"الأدلة القضائية في أمن الفضاء الحاسوبي"

يعتبر قطاع تكنلوجيا الاتصالات من أكثر القطاعات حيوية في سلطنة عمان، وذلك يظهر جلياً من خلال الأرقام والإحصاءات التي تقدمها وزارة الاقتصاد الوطني بشكل دوري، ففي نهاية شهر ديسمبر من العام 2007 شهد قطاع الاتصالات نمواً متسارعاً، حيث بلغ عدد المشتركين في خدمة الهاتف المتنقل 2.5 مليون مشترك بزيادة قدرها 37.5%، إلا أن عدد مستخدمي الهاتف الثابت إنخفض إلى 261 ألف مشترك بنسبة تغيير 0.6-% وبالرغم من ذلك الإنخفاض فقد ارتفعت نسبة مستخدمي خدمة الإنترنت 10% ليبلغ العدد أكثر من 70 ألف مشترك. وربما تكون الزيادة بسبب تقديم خدمات الانترنت المتطورة في الهاتف النقال مثل خدمة الجيل الثالث.

في عام 2002 أصدرت سلطنة عمان المرسوم السلطاني رقم 2002/30 القاض بتأسيس هيئة تنظيم الاتصالات لتعمل بشكل مستقل لتنفيذ السياسة العامة لقطاع الاتصالات وترجمة توجهات الحكومة لتحرير هذا القطاع الهام بهدف إطلاق سوق الاتصالات وإزاحة الستار أمام المستثمر الأجنبي لدخول هذا القطاع الذي تقوده الشركة العمانية للاتصالات باعتبارها المشغل الأول لجميع خدمات الاتصالات بالسلطنة.

في الوقت الذي نشعر فيه بالتقدم والتطور النوعي الكبير في هذا القطاع إلا أننا نلاحظ في الوقت ذاته محدودية مستخدمي الانترنت في السلطنة عموماً، وخارج العاصمة مسقط خصوصاً مما يجعل مستخدمي هذة الخدمة أقل بكثير عن ما هو موجود في الدول المجاورة. وتأتي أسباب محدودية المستخدمين لصعوبة توصيل خدمة الانترنت

وتغطيتها الشحيحة لمناطق السلطنة نظراً للتوسع العمراني الأفقي الذي تنتهجه السلطنة، كما أن الطبيعة الجغرافية الصعبة التي تقع فيها تلك المناطق الحجرية والصحراوية لها كلمة اخرى، على الأقل فيما يتعلق بخدمة الإنترنت الفائق السرعة ADSL.

إن إيمان السلطنة بضرورة بلوغ التقنيات الحديثة بشكل ناجح وتحقيق أهداف الحكومة المستقبلية في حوسبة الحياة اليومية للإنسان العماني كان الدافع الأول لخلق اتحاد قوي بين الحكومة والشركة العمانية للاتصالات لقناعة الطرفين بحاجته للأخر لبلوغ الهدف الذي يكفل بناء مجتمع رقمي قادر على التواصل باسلوب حديث مع مجتمعات دول العالم الأخرى. وربما يمكننا أن نأخذ هذا الإتحاد كمثال لإبراز أهمية دور القطاع الخاص في المشاركة لقيادة دفة تكنولوجيا المعلومات في السلطنة كما هو في جميع دول العالم. وقد ترجم هذا الاتحاد من خلال التوقيع على اتفاقية التعاون المشترك لتنفيذ مشروع الحكومة الالكترونية الطموح الذي كان القاعدة العريضة التي استندت عليها الكثير من الأنشطة والفعاليات مثل مشروع "مجتمع عمان الرقمي" ومشروع "نشر ثقافة تكنولوجيا المعلومات داخل المجتمع". وفي هذا الإطار وقعت الشركة العمانية للاتصالات مع هيئة تقنية المعلومات على اتفاقية تشغيل الشبكة الحكومية الموحدة للوزارات ومؤسسات القطاع العام لربط 750 موقعاً حكومياً، وتعرف هذة الشبكة بشبكة MPLS التي تتميز بالأمن والحماية من خلال المواصفات الأمنية التي وضعتها الحكومة بالتعاون مع الجهات المسؤلة في الدولة، أخذةً بعين الاعتبار حاجة القطاع الخاص ايضاً للإستفادة من هذا المشروع المهم.

