإنترنت لنشرها إلى أوسع نطاق لكونها استخدام تلك التقنية رخيصة جداً أو باستخدامها باسم

شخص مجهول فإن هذه تعتبر جريمة ولا تنسب تلك الجريمة إلى الأدوات التي استخدمت ( ص ٦٠ ) ويذكر أن الجرائم تغيرت مع نمو وتزايد استخدام تقنية المعلومات والاتصال .

فقدان المعلومات وأثرها على المنظمة

التنظيم عرضة لفقد المعلومات وبالتالي فقد الفرص التنافسية، ويمكن قياس مدى تدرج تلك المخاطر التي يمكن أن تدمر المعلومات من المتوسط إلى ا لهائل حسب ماذكره وتشمل هذه المخاطر:(Vallabhaneni, 1989)

١. فقدان المبيعات أو العوائد .
٢. فقدان الأرباح .
٣. فقدان المعلومات الشخصية .
٤. الفشل في تحقيق المتطلبات الحكومية أو القانونية .
٥. عدم القدرة على خدمة العملاء .
٦. عدم القدرة على تعزيز النمو .
٧. عدم القدرة على تحقيق الفاعلية والكفاءة في التنظيم (صـ ٩٨٩).

أثر الجريمة الإلكترونية

يذكر ( Vallabhaneni, 1989 ) أن المنظمة الأمريكية American Bar Asso Ciation (ABA) أجرت دراسة عن جرائم الحاسب الآلي على مجموعة من التنظيمات العامة والخاصة وبلغ عددها ١٠٠٠ وتشمل البنوك وشركات التأمين والشركات الحاسبية وشركة الخدمات المالية وشركات الحاسب الآلي والإلكترونيات وكانت نتيجة الدراسة تشير إلى ما يلي : ٢٥% من تلك الشركات قدرت خسارتها ما بين ١٤٥ مليون دولار إلى ٧٣٠ مليون دولار.

## الأنظمة والتشريعات الخاصة في الجريمة الإلكترونية

سيم استعراض الأنظمة والتشريعات الخاصة بالجريمة الإلكترونية في مجموعة من الدول. يذكر ( الشـــوابكة ، ٢٠٠٤ ) أن المشرع الفرنسي أصدر القانونين الخاصة بحماية المعلومات على الشبكة العالمية للمعلومات والتي تكون محـــلاً للاعتـــداء . ويضيف أن المشروع الأمريكي أصدر القوانين الخاصة في التصدي للجرائم باستخدام تلك التقنية . ويوقع العقوبة علـــى جرائم القذف والسب وانتهاك الآداب العامة .

يذكر Lessiy, أن تقنية المعلومات والاتصال لها دور فعال في خلق فرع آخر من القانون ذو أهمية بالغـــة في وقتنـــا الحاضر لحماية المعلومات والبيانات المتدفقة عبر الشبكة العالمية للمعلومات . ويذكر ( يـــونس،٢٠٠٤ ) دور الولايـــات المتحدة الأمريكية في تطوير قوانين لحماية العالم الافتراضي ( Cyber law ) وهذا العمل بدأ منذ عـــام ١٩٩٤م لفـــرض تقنين جرائم تقنية المعلومات ومنذ ذلك التاريخ بدأت تطوير هذه الأنظمة من فترة لأخرى. يذكر ( الشوابكه ، ٢٠٠٤ ) إن الجرائم المرتكبة عبر [ الشبكة العالمية للمعلومات ] تعد من الموضوعات الحديثة التي فرضت نفسها علـــى المســـتوى الوطني والدولي على حد سواء ، والتي ينبغي على المشرع الجنائي مواجهتها بتشـــريعات حاسمـــة لمكافحتـــها وعقـــاب مرتكبيها.

يقول (Lilley, 2002) أتمنى أن التشريعات عبر العالم خاضعة للتغيير المستمر وبما يتناسب مع التحديات الناتجـــة مـــن العصر الرقمي، ويوجد بعض الدول التي لم تسن التشريعات الدقيقة المتعلقة بانتهاك المعلومات الموجـــة علـــى الشـــبكة العالمية للمعلومات أو المخزنة في أدوات التخزين المختلفة وكذلك أثناء انتقالها عبر تلك الشبكة.

## الولايات المتحدة الأمريكية

يذكر ( يونس ، ٢٠٠٤ ) أن نظام الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي حريص على حمايـــة الحريـــة الفردية ولا يجوز التفتيش إلا بإذن مسبق ويجب أن يتوافر لدى الجهات المختصة سبباً معقولاً لإجراء التفتيش . إن تفتيش

الملفات الإلكترونية تعتبر من الأمور المعقدة والتي لا يمكن مقارنتها بالأشياء المادية المحسوسة مثل المنـــازل والســـيارات . لأن هذه الملفات الإلكترونية يمكن تخزينها في أماكن مختلفة أو بأسماء وهمية أو في أماكن مختلفة مـــن العـــالم في خـــادم ( Server ) وسهولة تحريكها من أي مكان في العالم. لذا فإن منا لمتطلبات الرئيسة في رجال الضبط القضائي القدرة على معرفة الأساليب التقنية التي يمكن بواسطتها التفتيش والتخطيط له. إن تفتيش أجهزة الحاسب الآلي تحتاج للمهارة اللازمة التي تمكن رجال الضبط القضائي من نجاح التفتيش .

إن نجاح عملية تفتيش الملفات الإلكترونية يتطلب توافر العناصر الآتية :

١. يتألف الفريق من ثلاثة أشخاص رجل الضبط القضائي الموكل إليه تلك القضية والخـــبير المخـــتص في تقنيـــة المعلومات والمدعي العام.

فإن الأمر يتطلب من رجل الضبط القضائي تنظيم وتوجيه التفتيش ويكون على علـــم بـــالأجهزة أو الجهـــاز الحاسوبي المراد تفتيشه . أما المدعي العام هو الشخص الذي يحدد السبب المعقول لتفتيش هذا الجهاز ويتأكـــد من أن إذن التفتيش يتوافق مع القوانين الفدرالية أما الخبير الفني هو القائد ويمثل الشخص الرئيسي في الجوانـــب الفنية ويحدد فنياً ما هي الأجزاء التي سيتم تقنيتها للحصول على الأدلة . إن التعاون بين هؤلاء الأشخاص أمـــر ضروري لضمان الوصول للأدلة ( يونس ، ٢٠٠٤ ).

إن نظام الولايات المتحدة الأمريكية يسمح للأشخاص أو المؤسسات التي تم الاعتداء على حواسيبهم بتفـــويض السلطات لمراقبة تحرك المعتدين وبالتالي تتولى السلطة متابعة اتصالات المعتدي التي يبثهـــا إلى تلـــك الأجهـــزة المحميـــة Protected Computer وعند طلب التفتيش بواسطة المعتدى عليه لا بد من توافر الآتي :

١. يجب أن يخول المعتدى عليه لمراقبة المعتدي ومن الأفضل الحصول على موافقة كتابية منه أو من وكليه.

٢. يجب أن يكون المراقب لتلك الاتصالات عضواً في لجنة التحقيق.

٣. يجب أن تتوافر لدى مراقب الاتصالات المعرفة حتى يتمكن من أن الاتصالات التي تحدث لها علاقة في الجريمة.

٤. يجب أن تكون المراقبة خاصة بالاتصالات من وإلى منتهك الحاسوب ولا يتم مراقبة اتصالات أخـــرى . و في حالة عدم القدرة على تفادي الاتصالات الأخرى المسموح بها للمستخدمين لتلك الأجهزة فإنه يجـــوز لهـــم مراقبة جميع الاتصالات ( يونس، ٢٠٠٤ ).

عندما يسفر التحقيق عن وجود الدليل الإلكتروني خارج حدود الولايات المتحدة الأمريكية تخزن في أي جهاز حاســـوبي أو بواسطة متردد الخدمة فإن الولايات المتحدة تسعى للحصول على الدليل من الدول بواسطة رجال الضـــبط القضـــائي ويتم ذلك على النحو الآتي :

١. موافقة الدولة الأجنبية على التحقق مع متردد الخدمة أو صاحب ذلك الجهاز.

٢. موافقة Office of International Affair ( OIA) مكتب الشئون الدولية مع وزارة العدل الأمريكية .

أشار كل من ( الشوابكه، ٢٠٠٤، Smedinghoff,1996) أن الولايات المتحـــدة الأمريكيـــة ســـنت القـــوانين والتشريعات اللازمة لحماية تدفق المعلومات عبر الشبكة العالمية للمعلومات والحاسوبات المحميـــة . وتم تحـــدد الجـــرائم الإلكترونية بواسطة المشرع الأمريكي على النحو التالي:

١. من يتجاوز الصلاحيات المخولة له بالدخول للحاسب الآلي أو الدخول العمد الغير مصرح به وحصل بناء عليه على معلومات تسئ إلى الولايات المتحدة الأمريكية وتم نقلها عمداً لدول أجنبيـــة بغـــرض إلحـــاق الضـــرر بالولايات المتحدة أو تسليمها لأشخاص آخرين أو الاحتفاظ بها أو عدم تسليمها إلى الأشـــخاص المخـــولين باستلامها .

٢. الوصول إلى الحاسبات المحمية بمعرفة وبقصد الغش بدون إذن شرعي أو يتجاوز هذا الإذن ويحصل على شـــئ ذا قيمة وأن قيمته لا تزيد عن ٥٠٠٠ دولار.

٣. كل من يلج إلى حاسب آلي محمي وبدون إذن شرعي ويكون من نتائجه الإضرار بالمنشأة.

٤. التهديدات الخاصة بالحاسبات المحمية والذي له دور في التأثير على نقل أو أي اتصالات خاصة بالتجـــارة بـــين الدول أو التجارة الخارجية الأمريكية.

إن العقوبات التي حددها المشرع الأمريكي لمرتكبي الجرائم الإلكترونية تشمل الغرامة أو الحبس وقد يصـــل الســـجن إلى عشر سنوات أو بهما معاً.

**استراليا**

١. الشخص الذي يدخل لأنظمة الحاسب الآلي من غير أذن شرعي ويتمكن من

الوصول إلى :

أ- البيانات الموجودة في الحاسبات الخاصة بدول الكومنولث أو

ب- البيانات الخاصة بدول الكومنولث ومخزنة في حاسبات أخرى لا تنتمي لهذه الدول، يعتبر هذا الشخص متهم ومنتهك للقوانين ويستحق عقوبة السجن لمدة ستة أشهر.

٢. الشخص الذي:

أ. لديه النية في التحايل وبدون تفويض شرعي للدخول للبيانات في أجهزة حاسبات دول الكومنولث أو البيانات المخزنة والخاصة في دول الكومنولث في حاسب آخر ليست خاصة بتلك الدول أو

ب. لديه النية وبدون أذن شرعي للوصول للمعلومات المخزنة في حاسبات دول الكومنولث أو البيانات المخزنة في حاسبات غير خاصة بتلك الدول ويعلم هذا الشخص بهذه المعلومات وبما لا يدعوا للشك أيضاً خاصة في:

١. الأمن والدفاع أو علاقة استراليا بالدول الأجنبية.

٢. مصدر سري للمعلومات ذات علاقة بتقرير وتنفيذ قوانين الجريمة في دول الكومنولث أو أي دولة أو مقاطعة.

٣. أمن وسلامة الجمهور.

٤. بالخاصة بالأفراد.

٥. أمن التجارة.

٦. سجلات المؤسسات المالية.

٧. كشف المعلومات التجارية والتي سعيت في الإساءة لأي شخص في هذه الحالة يعتبر متهم وعقوبتها السجن لمدة سنتين (Lilley, 2002).

**كندا**

ينص نظام الجريمة رقم ٣٤٢٠١ على ما يلي:

١. كل فرد يحتال أو يدون وجهه حق:

أ. الحصول بطريق مباشر أو غير مباشر على خدمات الحاسب الآلي بواسطة

ب. أدوات الكترومغناطيسية أو سمعية أو ميكانيكية أو أي أدوات تعترض أو تسبب بطريقة مباشرة أو غير مباشرة أي خلل لوظائف نظام الحاسب الآلي.

ج. استخدام أو حيازة أو السماح لشخص آخر باستخدام الرقم السري التي تمكن الشخص من الوصول للمعلومات.

يعتبر الفرد مدان نتيجة لانتهاكاته ويستحق عقوبة السجن لمدة لا تتعدى عشر سنوات (Lilley, 2002).

**جمهورية الصين**

أصدر جمهورية الصين أنظمة حماية أمن معلومات الحاسب الآلي وتشمل :

يعاقب الفرد بمبلغ ٥٠٠٠ ين والتنظيم ١٥٠٠٠ عندما يتم استخدام فيروسات لتدمير المعلومات أو أي معلومات أخرى تؤثر على نظام المعلومات أو في حال بيع أي أنظمة حماية لأنظمة المعلومات بدون أذن للحصول على دخل غير شرعي فالعقوبة المفروضة عليه تكون من مرة إلى ثلاثة مرات مماثلة للدخل غير الشرعي الذي حصل عليه( Lilley, 2002).

**هنج كونج**

ينص نظام الاتصالات جزء رقم 21A كل من يصل للمعلومات الموجودة بالحاسب الآلي من غير أذن شرعي بواسطة وسائل الاتصال الموضحة على النحو الآتي:

أ. أي شخص يملك المعرفة أو وسائل الاتصال التي تسبب تنفيذ أي عملية بواسطة الحاسب الآلي للحصول على دخول غير شرعي لأي برنامج أو معلومات موجودة بالحاسب يعاقب يبلغ وقدره ٢٠٠٠٠ دولار أمريكي

الجزء رقم ١٦١ الدخول للحاسب الآلي يقصد خيانة الأمانة أو الجريمة وينص على:

أي فرد يحل على أذن الدخول للحاسب الآلي :

١. يقصد الإساءة .

٢. يقصد الخداع وخيانة الأمانة .

٣. الحصول مكاسب للفرد نفسه أو شخص آخر .

٤. الذي يتسبب في خسارة للآخرين في نفس الوقت نتيجة لحصوله على الدخول غير الشرعي أو في الاستخدام المستقبلي يعاقب بالسجن لمدة تصل إلى خمس سنوات(Lilley, 2002).

**الدنمارك:**

ينص التشريع الدنمركي بالجزء رقم ٢٦٣

١. أي شخص يحصل على الدخول غير الشرعي للمعلومات أ، البرامج التي تخص السفير التي تستخدم في معالجة البيانات فالعقوبة المستحقة غرامة والسجن لمدة تصل إلى ستة أشهر(Lilley, 2002).

**فرنسا**

ينص التشريع الوارد في الجزء رقم III الخاص في الاعتداء على المنظمة المعلومات :

١. أي نشاط من شأنه التحايل على النظام الآلي والدخول إلى جميع أجزاء النظام أو جزء منه يعاقب بالسجن لمدة تصل إلى سنة وغرامة تصل إلى ١٠٠.٠٠٠ فرنك فرنسي.

وإذا نتج عن ذلك مسح البيانات أو المعلومات أو تعديلها فإن المجرم يعاقب بالسجن لمدة سنتين وغرامة تصل إلى ٢٠٠.٠٠٠ فرنك فرنسي.

٢. أي نشاط يعيق أو يعطل أو يدمر وظائف النظام الآلي تنص المادة بالسجن لمدة ثلاث سنوات وعقوبة تصل إلى ٣٠٠.٠٠٠ فرنك فرنسي .

٣. أي نشاط إلى تقديم بيانات إلى النظام معالجة العيانات أو التحاليل لطمسها أو تعديلا فالعقوبة تصل للسجن لمدة ثلاث سنوات وغرامةمالية تصل إلى ٣٠٠.٠٠ فرنك فرنسي.

٤. أي مشاركة جماعية أو اتفاق للتعامل أو التعاون فكرياً بواسطة أنشطة مادية يتم تطبيق ما ورد في المواد ١، ٢ ، ٣.

(Lilley, 2002).

**ألمانيا**

ينص القانون الألماني الخاص بأنظمة المعلومات على النحو الآتي :

١. أي شخص يدخل للنظام بدون أذن شرعي بنفسه أو بشخص آخر ويحصل على بيانات ليس خاصة به ومحمية ضد أي شخص غير مفوض للدخول إليها يسجن لمدة لا تجاوز ثلاث سنوات أو الغرامة.

٢. ينص النظام رقم ٣٠٣٦

يعاقب بالسجن لمدة تصل إلى خمس سنوات أو الغرامة لأي شخص يتدخل في معالجة العيانات التي تعتبر ضرورية ومهمة لقطاع الأعمال الأخرى أو الشركات (Lilley, 2002).

**ايرلندا**

ينص النظام الإيرلندي المدون في الجزء الخامس :

١. الشخص الذي يدخل للحاسب الآلي بدون إذن شرعي على النحو الآتي :

أ. داخل الدولة ويكون له النية للدخول لأي معلومات داخل أو خارج الدولة، أو

ب. الأشخاص من خارجه الدولة ولديهم النية بالدخول بدون أذن شرعي للمعلومات المحفوظة داخل الدولة

يكون الفرد مذنب سواء دخل للمعلومات أو لم يتم ذلك ويعاقب بغرامة مالية لا تتعدى ٥٠٠ جنيه إسترليني أو السجن لمدة لا تتجاوز ثلاثة أشهر أو يهما معاً(Lilley, 2002).

**الهند**

ينص نظام الاعتداء على أنظمة المعلومات على النحو الآتي :

١. أي شخص لديه النية أو المعرفة أنه من المحتمل أن يتسبب في فقدان أو تدمير المعلومات الخاصة بالجمهور أو أي شخص يسعى لمسح أو تغيير أي معلومات موجودة في مصادر الحاسب الآلي أو يقلل من قيمتها أو منفعتها أو التأثير عليها بواسطة أي أداة.

٢. أي فرد يسعى للاعتداء على أنظمة المعلومات يعاقب بالسجن لمدة تصل إلى ثلاث سنوات وبغرامة لا تتعدى ٢٠٠٠٠ روبية أو يهما معاً (Lilley, 2002).

**اليابان**

ينص قانون حماية أجهزة الدخول للحاسب الآلي الصادر في ١٩٩٩ رقم ١٢٨ على النحو الآتي :

١. أي نشاط يساهم في تأمين الدخول لأنظمة التشغيل الخاصة بحاسب إلى محدد وتتوافر فيه الحماية والتمكن في مدخلاته بواسطة خطوط الاتصالات أو أي معلومات شخصية لفرد آخر وبالتالي يعمل التمكن في وظائف الجهاز.

٢. أي نشاط يساهم في تأمين الدخول لأنظمة التشغيل الخاصة بحاسب إلى محدد وتتوافر فيه الحماية والتمكن في مدخلاته بواسطة خطوط الاتصالات أو أي معلومات (باستثناء المعلومات السرية الخاصة بالمستخدم) أو أي أوامر التي تؤدي إلى تجاوز الحماية والدخول غير المشروع بواسطة وظائف التمكن بواسطة استخدام محدد.

٣. أي نشاط يساهم في تأمين الدخول لأنظمة التشغيل الخاصة بحاسب آلي محدد المحمي بواسطة أجهزة حماية محملة في جهاز آخر والمربوط بأجهزة اتصالات أو معلومات أو أوامر تؤدي إلى الوصول للمعلومات في الجهاز الآخر.

٤. لا يحق لأي شخص تزويد الشخص الآخر بالمعلومات السرية الخاصة بالدخول الشرعي لأنظمة الحاسب الآلي.

٥. أي شخص يقوم بأي عمل من الأعمال السابقة ١-٣ يستق السجن لمدة لا تزيد عن عام وبغرامة مالية لا تتجاوز ٥٠٠.٠٠٠ ين.

٦. أي شخص يخالف أو يخترق المادة رقم ٤ يعاقب بغرامة لا تتجاوز ٣٠٠.٠٠٠ ين.

**ماليزيا**

١- أي شخص يكون مدين في الحالات الآتية:

أ. الذي يتسبب في تشغيل أي وظيفة حاسب آلي بقصد الوصول غير المشروع إلى معلومات آمنة أو برامج موجودة في أي حاسب آلي.

ب. الدخول إلى أنظمة الحاسب الآلي المحمية وبدون تفويض شرعي.

ج. عندما يعلم في وقت الدخول لأنظمة الحاسب ويتسبب في تشغيل وتنفيذ وظائف الخاصة بحالة معينة.

٢- تكون العقوبة بالغرامة المالية التي تصل إلى ٥٠٠٠٠ ربخت أو السجن وبحد أقصى خمس سنوات أو يهما معاً (Lilley, 2002).

**الإمارات العربية المتحدة ــ أمارة دبي**

١. أصدرت أمارة دبي أنظمة خاصة في الجريمة الإلكترونية ٣٠ ذي القعدة ١٤٢٢ هـــ، وتنص على:

٢. يعاقب كل من أفشى متعمداً المعلومات أو المستندات أو المراسلات الإلكترونية المؤتمن عليها بحكم السلطات الممنوحة له بالحبس و بغرامة لا تتجاوز ١٠٠.٠٠٠ درهم أو بإحداهما. وعندما يتم إفشاء هذه المعلومات بسبب الإهمال يعاقب بغرامة لا تتجاوز ١٠٠.٠٠٠ درهم.