وفي خط متواز تقوم هيئة تقنية المعلومات بالعمل على مساحة واسعة من المشاريع التكنلوجية اضافة الى ما تم ذكره سابقاً مشروع "مركز الحماية من الكوارث" وهو مشروع طموح جداً يهدف الى ضمان توفر البيانات الرقمية الحكومية حتى في ضل تعرض البلاد للكوارث الطبيعية المفاجأة، ويعمل هذا المركز على توفر خطوط اتصال

مباشرة لكل وحدة حكومية على حده بغرض اخذ نسخ احتياطية من بيانات تلك الوحدات بشكل دوري والاحتفاظ بها في مكان مخصص تم تجهيزه بأعلى المستويات الفنية والامنية ليعمل في اقصى الظروف الطبيعية كالعواصف والزلازل. كما ان الهيئة تقوم بمساعدة الوحدات الحكومية على رسم السياسات الامنية التي يتم تطبيقها في شبكات الحاسوب بالوحدات الحكومية لضمان موائمتها مع السياسة الامنية العامة للدولة.

إن التطور النوعي في تكنلوجيا الاتصالات والانترنت أعطى أفراد المجتمع مجالا واسعا للإطلاع على المعلومات وأدى إلى تغيير كبير في أسلوب الحياة والتعامل بين الناس، كما اثر بشكل مباشر على حجم ونوع الجريمة، وعلى مشروعية الفعاليات بشكل عام. ونتج عن ذلك نوع جديد من الجريمة اطلق عليها فيما بعد "الجريمة الالكترونية" والتي تتخذ أشكالا عديدة كما سنرى لاحقا.

وحيث أن الجريمة الإلكترونية حديثة النشوء فقد نتج عن ذلك انعدام الاتفاق على تعريف موحد لها، من ذلك مثلا نجد التعاريف التالية:

1) عرفت الشرطة البريطانية الجريمة الالكترونية بأنها:

"استعمال شبكة الحاسوب لعمل إجرامي."

2) بينما عرفها الإتحاد الأوربي بأنها:

"أي مخالفة جرمية ترتكب ضد أوباستعمال شبكة الحاسوب."

3) كما عرفها الإدعاء العام العماني على انها:

"تكون الجريمة إلكترونية اذا تم اقتراف الجرم بإستخدام التقنية الحديثة، سواءً كان جهاز حاسوب أو أي جهاز إلكتروني أخر حديث، ولولا ذلك لم يمكن اقترافها"

4) وعرفها القضاء العماني على أنها:

"يتفق القضاء العماني في تعريفه للجريمة الاكترونية مع تعريف الادعاء العام العماني إلا انه زاد عليه امكانية تفرع الجرم الالكتروني الى اكثر من جرم في نفس الواقعة"

5) واعرفها انا شخصياً بأنها:

"الاتصال من جهاز حاسوب الى أي جهاز حاسوب أخر، اوجهاز اليكتروني أخر بواسطة شبكة محلية اودولية كشبكة الانترنت بغرض إرتكاب ما يحرمه القانون"