٣. عندما يتم استخدام وسيلة الكترونية لتنفيذ جريمة فإن العقوبة تنص على الحبس لمدة لا تتجاوز ستة أشهر، وبغرامة مالية لا تتجاوز ١٠٠.٠٠٠ درهم، وعندما يكون هناك عقوبة أشد في أي قانون آخر يتم الأخذ بالعقوبة الأشد والتي تزيد على العقوبة المنصوص عليها في هذه المادة (الفريق العربي للأمن والحماية المعلوماتية، ١٤٢٨)

كما أصدرت الإمارات العربية تشريعات خاصة بالجريمة الإلكترونية ويعتبر القانون ألإتحادي لعام ٢٠٠٦ و ينص على ما يلي:

أ. يعاقب بالسجن مدة سنة وغرامة لا تقل عن ٥٠ ألف درهم لأي شخص اعتدى على القيم والمبادئ الإسلامية أو من اعتدى على الحياة الخاصة أو العائلية بنشر الصور أو اعتدى على حرمتها.

ب. كل من استخدم الوسائل التقنية للاستيلاء على أموال الغير مثل سرقة بطاقة الفيزا يعاقب بالسجن لمدة سنه وغرامة ثلاثين درهم.

ج. يعاقب كل من يحول أموال غير مشروعة بالسجن مدة لا تزيد عن سبع سنوات وغرامة لا تقل عن ثلاثين ألف درهم ولا تزيد عن مائتي ألف درهم.

د. في حالة اختراق المواقع تكون العقوبة على النحو الآتي:

ـــ يعاقب بالسجن مدة ستة أشهر وغرامة لمن يتلف بيانات الموقع.

ـــ يعاقب بالسجن مدة لا تقل عن سنة وغرامة عشرة آلاف درهم.

ـــ يعاقب بالسجن والغرامة لكل من يزور المعلومات المتدفقة في نظم المعلومات.

ـــ يعاقب بالغرامة مدة لا تزيد عن عشر سنوات و الغرامة لكل من يستخدم شبكة المعلومات أو وسائل تقنية المعلومات لابتزاز أي شخص.

ـــ يعاقب بالسجن لمدة لا تقل عن سنة وغرامة لا تتجاوز ثلاثين ألف درهم لمن يتجسس على الرسائل الإلكترونية وحسب أهمية تلك الرسائل (الفريق العربي للأمن والحماية المعلوماتية، ١٤٢٨).

**المملكة العربية السعودية**

لا يوجد أنظمة خاصة و محددة بالنسبة لجرائم الحاسب الآلي والشبكة العالمية للمعلومات لمعاقبة تلك الجرائم المتنوعة والمتطورة في ضوء التقدم التقني الذي ساد العالم، ولكن يوجد بعض النصوص الواردة في بعض الأنظمة، وتستخدم في تطبيقها على تقنية المعلومات ومن هذه الأنظمة قواعد ترخيص مقدمي خدمة الإنترنت الصادر من مدينة الملك عبد العزيز للعلوم والتقنية والذي ينص في بند الالتزامات العامة على ما يلي:

١. الإمتناع عن الوصول أو محاولة الوصول إلى أي من أنظمة الحاسبات الآلية الموصولة بشبكة الإنترنت أو إلى أي معلومات خاصة أو مصادر معلومات دون الحصول على موافقة المالكين أو من يتمتعون بحقوق الملكية لتلك الأنظمة أو المعلومات أو المصادر.
٢. الإمتناع عن استخدام الشبكة لأغراض غير مشروعة - ومن ذلك على سبيل المثال لا الحصر الرذيلة والقمار – أو القيام بأية نشاطات تخالف القيم الاجتماعية و الثقافية والسياسية والإعلامية والاقتصادية والدينية للمملكة العربية السعودية.
٣. الامتناع عن الإخلال بأي من حقوق النشر والتأليف أو حقوق الملكية الفكرية لأية معلومات أو مصادر.
٤. الإمتناع عن استخدام الشبكة بما يسبب الإزعاج أو التهديد أو نشر الإشاعات لأي شخص أو جهة أياً كانت.
٥. الإمتناع عن إرسال أو استقبال معلومات مشفرة إلا بعد الحصول على التراخيص اللازمة من إدارة الشبكة المعنية.
٦. الامتناع عن الدخول إلى حسابات الغير أو محاولة استخدامها بدون تصريح.
٧. الامتناع عن إشراك الغير في حسابات الاستخدام أو اطلاعه على الرقم السري للمستخدم.
٨. الالتزام باحترام الأنظمة الداخلية للشبكات المحلية والدولية عند النفاذ إليها.
٩. الامتناع عن تعريض الشبكة الداخلية للخطر بفتح ثغرات أمنية عليها.
١٠. الامتناع عن الاستخدام المكثف للشبكة بما يشغلها دوماً ويمنع الآخرين من الاستفادة من خدماتها.
١١. الالتزام بما تصدره الوحدة من ضوابط وسياسات لاستخدام الشبكة.

و لم يتم تحديد العقوبة في حالة انتهاك أي من هذه العناصر ما عدا حقوق الملكية الفكرية.

**أهمية إعداد فني شرعي**

يعتبر النواة الرئيسية التي تقدم المصادر والمبادئ و البراعة التي تساعد في التحقيق واتخـــاذ الإجـــراءات القانونية الخاصة بالأعمال الإجرامية . العلماء الشرعيين يستخدمون تدريباتهم لمساعدة المحققين على معرفة كيفية الجريمة ومحاولة إنتاج دلائل تؤدي إلى معرفة المجرم .

الفني الشرعي يقدم الأدوات والبراعة والتقنية والنظم التي يمكن بواسطتها تحليل جميع الأدلة الرقمية ومن ثم استخدامها لمعرفة كيفية الإعداد للجريمة التي وقعت.

وجود مجموعة من الفنيين المتخصصين في تقنية المعلومات أمر ضروري لمعرفة شواهد الجريمة الإلكترونية، ويتطلب الأمـــر مع تقدم التقنية الى تحديث معارفهم ومهاراتهم حتى يتكيفوا مع التطور السريع في التقنية. ويشير ( يـــونس، ٢٠٠٤ ) أن مكتب التحقيقات الفيدرالية ( FBI ) لديه الخبراء المتخصصون في تفتيش الحواسيب والإنترنت لمعرفة الأدلـــة والتأكـــد منها. كما تعمل على تدريبهم لضمان استمرارية تطوير المعارف والخبرات الفنية لديهم في عصر التقدم الفـــني في تقنيـــة المعلومات المستمر.

**مجرمي الشبكة العالمية للمعلومات**

ويصنف ( Thomas and Loader, 2000 ) مجرمي الشبكة العالمية للمعلومات إلى ثلاثة أنواع : مجـــرم في تـــدمير أنظمة الحاسب الآلي والشبكة ، المستأجر الذي يعمل لتأدية جريمة معينة ، الإرهابيين والمتطرفين لأداء أعمال إجرامية .

١. مجرمي شبكة الحاسب ألآلي ( Hackers ) وينطبق هذا على الأشخاص الذين لديهم المعرفة التامة بأنظمـــة وبرمجـــة الحاسب الآلي ويستخدمونها في أمور غير شرعية بواسطة تقنية المعلومات والاتصال ومنها الدخول لأنظمة الحاسب الآلي لغرض استكشاف المعلومات أو حب الاستطلاع على بعض المعلومات بشكل عام وليس لديهم دوافع إجراميـــة لتـــدمير

المعلومات أو سرقات مالية وعلى الرغم من أنها جريمة تعتبر من المزاح مثل بعض الاتصالات الهاتفية وربما يكون لها نتائج مالية للأشخاص أو للشركات أو للصناعة لكن ليس هدفهم الأساسي هو الحصول على مكاسب ربحية من وراء هـــذه الجريمة . إن هؤلاء يسعون لتكوين لهم سمعة من خلال جرأتهم على دخول نظام المنشأة نتيجة لوجود ثغـــرة في النظـــام الآلي الذي سمحت لهم الولوج إليه .

ولكن توجد مجموعة صغيرة من التخصصين للدخول للنظم لغرض تدمير ومسح وإلغاء بعض أو كل الملفات الإلكترونية وتشمل هذه المجموعة المجرمين الذين يسعون للحصول على معلومات بطاقة الائتمان لغرض استخدامها بالشراء . والذين يكتبون فيروسات الحاسب الآلي وكذلك الذين يلغون صفحات الإنترنت الخاصة في منظمة معينة أو مقدمة الخدمة .

إن الأشخاص الذين يدخلوا إلى الأنظمة لغرض الاستطلاع على المعلومات فيطبق عليهم المستوى الأدنى من قانون عقوبة الجريمة الإلكترونية وذلك نتيجة لدخولهم النظام الآلي من دون إذن .

٢. الإرهابيين والمتطرفين، هذا الصنف من المجرمين يستخدمون تقنية المعلومات والاتصال لأغـــراض سياســـية وأنشـــطة اجتماعية غير شرعية مثل الحث على الكراهية، واستخدامها في أنشطة غير مشروعة أو الانخراط في سلوكيات اجتماعيـــة غير مشروعة مثل تشجيع الأطفال على أعمال الفسق والخلاعة أو انخراطهم في أعمال الخلاعة المعروضة علـــى الشـــبكة العالمية للمعلومات . إن هذا النصف من المجرمين يعتمدون اعتماداً كلياً على تقنية المعلومات والاتصـــال للإنخـــراط في الأنشطة غير الشرعية . وهذه المجموعة تشمل الذين يندمجون في المعلومات التي تسعى إلى الصـــراع وتـــأجيج الحـــروب وكذلك الذين يسعون إلى تنظيم أنشطة سياسية غير شرعية.

.( Thomas and Loader, 2000 )

ويصنف ( Parker, 1998 ) حسب ما ذكرت قورة٢٠٠٥ المجرمين الذين يســـتخدمون تقنيـــة المعلومـــات في تنفيـــذ جرائمهم إلى سبعة أصناف تتباين هذه الأصناف من ناحية الخبرة ودرجة إلحاق الضرر بالغير ، موضحة على النحو التالي :

١. جرائم التسلية والمزاح (Pranksters) لا يكون لديه النية في إلحاق الضرر في المعلومات التي يصلون إليها ولكن الهدف الرئيسي لديهم التسلية والمزاح .

٢. دخول الأنظمة الإلكترونية الغير مصرحة (Hackers ) ويتمكن هؤلاء إلى الدخول إلى الأنظمة المحمية وذلك من خلال كسر الحواجز الأمنية والدافع الرئيس لذلك الفضول أ وتوضيح قدرتهم على تجاوز هذه الحواجز الأمنية .

٣. إلحاق الخسائر ، هذه الفئة هدفها تحقيق خسائر بالغير وليس تحقيق أرباح من هذا الاعتداء وينصف في هذه المجموعة مخترعي الفيروسات . Malicious Hackers .

٤. المجرم الإلكتروني ( Career Criminals ) هذه الفئة يكون لديهم هدف رئيس للدخول إلى الأنظمة والحصول على المعلومات التي يمكن الاستفادة منها لتحقيق الربح المادي وتعتبر نسبة هذه الجرائم منخفضة مقارنة بالجرائم الأخرى وتصل إلى ١.٥ % لأن هذه الجرائم تحتاج إلى مهارات ومعارف دقيقة بالأنظمة الإلكترونية .