بالرغم من إختلاف تعبير كل تعريف إلا إن كلمتي الحاسوب واجرام حاضرتين في جميع التعاريف وذلك يوحي بطريقة غير مباشرة على الخطر الكامن بين براثن التكنلوجيا الحديثة. اما انا فقد سلكت طريقاً مشروطاً في تعريف الجريمة الالكترونية، فقد جمعت الجانبين الفني والقانوني لكي يجوز تكييف الجريمة على انها جريمة إلكترونية، وقد شددت على ضرورة حدوث إتصال بين جهاز حاسوب وجهاز حاسوب اخر، خلاف ذلك لا يمكن ارتكاب جريمة إلكترونية من خلال العمل على جهاز منفرد مهما كان نوع الجرم المفتعل. والدليل على ذلك - حسب قراءتي للقوانين الجزائية في بعض الدول العربية - فإنه يمكن استخدام الحاسوب في الكثير من الجرائم لكن ليس بالضرورة يتم تكييفها على انها جريمة الاكترونية، كنشر مطبوعات يحرمها القانون، اوجريمة تزوير في المستندات والوثائق، اوالتلاعب بصور الافراد وتشويهها بقصد اهانة الكرامة. كل تلك الجرائم ربما لا يمكن لها ان تقع لولا استخدام الحاسوب في وقوعها، إلا انه لا يمكن ان تصنف كجريمة الكترونية بل ترد الى أصل الفعل. في الوقت ذاته يتم تكييف جميع تلك الجرائم كجرائم إلكترونية تلقائياً بمجرد ارسالها من جهاز حاسوب إلى أخر اذا تم الأخذ بعين الاعتبار التعريف الذي قدمته في ورقة العمل هذة، كنشر مطبوعات ومقالات محرمة قانوناً مثل القذف والتشهير في مواقع الانترنت، أو تزوير مستندات وارسالها/استقبالها من/الى الانترنت، أو ارسال صور عبر البريد الالكتروني تمت معالجتها ببرامج الحاسوب بقصد اهانة الكرامة، وجميع تلك الجرائم لا تتم لو لم يحدث الاتصال بين اجهزة الحاسوب وهوشرط مهم في تكييف الجريمة وتصنيفها جريمة الكترونية.

أنه مما لا يخفى على أحد نسبة تطور الجريمة الإليكترونية في تزايد مستمر خلال الآونة الأخيرة كما انها بدأت في اخذ اشكالاً جديدة من التعدد و التنوع مثل:

1- **سرقة الهوية**: وتشمل ادعاء هوية شخص حي أوميت.
2- **الحصول على نفع غير مشروع بواسطة بيانات تخص الغير**: وتشمل على سبيل المثال استعمال هوية شخص آخر لهدف محدد مثل تسجيل سيارة باسمه لتحميله غراماتها.
3- **الإحتيال عبر الانترنت**: وتشمل كل أنواع الاحتيال للحصول على المال بادعاء شخصية أخرى أواستعمال معلومات شخصية لآخر.
4- **الدخول لمواقع إباحية الخاصة بالاطفال**: وتشمل الجرائم المتعلقة بالجنس مثل التجارة بالجنس على الشبكة والنشاط الجنسي مع الأطفال.
5- **نشر صور فاضحة للأطفال عن طريق الإنترنت**: وهي نشر صور جنسية للأطفال على شبكة الانترنت.
6- **إهانة الكرامة بإستخدام الحاسب الآلي**: وتشمل التهديد والتهجم والتشهير عن طريق الشبكة.
7- **سوء استعمال الحاسوب**: وتشمل الدخول غير المخول على شبكة حاسوب بدون هدف أوبهدف ارتكاب عمل غير مشروع وتغيير أوتعطيل عمل الحاسوب كما في حالة نشر الفيروسات.
8- **الإحتيال بإستخدام بطاقات إئتمان مزورة**: إستخدام التقنيات الحديثة لتزوير بطاقات الإئتمان.

ويرجع ذلك التعدد والتنوع إلى الانفتاح التقني والفكري لمستخدمي الحاسب الآلي سواءً كانوا جناةً أومجني عليهم. إلا أن مستويات ارتكاب هذه الجرائم في السلطنة تعتبر مطمئنة، بحيث لا تشكل تهديداً كبيراً للدولة، وعلى الرغم من ذلك ينبغي التأهب لها

نظراً لآثارها السلبية على الأمن والاقتصاد الوطني، والخطر في ذلك يكمن في التطور السريع للتقنيات الحديثة والأساليب الجرمية المتجددة والمستخدمة في هذه الجرائم من قبل الجناة، كما ان هناك صعوبات حقيقية تواجه الجهات الامنية للتوصل الى أولائك الجناة اذا كانو من الخارج لأسباب كثيرة منها:

1- التباين في الامكانات الفنية والبشرية بين دولنا العربية وبين الجناة انفسهم.
2- عدم وجود قانون يكافح الجريمة الالكترونية في الكثير من دول العالم.
3- حتى وإن وجد القانون لكن قد تظهر مصطلحات قانونية غير متعارف عليها بين دول العالم المختلفة ما يؤثر على التعاون المشترك.
4- صعوبة تسليم الجناة في الجرائم الالكترونية لعدم وجود قانون أواتفاقيات دولية تنظم ذلك.
5- عدم وجود اتفاقيات تعاون مشترك لتتبع الجرائم الالكترونية بين دول العالم وخصوصاً الأجنبية منها.
6- حتى في حال وجود تلك الاتفاقيات ففي الكثير من الاحيان يتم خرقها من خلال تجاهل طلب تسليم الجناة لأسباب تكون مجهولة غالباً.
7- مدى التغير النوعي للجريمة الإليكترونية مقارنة بالفترة السابقة: أصبح الجناة في هذه الجرائم أكثر حيطةٍ وحذر من السابق وتجلى ذلك في استخدامهم تقنيات أكثر تطوراً، وأصعب تعقباً من الجهات الأمنية كذلك نظراً لابتكار أساليب جرمية جديدة تحيل دون سهولة إلقاء القبض عليهم وإحالتهم للعدالة.

هنا نستعرض جدول لأنواع و اعداد الجرائم الالكترونية في سلطنة عمان خلال الفترة من 2003 – 2007 من واقع سجلات شرطة عمان السلطانية:

نوع القضية	عدد الجرائم	جنسية المتهمين وأعدادهم	أعمار المتهمين
الحصول على نفع غير مشروع بواسطة بيانات تخص الغير	3	- سبعة من دول شرق أسيا - اثنان من دول أوروبا الشرقية - اثنان من دول أسيا الوسطى	45 - 26
الإحتيال عبر الانترنت	6	- أربعة من دول افريقيا الجنوبية - واحد من الدول العربية - واحد من دول شرق أسيا	غير محدد الأعمار
الإحتيال بإستخدام بطاقات إئتمان مزورة	8	- خمسة عشر من دول شرق أسيا - أثنين من الدول العربية - واحد مواطن - اثنان من بريطانيا	45 - 23
إهانة الكرامة بإستخدام الحاسب الآلي	1	- مواطن واحد	19
الدخول لمواقع إباحية الخاصة بالاطفال	1	- غير معروف	غير معروف
نشر صور فاضحة للأطفال عن طريق الإنترنت	1	- غير معروف	غير معروف

إحصائيات رسمية عن القسم الخاص بشرطة عمان السلطانية

يعمل جهاز شرطة عمان السلطانية بشكل دءوب على مكافحة هذه الجرائم منذ بروزها، وعمدت إلى إنشاء إدارة مكافحة الجرائم الاقتصادية بالإدارة العامة للتحريات والتحقيقات الجنائية، والتي تعني بمكافحة هذه النوعية من الجرائم وغيرها، وتم تزويدها بجميع الإمكانيات البشرية والمادية والفنية التي تؤهلها للقيام بمهامها على أكمل وجه، كذلك تم إلحاق هذه الكوادر العاملة بالعديد من الدورات التدريبية سواءً الداخلية

أوالخارجية، وذلك لمواكبة ما شهدته هذه الجرائم من نمو وتطور سريع وقد تمخض عن ذلك الجهد حصول السلطنة على جائزة أفضل محققين في الجرائم الالكترونية في العالم للعام 2004. كما يقوم جهاز الشرطة بالمشاركة في العديد من المؤتمرات والمنتديات الدولية التي تبحث في هذه المواضيع، بحيث أن هذه الجهود المبذولة سيكون لها صدى في حماية المتعاملين في هذه الوسائل الإليكترونية، وبالتالي تعزي ثقتهم فيها.