أصبحت الحاسبات ذات أهمية بالغة وخصوصاً بعدما تم تطوير الحاسب الشخص وبدأ استخدامه بين الأفراد والشركات ولما تتمتع به من قدرة عالية على تخزين المعلومات والبيانات ، ومما زاد في قيمتها وأهميتها ربطها بالشبكات المحلية أو الخارجية ( الشبكة العالمية للمعلومات )وبدأ الاعتماد عليها في تبادل المعلومات وأصبحت المعلومات تبحر عبر حدود الدول ، وتمتاز هذه المعلومات بقيمتها للمنظمة والفرد فإن اختلاسها أو اتلافها أو مسحها يسبب ضرراً لأصحابها، فالحاجة إلى وضع التشريعات والتنظيمات أصبح أمراً ضرورياً بحق من يرتكب الجرائم الإلكترونية ( قورة ، ٢٠٠٥).

## خسائر الجريمة الإلكترونية

يوجد كمية هائلة من المعلومات منشورة على صفحات الشبكة العالمية للمعلومات وتتفاوت المعلومات ، ولكن يوجد معلومات أهميتها عالية تبحر في تلك الشبكة فإن الاعتداء والاستيلاء عليها يسبب مساوئ كبيرة للمنظمة أو الفرد.

وتذكر ( قورة، ٢٠٠٥ ) إن أبرز تلك الأساليب وأكثرها خطورة استخدام صفحات الشبكة العالمية للمعلومات المضللة ( Web Spoofing ) وهذا النوع من الصفحات الإلكترونية لها دور كبير في تضليل المستخدم للصفحات الأصلية وتكون درجة الخطورة عالية عندما يكون عدد المستخدمين كبيراً جداً لتلك الصفحة . مثل استخدام صفحات البنوك الإلكترونية للتحويل وعندما يتم الاستيلاء على معلومات عملاء المصرف يؤدي إلى إيقاع خسائر كبيرة بتلك المصارف.

تذكر قورة أن الإحصائية الناتجة عن وزارة الداخلية الفرنسية بلغت ١٢٠٠ جريمة إلكترونية بينها ٥٣٦ جريمة ضد الأشخاص وجرائم الآداب ١٨٩ بينما الجرائم ضد الأموال ٣ مليون جريمة . ويذكر Rose ( أشارت إليه قورة ٢٠٠٥ ) أن معدل الخسائر المالية الناتجة عن الجريمة المعلوماتية تقدر بـ ٥٠٠٠٠٠ دولار بينما الخسائر المالية الناتجة عن السرقة العادية تبلغ ٣٥٠٠ دولار حسب تقرير مكتب التحقيقات الفدرالية في الولايات المتحدة الأمريكية ( FBI ).

## أركان الجريمة الإلكترونية

### الركن المعنوي

إن الاعتداء على المعلومات الخاصة بالمنظمات الحكومية أو الخاصة أو مملوكة للأفراد بقصد إتلافها كلياً أو جزئياً أو تقليل منفعتها مما يؤدي إلى إلحاق الضرر بمالكي المعلومات تعتبر من الجرائم العمدية في حالة تحقق عنصري العلم بملكيتها للغير والإرادة في تدميرها مما له الأثر السلبي في تنفيذ أنشطة المنظمة جزئياً أو كلياً (الشوابكة، ٢٠٠٤).

ويقسم الشوابكة الركن المعنوي إلى محورين هما:

١. الاعتداء على نظام تشغيل بخلق مشكلة تؤدي إلى تباطؤ النظام في تنفيذ العمليات المطلوبة مثل معالجة المعلومات واسترجاعها وإرسالها مما يكون له الأثر السلبي على أداء المنظمة.

٢. الدخول غير المرخص إلى أنظمة المنظمة الإلكترونية، ويتم في هذه الحالة تدمير البيانات والمعلومات كلياً الموجودة في النظام أو التعديل والتشويه للبيانات والمعلومات مما تكون عائقاً أمام المنظمة للاستمرار في تنفيذ عملياتها أو الحد من اتخاذ القرارات السليمة (قشقوش، ١٩٩٢). ويحدث ذلك إما بالدخول أو البقاء بدون إذن أو يكون لدى المعتدي الخبرة والمعرفة التقنية التي تؤهله لاختراق النظام والتلاعب في النظام المنطقي لوحدة المعالجة في الحاسب الآلي، وقد يأخذ اسلونا آخر يتمثل في إدخال معلومات غير حقيقية تؤثر على المخرجات النهائية مثل تقديم قوائم مالية مزورة أو استمرارية أسماء بعض العاملين رغم تركهم العمل (الشوابكة، ٢٠٠٤).

وتذكر قورة (٢٠٠٥) أن الإعتداء على المعلومات من جرائم النصب ومن الجرائم العمدية ويكون الركن المعنوي في هذا النوع من الجرائم القصد الجنائي الذي يجب أن يتحقق في الجريمة. ويتحقق عنصر القصد عندما يكون المتهم على علم تام بأن المعلومات التي يعمل على تشويهها أو ادخال معلومات أخرى غير حقيقية أو أوامر للحاسب الآلي من شأنها تأدية ومعالجة تلك المعلومات باسلوب غير حقيقي ومظلل للمنظمة، وفي ضوء ذلك يتحقق علم الفاعل بذلك. ومن ناحية أخرى أن الشخص الذي يعتقد أن المعلومات التي يدخلها للحاسب الآلي أمرضروري لإتمام العمليات ومن ثم وقع الضرر فإن هذه الحالة لايتوافر فيها عنصر القصد.

الركن المادي

يتعلق بالإتلاف الجزئي أو الكلي للجانب المادي من نظم المعلومات الذي يفقده القدرة على تأدية أعمل المنظمة وبالتالي لا يحقق المنفعة التي أوجد من أجلها هذا النظام الإلكتروني (قشقوش، ١٩٩٢؛ الشوابكة، ٢٠٠٤). ويذكر الشوابكة، ٢٠٠٤ أن اتلاف الجواتب المعلوماتية المادية تتعلق " بالإتلاف الذي يقع على أجهزة الحاسب الآلي ومعداته وملحقاته، كالدعامات والبرامج المنسوخ عليها المعلومات والأوراق المستعملة في عمله والشرائط الممغنطة..." (صـــ ٢٢٠) مثل كسر اسطوانة البرمجيات أو أدوات تخزين المعلومات الخارجية(External Storages) أو إتلاف الخادم (Server) أو

وحدات المعالجة. ويؤكد الشوابكة، ٢٠٠٤ على أهمية وجود نصوص قانونية تحمي الجوانب المعلوماتية المادية وخصوصاً مع التطور السريع في تقنية المعلومات.

الركن القانوني

اهتمت الشريعة الإسلامية وقوانين الدول المتقدمة بحماية الحقوق الخاصة بالإفراد والمجتمع. ويتميز هذا العصر بالسرعة المذهلة في تطور تقنية المعلومات واعتماد جميع المجالات عليها وبما تحققه للفرد والمجتمع من توفير للوقت والسرعة في انجاز الأعمال. إن هذه المميزات فرضت على كافة مكونات المجتمع من أفراد ومنظمات عامة وخاصة استخدام تلك التقنية. ويذكر (Cate, 1997) إن الاستفادة من الشبكة العالمية للمعلومات والتقنية المصاحبة لها من الحاسبات والشبكات الأخرى أصبحت عرضة للاعتداءات. ويذكر (الشوابكة، ٢٠٠٤) " أن النصوص التقليدية تقف عاجزة أمام هذه الاعتداءات على الخصوصيات الفردية وأسرارهم. لذا فإن الحاجة تغدو ملحة لسد كل فراغ تشريعي في حماية ما يتم تداوله من معلومات وأسرار على هذه الشبكة، ولحماية الاتصالات والمراسلات فيما بين الأفراد على الخط، وتشديد هذه العقوبة في حال ما إذا وقعت هذه الانتهاكات للخصوصية من قبل مزودي خدمة الإنترنت ISPs أو أحد العاملين بالاتصالات(صـ صـ٥٨، ٥٩).

## تحليل البيانات

أولاً: تحليل بيانات المشاركين في الدراسة من كلية الشريعة في جامعة الإمام محمد بن سعود الإسلامية وقسم الأنظمة في معهد الإدارة العامة بمدينة الرياض

الوسط الحسابي و الانحراف المعياري لعناصر العينة

جدول (٢)

| العناصر | الانحراف المعياري | الوسط الحسابي |
|---|---|---|
| يتم تدريس أنظمة وتشريعات سعودية خاصة بالجريمة الإلكترونية. | ١.١٢ | ٢.٦٢ |
| أنواع الجرائم الإلكترونية محددة في المناهج التي يتم تدريسها. | ١.٠٣ | ٢.٦٩ |
| يتم تدريس أنظمة وتشريعات عربية خاصة بالجريمة الإلكترونية. | ١.٣٣ | ٢.٥٤ |
| يتم تدريس أنظمة وتشريعات عالمية خاصة بالجرائم الإلكترونية. | ١.٤٢ | ٢.٢٣ |
| توجد حاجة لخبراء في تحديد مستوى الجريمة الإلكترونية عند تشريع العقوبة الخاصة بها. | ٠.٦٦ | ١.٥٤ |
| توجد حاجة لإعطاء دورات برامج وورش عمل لأعضاء هيئة التدريس عن الجريمة الإلكترونية وطرق اختراق أنظمة أمن المعلومات. | ٠.٥٢ | ١.٤٦ |
| المملكة بحاجة إلى صياغة أنظمة وتشريعات خاصة بالجريمة الإلكترونية حسب تدرجها. | ٠.٥٢ | ١.٤٦ |
| حدد أهمية تدريس مادة تقنية وأمن المعلومات في كليات الشريعة والقانون في المملكة لتكوين معارف ومهارات لدى المتعلمين. | ٠.٥٢ | ١.٥٤ |
| حدد أهمية تدريس مادة التشريعات والأنظمة الخاصة بالجريمة الإلكترونية في كليات الحاسب الآلي المعلومات. | ٠.٦٥ | ١.٦٢ |

يوضح الجدول رقم ٢ الوسط الحسابي و الانحراف المعياري للعناصر للتساؤلات التي وردت في الإستبانة، نجد أن الإنحراف المعياري و الوسط الحسابي لتدريس أنظمة سعودية خاصة بالجريمة الإلكترونية يساوي(١.١٢، ٢.٦٢). وكذلك الإنحراف المعياري و الوسط الحسابي لتحديد أنواع الجرائم الإلكترونية في المنهج يساوي (١.٠٣، ٢.٦٩). بينما الإنحراف المعياري و الوسط الحسابي لمعرفة مدى تدريس أنظمة وتشريعات عربية خاصة بالجريمة الإلكترونية بالوقت

الحالي يساوي (١.٣٣، ٢.٥٤). الإنحراف المعياري و الوسط الحسابي لمعرفة مدى تدريس أنظمة وتشريعات عالمية خاصة بالجرائم الإلكترونية يساوي (١.٤٢، ٢.٢٣). بينما الإنحراف المعياري و الوسط الحسابي لأهمية الاستعانة بخبراء لتحديد مستوى الجريمة الإلكترونية يساوي (٠.٦٦، ١.٥٤). بينما الإنحراف المعياري و الوسط الحسابي لمعرفة مدى الحاجة لتقديم ورش عمل لأعضاء هيئة التدريس عن الجريمة الإلكترونية وطرق اختراق أنظمة أمن المعلومات يساوي (٠.٥٢، ١.٤٦). بينما الإنحراف المعياري و الوسط الحسابي لمعرفة مدى حاجة المملكة إلى صياغة أنظمة وتشريعات خاصة بالجريمة الإلكترونية حسب تدرجها يساوي (٠.٥٢، ١.٤٦). بينما الإنحراف المعياري و الوسط الحسابي لمعرفة أهمية تدريس مادة تقنية وأمن المعلومات في كليات الشريعة والقانون في المملكة حتى يكون هناك معارف ومهارات لدى المتعلمين يساوي (٠.٥٢، ١.٥٤). بينما الإنحراف المعياري و الوسط الحسابي لمعرفة أهمية تدريس مادة التشريعات والأنظمة الخاصة بالجريمة الإلكترونية في كليات الحاسب الآلي المعلومات يساوي (٠.٦٥، ١.٦٢).

يتم تدريس أنظمة وتشريعات سعودية خاصة بالجريمة الإلكترونية.

جدول (٣)

| | التكرارات | النسبة |
|---|---|---|
| موافق | ٣ | ٢٣.١ |
| موافق بشدة | ٢ | ١٥.٤ |
| غير موافق | ٥ | ٣٨.٥ |
| غير موافق بشدة | ٣ | ٢٣.١ |

يوضح الجدول رقم ٣ التكرارات والنسبة المئوية لمعرفة مدى تدريس أنظمة وتشريعات سعودية خاصة بالجريمة الإلكترونية، نجد أن نسبة من قال موافق و موافق بشدة تساوي (٣٨.٥) و نسبة من قال غير موافق و غير موافق بشدة تساوي (٦١.٦) وتمثل معظم العينة.

أنواع الجرائم الإلكترونية محددة في المناهج التي يتم تدريسها.

جدول (٤)

| | التكرارات | النسبة |
|---|---|---|
| موافق | ٢ | ١٥.٤ |
| موافق بشدة | ٣ | ٢٣.١ |
| غير موافق | ٥ | ٣٨.٥ |
| غير موافق بشدة | ٣ | ٢٣.١ |

يوضح الجدول رقم ٤ التكرارات والنسبة المئوية لمعرفة مدى تحديد أنواع الجرائم الإلكترونية محددة في المناهج التي يتم تدريسها، نجد أن نسبة من قال موافق و موافق بشدة تساوي (٣٨.٥) و نسبة من قال غير موافق و غير موافق بشدة تساوي (٦١.٦) وتمثل معظم العينة.

يتم تدريس أنظمة وتشريعات عربية خاصة بالجريمة الإلكترونية.

جدول (٥)

| | التكرارات | النسبة % |
|---|---|---|
| موافق | ٥ | ١٥.٤ |
| موافق بشدة | ٤ | ٢٣.١ |
| غير موافق بشدة | ٤ | ٢٣.١ |

يوضح الجدول رقم ٥ التكرارات والنسبة المئوية لمعرفة هل يتم تدريس أنظمة وتشريعات عربية خاصة بالجريمة الإلكترونية.في الوقت الحاضر، نجد أن نسبة من قال موافق و موافق بشدة تساوي (٣٨.٥) و نسبة من قال غير موافق بشدة تساوي (٢٣.١ %) و لم يتم الإجابة بغير موافق.

يتم تدريس أنظمة وتشريعات عالمية خاصة بالجرائم الإلكترونية.

جدول (٦)

| | التكرارات | النسبة |
|---|---|---|
| موافق | ٧ | ٥٣.٨ |
| غير موافق | ٢ | ١٥.٤ |
| غير موافق بشدة | ٤ | ٣٠.٨ |

يوضح الجدول رقم ٦ التكرارات والنسبة المئوية لمعرفة هل يتم تدريس أنظمة وتشريعات عالمية خاصة بالجريمة الإلكترونية.في الوقت الحاضر، نجد أن نسبة من قال موافق تساوي (٥٣.٨) ولا توجد إجابة بموافق بشدة، و نسبة من قال غير موافق بشدة تساوي (٤٦.٢ %) ولم يتم الإجابة بغير موافق.

توجد حاجة لخبراء في تحديد مستوى الجريمة الإلكترونية عند تشريع العقوبة الخاصة بها.

جدول (٧)

| | التكرارات | النسبة |
|---|---|---|
| موافق | ٧ | ٥٣.٨ |
| موافق بشدة | ٥ | ٣٨.٥ |
| غير موافق | ١ | ٧.٧ |

يوضح الجدول رقم ٧ التكرارات والنسبة المئوية لمعرفة أهمية الحاجة لخبراء في تحديد مستوى الجريمة الإلكترونية عند تشريع العقوبة الخاصة بها، نجد أن نسبة من قال موافق و موافق بشدة تساوي (٩٢.٣) وتمثل معظم العينة. و نسبة من قال غير موافق (٧.٧ %) ولم يتم الإجابة بغير موافق بشدة.

توجد حاجة لإعطاء دورات برامج وورش عمل لأعضاء هيئة التدريس عن الجريمة الإلكترونية وطرق اختراق أنظمة أمن المعلومات.

جدول (٨)

| | التكرارات | النسبة |
|---|---|---|
| موافق | ٧ | ٥٣.٨ |
| موافق بشدة | ٦ | ٤٦.٢ |

يوضح الجدول رقم ٨ التكرارات والنسبة المئوية لمعرفة أهمية الحاجة لإعطاء دورات برامج وورش عمل لأعضاء هيئة التدريس عن الجريمة الإلكترونية وطرق اختراق أنظمة أمن المعلومات، نجد أن نسبة من قال موافق و موافق بشدة تساوي (٥٣.٨) و نسبة من قال موافق (٤٦.٢ %) وتمثل جميع أفراد العينة، و لم يتم الإجابة بغير موافق أو غير موافق بشدة.

حاجة المملكة إلى صياغة أنظمة وتشريعات خاصة بالجريمة الإلكترونية حسب تدرجها.

جدول (٩)

| | التكرارات | النسبة |
|---|---|---|
| موافق | ٧ | ٥٣.٨ |
| موافق بشدة | ٦ | ٤٦.٢ |

يوضح الجدول رقم ٩ التكرارات والنسبة المئوية حاجة المملكة إلى صياغة أنظمة وتشريعات خاصة بالجريمة الإلكترونية حسب تدرجها، نجد أن نسبة من قال موافق و موافق بشدة تساوي (٥٣.٨) و نسبة من قال موافق (٤٦.٢ %) وتمثل جميع أفراد العينة، و لم يتم الإجابة بغير موافق أو غير موافق بشدة.

حدد أهمية تدريس مادة تقنية وأمن المعلومات في كليات الشريعة والقانون في المملكة حتى يكون هناك معارف ومهارات لدى المتعلمين.

جدول (١٠)

| | التكرارات | النسبة |
|---|---|---|
| مهم | ٦ | ٤٦.٢ |
| مهم جداً | ٧ | ٥٣.٨ |
| غير مهم | ٠ | ٠ |
| غير مهم جداً | ٠ | ٠ |

يوضح الجدول رقم ١٠ التكرارات والنسبة المئوية لمعرفة أهمية تدريس مادة تقنية وأمن المعلومات في كليات الشريعة والقانون في المملكة حتى يكون هناك معارف ومهارات لدى المتعلمين، نجد أن نسبة من قال مهم تساوي (٤٦.٢) و نسبة من قال مهم جداً (٥٣.٨ %) وتمثل جميع أفراد العينة، و لم يتم الإجابة بغير مهم أو غير مهم جداً.

حدد أهمية تدريس مادة التشريعات والأنظمة الخاصة بالجريمة الإلكترونية في كليات الحاسب الآلي المعلومات.

جدول (١١)

| | التكرارات | النسبة |
|---|---|---|
| مهم | ٦ | ٤٦.٢ |
| مهم جداً | ٦ | ٤٦.٢ |
| غير مهم | ١ | ٧.٧ |
| غير مهم جداً | ٠ | ٠ |

يوضح الجدول رقم 11 التكرارات والنسبة المئوية لمعرفة أهمية تدريس مادة التشريعات والأنظمة الخاصة بالجريمة الإلكترونية في كليات الحاسب الآلي المعلومات، نجد أن نسبة من قال مهم تساوي (٤٦.٢) و نسبة من قال مهم جداً (٤٦.٢ %) وتمثل معظم أفراد العينة،. و نسبة من قال غير مهم (٧.٧) و لم يتم الإجابة بغير مهم جداً.

## ثانياً: تحليل بيانات القطاعين الحكومي والخاص

الوسط الحسابي والإنحراف المعياري لعناصر العينة.

جدول (١٢)

| العناصر | الانحراف المعياري | الوسط الحسابي |
|---|---|---|
| توضح السياسات الخاصة في تقنية المعلومات بالمنشأة عقوبة الجريمة الإلكترونية. | ١.٢٥ | ٢.٤٧ |
| يوجد لدى العاملين في المنشأة إلمام بالعقوبة الخاصة بالجريمة الإلكترونية في المملكة. | ١.٢١ | ٢.٨٠ |
| يوجد لدى العاملين في المنشأة إلمام بالعقوبة الخاصة بالجريمة الإلكترونية الدولية (دول العالم الأخرى). | ١.٢١ | ٢.٨٠ |
| توجد أنظمة سعودية خاصة بالجريمة الإلكترونية يتم تطبيقها في المنشأة. | ٠.٥١ | ٣.٤٠ |
| توضح السياسات الخاصة بتقنية المعلومات أسس تشغيل تقنية المعلومات في المنشأة. | ٠.٩٩ | ١.٥٣ |
| يوجد أنظمة معدة بواسطة المنشأة تطبقها على الجريمة الإلكترونية. | ١.٠٣ | ٢.٧٣ |
| يوجد أنظمة خاصة بالجريمة الإلكترونية في المنشأة متدرجة حسب الجريمة. | ٠.٧٠ | ٣.٠٧ |
| يوجد في المنشأة أنظمة حماية (Security Programs) لمعلوماتها. | ٠.٦٣ | ١.٦٠ |
| توجد مراجعة دورية لأنظمة تقنية المعلومات وتحديثها في المنشأة. | ٠.٥٢ | ١.٤٧ |
| حدد أهمية تدريس مادة تقنية وأمن المعلومات في كليات الشريعة والقانون في المملكة حتى يكون هناك معارف ومهارات لدى المتعلمين. | ٠.٤١ | ١.٨٠ |
| حدد أهمية تدريس مادة التشريعات والأنظمة الخاصة بالجريمة الإلكترونية في كليات الحاسب الآلي والمعلومات. | ٠.٤١ | ١.٨٠ |

يوضح الجدول رقم ١٢ الوسط الحسابي و الانحراف المعياري للعناصر للتساؤلات التي وردت في الإستبانة الخاصة بالقطاعين العام والخاص، نجد أن الإنحراف المعياري و الوسط الحسابي للعقوبة الخاصة بالجريمة الإلكترونية ضمن سياسات استخدام تقنية المعلومات (١.٢٥، ٢.٤٧). وكذلك الإنحراف المعياري و الوسط الحسابي مدى إلمام العاملين في المنشأة بالعقوبة الخاصة بالجريمة الإلكترونية في المملكة يساوي (١.٢١، ٢.٨٠). بينما الإنحراف المعياري و الوسط الحسابي لمعرفة مدى إلمام العاملين في المنشأة بالعقوبة الخاصة بالجريمة الإلكترونية الدولية يساوي (١.٢١، ٢.٨٠).

الإنحراف المعياري و الوسط الحسابي لمعرفة مدى تطبيق أنظمة سعودية خاصة بالجريمة الإلكترونية يتم تطبيقها في المنشأة يساوي (٠.٥١، ٣.٤٠). بينما الإنحراف المعياري و الوسط الحسابي لمدى توضح السياسات الخاصة بتقنية المعلومات أسس تشغيل تقنية المعلومات في المنشأة يساوي (٠.٩٩، ١.٥٣).

بينما الإنحراف المعياري و الوسط الحسابي لمعرفة وجود أنظمة معدة بواسطة المنشأة تطبقها على الجريمة الإلكترونية يساوي (١.٠٣، ٢.٧٣). بينما الإنحراف المعياري و الوسط الحسابي لمعرفة هل هناك أنظمة خاصة بالجريمة الإلكترونية في المنشأة متدرجة حسب الجريمة يساوي (٠.٧٠، ٣.٠٧). بينما الإنحراف المعياري و الوسط الحسابي لمعرفة وجود أنظمة حماية لمعلوماتها (٠.٦٣، ١.٦٠). بينما الإنحراف المعياري و الوسط الحسابي لمعرفة وجود مراجعة دورية لأنظمة تقنية المعلومات وتحديثها في المنشأة يساوي (٠.٥٢، ١.٤٧). بينما الإنحراف المعياري و الوسط الحسابي لمعرفة أهمية تدريس مادة تقنية وأمن المعلومات في كليات الشريعة والقانون في المملكة حتى يكون هناك معارف ومهارات لدى المتعلمين يساوي (٠.٤١، ١.٨٠). بينما الإنحراف المعياري و الوسط الحسابي لمعرفة أهمية تدريس مادة التشريعات والأنظمة الخاصة بالجريمة الإلكترونية في كليات الحاسب الآلي المعلومات يساوي (٠.٤١، ١.٨٠).

توضح السياسات الخاصة في تقنية المعلومات بالمنشأة عقوبة الجريمة الإلكترونية.

جدول (١٣)

| | التكرارات | النسبة |
|---|---|---|
| موافق | ٥ | ٣٣.٣ |
| موافق بشدة | ٢ | ١٣.٣ |
| غير موافق | ٤ | ٢٦.٧ |
| غير موافق بشدة | ٤ | ٢٦.٧ |

يوضح الجدول رقم ١٣ التكرارات والنسبة المئوية الخاصة بتوضيح عقوبة للجريمة الإلكترونية ضمن سياسات استخدام تقنية المعلومات بالمنشأة، نجد أن نسبة من قال موافق و موافق بشدة تساوي (٤٦.٦) و نسبة من قال غير موافق و غير موافق بشدة تساوي (٥٣.٤) وتمثل معظم العينة.

يوجد لدى العاملين في المنشأة إلمام بالعقوبة الخاصة بالجريمة الإلكترونية في المملكة.

جدول (١٤)

| | التكرارات | النسبة |
|---|---|---|
| موافق | ٤ | ٢٦.٧ |
| غير موافق بشدة | ٦ | ٤٠.٠ |
| غير موافق | ٥ | ٣٣.٣ |

يوضح الجدول رقم ١٤ التكرارات والنسبة المئوية الخاصة بمدى إلمام العاملين في المنشأة بعقوبة الجريمة الإلكترونية في المملكة، نجد أن نسبة من قال موافق تساوي (٢٦.٧) و نسبة من قال غير موافق تساوي أو غير موافق بشدة (٧٣.٣) وتمثل معظم العينة.

يوجد لدى العاملين في المنشأة إلمام بالعقوبة الخاصة بالجريمة الإلكترونية الدولية (دول العالم الأخرى).

جدول (١٥)

| | التكرارات | النسبة |
|---|---|---|
| موافق | ٤ | ٢٦.٧ |
| غير موافق بشدة | ٦ | ٤٠.٠ |
| غير موافق | ٥ | ٣٣.٣ |

يوضح الجدول رقم ١٥ التكرارات والنسبة المئوية الخاصة بمدى إلمام العاملين في المنشأة بعقوبة الجريمة الإلكترونية الدولية، نجد أن نسبة من قال موافق تساوي (٢٦.٧) و نسبة من قال غير موافق تساوي أو غير موافق بشدة (٧٣.٣) وتمثل معظم العينة.

توجد أنظمة سعودية خاصة بالجريمة الإلكترونية يتم تطبيقها في المنشأة.

جدول (١٦)

| | التكرارات | النسبة |
|---|---|---|
| غير موافق | ٩ | ٦٠.٠ |
| غير موافق بشدة | ٦ | ٤٠.٠ |

يوضح الجدول رقم ١٦ التكرارات والنسبة المئوية الخاصة بمدى وجود أنظمة سعودية خاصة بالجريمة الإلكترونية يتم تطبيقها في المنشأة، نجد أن نسبة من قال غير موافق أو غير موافق بشدة (١٠٠.٠) وتمثل كامل العينة.

توضح السياسات الخاصة بتقنية المعلومات أسس تشغيل تقنية المعلومات في المنشأة.

جدول (١٧)

| | التكرارات | النسبة |
|---|---|---|
| موافق | ١١ | ٧٣.٣ |
| موافق بشدة | ١ | ٦.٧ |
| غير موافق | ٢ | ١٣.٣ |
| غير موافق بشدة | ١ | ٦.٧ |

يوضح الجدول رقم ١٧ التكرارات والنسبة المئوية الخاصة بوجود أسس تشغيل تقنية المعلومات في المنشأة من ضمن السياسات الموجودة في المنشأة، نجد أن نسبة من قال موافق و موافق بشدة تساوي (٨١.٠) و نسبة من قال غير موافق و غير موافق بشدة تساوي (١٩.٠).

يوجد أنظمة معدة بواسطة المنشأة تطبقها على الجريمة الإلكترونية.

جدول (١٨)

| | التكرارات | النسبة |
|---|---|---|
| موافق | ٣ | ٢٠.٠ |
| موافق بشدة | ١ | ٦.٧ |
| غير موافق | ٨ | ٥٣.٣ |
| غير موافق بشدة | ٣ | ٢٠.٠ |

يوضح الجدول رقم ١٨ التكرارات والنسبة المئوية الخاصة بوجود أنظمة معدة بواسطة المنشأة تطبقها على الجريمة الإلكترونية، نجد أن نسبة من قال موافق و موافق بشدة تساوي (٢٦.٧) و نسبة من قال غير موافق و غير موافق بشدة تساوي (٧٣.٣) وتمثل معظم العينة.

يوجد أنظمة خاصة بالجريمة الإلكترونية في المنشأة متدرجة حسب الجريمة.

جدول (١٩)

| | التكرارات | النسبة |
|---|---|---|
| موافق | ١ | ٦.٧ |
| غير موافق | ١١ | ٧٣.٣ |
| غير موافق بشدة | ٣ | ٢٠.٠ |

يوضح الجدول رقم ١٩ التكرارات والنسبة المئوية الخاصة بوجود أنظمة خاصة بالجريمة الإلكترونية في المنشأة متدرجة حسب الجريمة معدة بواسطة المنشأة تطبقها على الجريمة الإلكترونية، نجد أن نسبة من قال موافق تساوي (٢٦.٧) و لا توجد إجابة بموافق بشدة و نسبة من قال غير موافق و غير موافق بشدة تساوي (٩٣.٣) وتمثل معظم العينة.

يوجد في المنشأة أنظمة حماية (Security Programs) لمعلوماتها.

جدول (٢٠)

| | التكرارات | النسبة |
|---|---|---|
| موافق | ٧ | ٤٦.٧ |
| موافق بشدة | ٧ | ٤٦.٧ |
| غير موافق | ١ | ٦.٧ |

يوضح الجدول رقم ٢٠ التكرارات والنسبة المئوية الخاصة بوجود أنظمة حماية لمعلوماتها، نجد أن نسبة من قال موافق وموافق بشدة تساوي (٩٣.٤). و نسبة من قال غير موافق تساوي (٦.٧) ولا يوجد إجابة غير موافق بشدة.

توجد مراجعة دورية لأنظمة تقنية المعلومات وتحديثها في المنشأة.

جدول (٢١)

| | التكرارات | النسبة |
|---|---|---|
| موافق | ٨ | ٥٣.٣ |
| موافق بشدة | ٧ | ٤٦.٧ |

يوضح الجدول رقم ٢١ التكرارات والنسبة المئوية الخاصة مراجعة دورية لأنظمة تقنية المعلومات وتحديثها في المنشأة ، نجد أن نسبة من قال موافق وموافق بشدة تساوي (١٠٠.٠). ولا يوجد إجابة غير موافق أو غير موافق بشدة.

حدد أهمية تدريس مادة تقنية وأمن المعلومات في كليات الشريعة والقانون في المملكة حتى يكون هناك معارف ومهارات لدى المتعلمين.

جدول (٢٢)

| | التكرارات | النسبة |
|---|---|---|
| مهم | ٣ | ٢٠.٠ |
| مهم جداً | ١٢ | ٨٠.٠ |
| غير مهم | ٠ | ٠ |
| غير مهم جداً | ٠ | ٠ |

يوضح الجدول رقم ٢٢ التكرارات والنسبة المئوية لمعرفة أهمية تدريس مادة تقنية وأمن المعلومات في كليات الشريعة والقانون في المملكة حتى يكون هناك معارف ومهارات لدى المتعلمين، نجد أن نسبة من قال مهم تساوي (٢٠.٠) و نسبة من قال مهم جداً (٨٠.٠ %) وتمثل جميع أفراد العينة، و لم يتم الإجابة بغير مهم أو غير مهم جداً.

حدد أهمية تدريس مادة التشريعات والأنظمة الخاصة بالجريمة الإلكترونية في كليات الحاسب الآلي والمعلومات.

جدول (٢٣)

| | التكرارات | النسبة |
|---|---|---|
| مهم | ٣ | ٢٠.٠ |
| مهم جداً | ١٢ | ٨٠.٠ |
| غير مهم | ٠ | ٠ |
| غير مهم جداً | ٠ | ٠ |

يوضح الجدول رقم 23 التكرارات والنسبة المئوية لمعرفة أهمية تدريس مادة التشريعات والأنظمة الخاصة بالجريمة الإلكترونية في كليات الحاسب الآلي المعلومات، نجد أن نسبة من قال مهم تساوي (٢٠.٠) و نسبة من قال مهم جداً (٨٠.٠ %) وتمثل جميع أفراد العينة،. و و لم يتم الإجابة بغير مهم أو غير مهم جداً.

## النتائج

١. لا يتم تدريس أنظمة وتشريعات سعودية خاصة بالجريمة الإلكترونية، و توضح إجابة المشاركين أن نسبة من قال غير موافق أو غير موافق بشدة تساوي٦١.٦ %.

٢. أنواع الجرائم الإلكترونية عقوبتها غير محددة، وبلغت نسبة المشاركين ٦١.٦ %.

٣. أهمية وجود خبراء في حالة تشريع الجريمة الإلكترونية، وبلغت نسبة من يؤيد ذلك من المشاركين ٩٢.٣%.

٤. تؤيد كافة أفراد العينة سن أنظمة وتشريعات خاصة بالجريمة الإلكترونية.

٥. تؤكد كافة أفراد العينة المشاركة من القطاع العام والخاص و أعضاء هيئة التدريس في كلية الشريعة بجامعة الإمام محمد بن سعود الإسلامية و أعضاء هيئة التدريس في قسم الأنظمة في معهد الإدارة العامة أهمية تدريس مادة تقنية وأمن المعلومات في كليات الشريعة والقانون في المملكة حتى يكون هناك معارف ومهارات لدى المتعلمين.

٦. تؤكد كافة أفراد العينة المشاركة من القطاع العام والخاص و أعضاء هيئة التدريس في كلية الشريعة في جامعة الإمام محمد بن سعود الإسلامية و أعضاء هيئة التدريس في قسم الأنظمة في معهد الإدارة العامة أهمية تدريس مادة التشريعات والأنظمة الخاصة بالجريمة الإلكترونية في كليات الحاسب الآلي والمعلومات.

٧. توضح النتائج أن بعض عناصر العينة من القطاعين العام والخاص لا تنص في سياساتها و إجراءاتها الخاصة باستخدام تقنية المعلومات على عقوبة الجريمة الإلكترونية ونسبتها ٥٣.٤%.

٨. معظم عناصر العينة الخاصة بالقطاعين العام والخاص تؤكد عدم إلمام العاملين بالمنشأة بعقوبة الجريمة الإلكترونية في المملكة وتبلغ هذه النسبة ٧٣.٣%.

٩. معظم عناصر العينة الخاصة بالقطاعين العام والخاص تؤكد عدم إلمام العاملين بالمنشأة بعقوبة الجريمة الإلكترونية الدولية (مختلف دول العالم) وتبلغ هذه النسبة ٧٣.٣%.

١٠. تؤكد جميع عناصر العينة عدم وجود أنظمة سعودية خاصة بالجريمة الإلكترونية.

١١. لا يوجد لدى المنشآت في القطاع الخاص والعام أنظمة وتشريعات بالجريمة الإلكترونية وتبلغ النسبة ٧٣.٣%.

١٢. تؤكد معظم عناصر العينة عدم وجود أنظمة وتشريعات متدرجة حسب الجريمة وتبلغ النسبة ٩٣.٣%.

١٣. تؤكد معظم عناصر العينة بوجود أنظمة حماية لمعلوماتها وتبلغ هذه النسبة ٩٣.٤%.

## نتائج تساؤلات الدراسة

### السـؤال الأول

هل يتم تدريس أنظمة وتشريعات خاصة بالجريمة الإلكترونية في كلية الشريعة في جامعة الإمام محمد بن سعود الإسلامية، وقسم الأنظمة في معهد الإدارة بالرياض؟ وهل أنواع الجرائم محددة في المنهج؟

لا يتم تدريس أنظمة وتشريعات سعودية خاصة بالجريمة الإلكترونية، و نسبة إجابة المشاركين ٦١.٦%؛ كما أن أنواع الجرائم الإلكترونية غير محددة في المنهج، و نسبة إجابة المشاركين ٦١.٦% وتمثل معظم عناصر العينة.

### السـؤال الثاني

ما وجهة نظر عناصر العينة من القطاعين العام والخاص نحو سن أنظمة وتشريعات خاصة بالجريمة الكتروني في المملكة؟

تؤيد كافة أفراد العينة سن أنظمة وتشريعات خاصة بالجريمة الإلكترونية. كما يؤكد معظم عناصر العينة على أهمية وجود خبراء في حالة تشريع الجريمة الإلكترونية، وبلغت نسبة من يؤيد ذلك من المشاركين ٩٢.٣%.

### السـؤال الثالث

ما الحاجة لتدريس مادة خاصة في التشريعات والأنظمة الخاصة بالجريمة الإلكترونية في كليات الحاسب الآلي والمعلومات؟

ما أهمية تدريس مادة تقنية وأمن المعلومات في كليات الشريعة والقانون في المملكة؟

نؤكد كافة أفراد العينة المشاركة من القطاع العام والخاص و أعضاء هيئة التدريس في كلية الشريعة في جامعة

الإمام محمد بن سعود الإسلامية و أعضاء هيئة التدريس في قسم الأنظمة في معهد الإدارة العامة أهمية تدريس مادة التشريعات والأنظمة الخاصة بالجريمة الإلكترونية في كليات الحاسب الآلي والمعلومات.

نؤكد كافة أفراد العينة المشاركة من القطاع العام والخاص و أعضاء هيئة التدريس في كلية الشريعة في جامعة الإمام محمد بن سعود الإسلامية و أعضاء هيئة التدريس في قسم الأنظمة في معهد الإدارة العامة أهمية تدريس مادة تقنية وأمن المعلومات في كليات الشريعة والقانون في المملكة حتى يكون هناك معارف ومهارات لدى المتعلمين.

السؤال الرابع

هل يوجد لدى المنشآت أنظمة وتشريعات للجريمة الإلكترونية؟ وما مدى إلمام العاملين بالمنشآت بتلك الأنظمة والتشريعات؟

تؤكد جميع عناصر العينة عدم وجود أنظمة سعودية خاصة بالجريمة الإلكترونية، وكذلك عدم وجود أنظمة وتشريعات بالجريمة الإلكترونية لدى المنشآت في القطاع الخاص والعام خاصة يهما و النسبة ٧٣.٣%. كما تؤكد معظم عناصر العينة عدم وجود أنظمة وتشريعات متدرجة حسب الجريمة و نسبتها ٩٣.٣%.

معظم عناصر العينة الخاصة بالقطاعين العام والخاص تؤكد عدم إلمام العاملين بالمنشأة بعقوبة الجريمة الإلكترونية في المملكة ونسبتها ٧٣.٣%؛ وتشير معظم عناصر العينة الخاصة بالقطاعين العام والخاص عدم إلمام العاملين بالمنشأة بعقوبة الجريمة الإلكترونية الدولية (مختلف دول العالم) ونسبتها ٧٣.٣%.

## الخاتمة والإقتراحات

### الخاتمة

فرضت تقنية المعلومات مجموعة من التحديات عل مختلف القطاعات ومن أهمها دمجها في كافة أنشطتها المختلفة و تضمنت هذه الدراسة الأنظمة والتشريعات الخاصة بالجريمة الإلكترونية لعدد من الدول وتشمل استراليا والولايات المتحدة الأمريكية و ماليزيا وفرنسا وكندا وجمهورية الصين وهنج كونج والدنمرك وألمانيا وايرلندا والهند واليابان والإمارات العربية المتحدة. و تعتبر دولة الإمارات العربية المتحدة الدولة العربية التي سنت أنظمة وتشريعات لمعالجة هذا النوع الجديد من الجريمة وتتميز بدقتها. كما تطرق البحث لمعرفة مدى تدريس الأنظمة والتشريعات الخاصة بالجريمة الإلكترونية على النطاق المحلي والعربي والدولي في كلية الشريعة بجامعة الإمام محمد بن سعود الإسلامية وقسم الأنظمة بمعهد الإدارة العامة بالرياض وإمكانية تدريس مادة امن المعلومات في تلك البرامج لتعزيز المعارف والمهارات لدى المتعلمين. كما شملت الدراسة القطاعين الحكومي والخاص لمعرفة تطبيق تلك الأنظمة والتشريعات والحاجة لتدريسها في كليات علوم الحاسب الآلي.

### والإقتراحات

من نعم الله على هذا البلد تطبيق الأحكام المستمدة من القرآن الكريم والسنة النبوية الصالحة لكل زمان ومكان، والتي تعالج المستجدات في حالة وجودها أو وقوعها. و من هذه المستجدات استخدام تقنية المعلومات في معظم أنشطة الحياة الذي يفرض سن الأنظمة والتشريعات الكفيلة بحماية بتدفق المعلومات ونشرها بواسطة تلك الأدوات. ويقترح الباحثان التوصيات الآتية:

١. تطور تقنية المعلومات والإعتماد عليها في جميع المجالات في المملكة العربية السعودية و ضمان التوسع في استخدامها يتطلب سن الأنظمة والتشريعات التي تناسب الجريمة الإلكترونية مثل:

أ. انتهاك الخصوصية الفردية والعائلية مثل القذف.

ب. الإعتداء على التحويلات والمعاملات النقدية والتجارية عبر الشبكة العالمية للمعلومات.

ت. الدخول إلى المعلومات الخاصة بالأفراد والمنشآت الحكومية والتجارية والصناعية والتعليمية.

ث. الدخول على المعلومات وتدميرها أو تشويهها أو التقليل من أهميتها.

ج. إفشاء المعلومات بقصد أو غير قصد أو السماح باستخدام الصلاحيات للدخول إلى أنظمة تقنية المعلومات.

٢. أهمية تدريس مادة أمن المعلومات وكيفية الإعتداء على النظام لطلاب كليات الشريعة والأنظمة حتى يكون لديهم المعرفة التامة والقدرة على تطبيق الحكم.

٣. أهمية تدريس مادة في أحكام تقنية المعلومات العربية والدولية، مما تتيح الفرصة للمتعلم الإلمام بتلك الأنظمة والمساهمة في تطوير بيئة المنشأة ونشر الوعي بين العاملين.

٤. الإستعانة بالخبراء في حالة تحديد الجريمة الإلكترونية لغرض تطبيق العقوبة المناسبة.

٥. أهمية تطبيق أنظمة حماية المعلومات ومراجعتها بصورة دورية لتطويرها وبما يناسب مع سرعة التقدم التقني.

٦. تدريس الأنظمة الإقليمية والعربية والدولية في كليات الأنظمة والشريعة.

٧. التعاون الإقليمي والعربي والدولي في مكافحة هذه الجريمة.

٨. أهمية نشر الأنظمة والتشريعات الإقليمية والعربية والدولية في المنشآت وتنمية الوعي بين أفرادها. كذلك ينبغي نشرها في مقاهي الإنترنت.

٩. متابعة التطور التقني والعمل على متابعة تطوير الأنظمة والتشريعات التي تناسب ما يستجد في التطور التقني.

الوضع الحالي وتطبيق أنظمة وتشريعات قوانين الجريمة الإلكترونية
في المملكة العربية السعودية في القطاعين العام و الخاص

أولا: المعلومات الشخصية

تعليمات: من فضلك ضع علامة (√) في المكان المناسب:

| | | | |
|---|---|---|---|
| ١. | المؤسسة التعليمية:<br>□ معهد الإدارة العامة □ جامعة الإمام محمد بن سعود | ٢. | العمر:<br>□ ٢٥-٣٠ □ ٣١-٣٥ □ ٣٦- ٤٠ □ ٤١-٤٥<br>□ ٤٦ – ٥٠ □ ٥١ – ٥٥ □ ٥٦ فأكبر |
| ٣. | الجنسية: | ٤. | الدرجة العلمية:<br>□ أستاذ □ أستاذ مشارك □ أستاذ مساعد |
| ٥. | الجامعة المتخرج منها والدولة: | ٦. | الخبرة في استخدام الحاسب الآلي والإنترنت:<br>□ لا يوجد □ ضعيفة □ متوسطة □ عالية |

ثانياً: تضمين التشريعات والأنظمة الخاصة بالجرائم الإلكترونية في البرامج الأكاديمية.

تعليمات: من فضلك ضع علامة (√) في المكان المناسب أمام كل عبارة.

| | العبـــــارة | موافق | موافق بشدة | غير موافق | غير موافق بشدة |
|---|---|---|---|---|---|
| ٧. | يتم تدريس أنظمة وتشريعات سعودية خاصة بالجريمة الإلكترونية. | | | | |
| ٨. | أنواع الجرائم الإلكترونية محددة في المناهج التي يتم تدريسها. | | | | |
| ٩. | يتم تدريس أنظمة وتشريعات عربية خاصة بالجريمة الإلكترونية. | | | | |
| ١٠. | يتم تدريس أنظمة وتشريعات عالمية خاصة بالجرائم الإلكترونية. | | | | |
| ١١. | توجد حاجة لخبراء في تحديد مستوى الجريمة الإلكترونية عند تشريع العقوبة الخاصة بها. | | | | |
| ١٢. | توجد حاجة لإعطاء دورات برامج وورش عمل لأعضاء هيئة التدريس عن الجريمة الإلكترونية وطرق اختراق أنظمة أمن المعلومات. | | | | |
| ١٣. | المملكة بحاجة إلى صياغة أنظمة وتشريعات خاصة بالجريمة الإلكترونية حسب تدرجها. | | | | |

ثالثاً: حدد أهمية تدريس مادة تقنية وأمن المعلومات في كليات الشريعة والقانون في المملكة لتكوين معارف ومهارات لدى المتعلمين.

□ مهم □ مهم جداً □ غير مهم □ غير مهم جداً

رابعاً: حدد أهمية تدريس مادة التشريعات والأنظمة الحاصة بالجريمة الإلكترونية في كليات الحاسب الآلي والمعلومات.

□ مهم □ مهم جداً □ غير مهم □ غير مهم جداً

الوضع الحالي لتدريس أنظمة وتشريعات قوانين الجريمة الإلكترونية
في جامعات المملكة العربية السعودية

أولا: المعلومات الشخصية

تعليمات: من فضلك ضع علامة (√) في المكان المناسب:

| | | | |
|---|---|---|---|
| ١. | نوع القطاع:<br>☐ حكومي ☐ خاص | ٢. | سنوات الخبرة في مجال العمل الحالي:<br>☐ ٣ فأقل ☐ ٤-٦ ☐ ٧- ١٠ ☐ ١٠ فأكثر |
| ٣. | المرحلة التعليمية:<br>☐ دبلوم ☐ بكالريوس ☐ ماجستير<br>☐ أخرى (من فضلك حدد)..... | ٤. | الخبرة في مجال تقنية المعلومات: (من فضلك حدد)..... |
| ٥. | الجامعة المتخرج منها: | ٦. | الدولة المتخرج منها: |

ثانياً: الوضع الحالي لتطبيق أنظمة وتشريعات جرائم الحاسب الآلي و الشبكة العالمية للمعلومات .

تعليمات: من فضلك ضع علامة (√) في المكان المناسب أمام كل عبارة.

| | العبـــــارة | موافق | موافق بشدة | غير موافق | غير موافق بشدة |
|---|---|---|---|---|---|
| ٧. | توضح السياسات الخاصة في تقنية المعلومات بالمنشأة عقوبة الجريمة الإلكترونية. | | | | |
| ٨. | يوجد لدى العاملين في المنشأة إلمام بالعقوبة الخاصة بالجريمة الإلكترونية في المملكة. | | | | |
| ٩. | يوجد لدى العاملين في المنشأة إلمام بالعقوبة الخاصة بالجريمة الإلكترونية الدولية (دول العالم الأخرى). | | | | |
| ١٠. | توجد أنظمة سعودية خاصة بالجريمة الإلكترونية يتم تطبيقها في المنشأة. | | | | |
| ١١. | توضح السياسات الخاصة بتقنية المعلومات أسس تشغيل تقنية المعلومات في المنشأة. | | | | |
| ١٢. | يوجد أنظمة معدة بواسطة المنشأة تطبقها على الجريمة الإلكترونية. | | | | |
| ١٣. | يوجد أنظمة خاصة بالجريمة الإلكترونية في المنشأة متدرجة حسب الجريمة. | | | | |
| ١٤. | يوجد في المنشأة أنظمة حماية (Security Programs) لمعلوماتها. | | | | |
| ١٥. | توجد مراجعة دورية لأنظمة تقنية المعلومات وتحديثها في المنشأة. | | | | |

ثالثاً: حدد أهمية تدريس مادة تقنية وأمن المعلومات في كليات الشريعة والقانون في المملكة لتكوين هناك معارف ومهارات لدى المتعلمين.

☐ مهم ☐ مهم جداً ☐ غير مهم ☐ غير مهم جداً

رابعاً: حدد أهمية تدريس مادة التشريعات والأنظمة الخاصة بالجريمة الإلكترونية في كليات الحاسب الآلي والمعلومات.

☐ مهم ☐ مهم جداً ☐ غير مهم ☐ غير مهم جداً

**المراجع باللغة العربية**


الشوابكة، محمد أمين (٢٠٠٤). جرائم الحاسوب والإنترنت الجريمة المعلوماتية، عمان، الأردن: مكتبة دار الثقافةللنشر والتوزيع.

العريان، محمد علي (٢٠٠٤). الجرائم المعلوماتية. الاسكندرية، مصر: دار الجامعة الجديدة للنشر.

الصغير، جميل عبد الباقي (١٩٩٢). القانون الجنائي والتكنولوجيا الحديثة، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية. القاهرة، مصر: دار الفكر العربي.

الفريق العربي للأمن والحماية المعلوماتية (١٤٢٨). قانون المعاملات والتجارة الإلكترونية في دبي. http://www.atsdp.com/forum/showthread.php?s=2ab2ab3452650bba656c8455f845fb48&t=1612

الفريق العربي للأمن والحماية المعلوماتية (١٤٢٨). القانون الإتحادي في شأن مكافحة جرائم تقنية المعلومات. http://www.atsdp.com/forum/showthread.php?s=2ab2ab3452650bba656c8455f845fb48&t=298

قشقوش، هدى حامد (١٩٩٢). جرائم الحاسب الإلكتروني في التشريع المقارن. القاهرة: دار النهضة العربية.

قورة، نائلة عادل محمد (٢٠٠٥). جرائم الحاسب الآلي الاقتصادية دراسة نظرية وتطبيقية. بيروت، لبنان: منشورات الحلبي الحقوقية.

يونس، عمر محمد (٢٠٠٥) الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي.

## المراجع الأجنبية


Ada, S., (1999). The impact of electronic commerce on the publishing industry: towards a business value complementarily framework of electronic publishing. Journal of Information Science, 25(2), 133-145.

Carter, D. and Katz, A. (1996). Computer crime: An emerging challenge for law enforcement. FBI law enforcement bulletin, Available at http://www.fbi.gov/leb/dec961.txt.

Casey, E., (2000). Digital evidence computer crime. San Diego, CA: ACADEMIC Press.

Castells, M. (1996). The information age: Economy , society and culture. Vol. I, The Rise of the Network Society, Oxford: Blackwell.

Castells, M. (1998). ). The information age: Economy , society and culture. Vol. III, End of Millennium, Oxford: Blackwell.

Chang, K., Jackson, J., & Gover, V. (2003). E-commerce and corporatate strategy: an executive perspective. Information and Management, 40(7), 663-675.

Cate, F. (1997). Privacy in the information age. Washington: The Brookings Institution.

Mellahi, K., Frynas, J., & Finlay, P. (2005). Global strategic management. UK: Oxford University Press.

Lilley, P. (2002). hacked attacked & abused digital crime exposed. London, UK: Kogan Page Limited.

Gallagher, N. (1998). Cybercrime, transnational crime and intellectual property, Congressional Statement, FBI at: http://www.fbi.gov/pressrm/congress98/gallagher.htm.

Gupta, J., & Sharma, S., (2003). Creating business value through e-commerce. In Namchul Shin, (edet). Creating business value with information technology challenge and solutions. Hershey, PA: IRM Press.

Filos, E. (2005). Virtuality and the future of organization. In Goran Putnik and Maria Cunha, Virtual Enterprise Integration Technological and Organizational Perspectives. Hershey, PA: IDEA Press.

Filos, E. and Bnahan, E. (2001a). will the organization disappear? The challenges of the new economy and future perspectives. In L. M. Camarinha-Matos, H. Afsharmanesh, &

R. J. Rabelo(Eds.), E-business and virtual enterprises: Managing business-to-business cooperation(pp. 3-20). Dordrecht: Kluwer.

Iwaarden, J., Wiele, T., Ball, L., and Millen, R. (2004). Perceptions about the quality of web sites: a survey amongst students at Northeastern University and Erasmus University. Information and Management, 41(8), 947-959.

Smedinghoff, T. (1996). On line law (The Spa's legal guide to doing business on the Intenet): the software Publisher Association.

Thomas, D., & Loader, B. (2000). Cybercrime law enforcement, security and surveillance in the information age. London, UK: Routledge.

Vallabhaneni, S., (1989). Auditing computer security a manual with case studies. new York, NY: John Wiley & Sons.