إن الاجراءات التي تتبعها الحكومة للحد من نمو معدل الجريمة الالكترونية تعتبر جيدةً جداً إلا اننا يجب ان نقترب اكثر من الداخل، لنبحث ونتحرى عن اهم الصعوبات التي تواجه المؤسسة القضائية في التعامل مع قضايا الجرائم الالكترونية، وهذا ما تم بالفعل. حيث رصدنا اهم النقاط المشاهده في منظومة العدالة الجزائية في السلطنة:

1- **الإعتماد على مواد مضافة وعدم وجود قانون مستقل**: إن وجود نصوص ومواد قانونية منظمة للجريمة الالكترونية في سلطنة عمان كما ورد في الفصل الثاني مكرر - المادة رقم 276 - من قانون الجزاء العماني المضافة بالمرسوم السلطاني رقم 2001/72 له دور كبير بلا شك في خفظ معدل الجريمة الالكترونية، أوعلى الاقل المحافظة على نسبتها دون زيادة طوال الخمس سنوات السابقة، وذلك يشير الى تناسب بين ما ورد في القانون وبين الحجم النوعي والكيفي للجريمة الالكترونية في المجتمع العماني، إلا أننا سنحتاج بلا شك الى الاستقلالية في القانون تحسباً لإنفجار تكنلوجي قادم لا محاله، وحكومة السلطنة تعي ذلك تمامً، عليه فهي تحرص على استصدار قانون مستقل للجريمة الالكتروينة وقد انتهت من اعداده فعلاً بالرغم من عدم حاجتها نسبياً لذلك.
2- **التفسير الدقيق للمواد القانونية الحالية:** من الملاحظ ان عدم وجود قانون مستقل وواضح ينظم الجريمة الالكترونية يفتح المجال امام المفسر القانوني للذهاب الى ابعاد كثيرة قبل تكييف الجريمة وتصنيفها كجريمة إلكترونية، وربما

نفسر جريمة معينة بأنها جريمة إلكترونية تارة، ونفسرها بأنها جريمة غير إليكترونية تارة أخرى، وذلك يعتمد على المفسر للجرم المقترف. ولنأخذ مثالاً لذلك من واقع جرم منظور أمام محاكم السلطنة: قام "م" بإرتكاب جريمة تزوير من خلال تزوير بعض البيانات الحكومية المخزنة في الحاسب الآلي بقصد اصدار وثائق مزورة لتحقيق منفعة شخصية، وبطبيعة الحال إن عملية تزوير تلك الوثائق لم تتم لولا إستخدام الحاسب الآلي، وذلك يطابق تعريف الادعاء العام العماني للجريمة الالكترونية، ويطابق ما ورد في قانون الجزاء العماني الفصل ثاني مكرر المادة رقم 276 عندما قال:

'يعاقب بالسجن مدة لا تقل عن ثلاثة اشهر ولا تزيد عن سنتين وبغرامة من مائة ريال الى خمسمائة ريال أوبإحدى هاتين العقوبتين كل من تعمد استخدام الحاسب الآلي في ارتكاب أحد الافعال الأتية:

5- تزوير بيانات أووثائق مبرمجة أياً كان شكلها.

وبالرغم من تطابق الجرم مع تفسير الادعاء العام للجريمة الالكترونية، وبالرغم من صراحة المادة القانونية المذكورة سابقاً إلا انه تم تكييف الجرم اعتماداً الى أصل الفعل وهو"تزوير في وثائق رسمية" والتي قد تصل عقوبتها الى السجن مدة ثلاث سنوات.

3- **توعية هيئة القضاء بماهية الجريمة الالكترونية:** إن عدم التوعية الصحيحة لهيئة القضاء في المحاكم بماهية الجريمة الالكترونية وطرق حدوثها قد يشكل صعوبة في اتخاذ الحكم الصحيح في القضية المنظورة امام المحكمة، حتى وإن تم الاعتماد على الخبراء في مجال تقنية المعلومات للرد على اسئلة هيئة القضاء إلا انه من الممكن ان تكون هناك نسبة حتى لوكانت ضئيلة بعدم قناعة القضاء

بما هو معروض امامه لعدم فهمه الكافي للعوامل المؤثرة في حدوث الجريمة الالكترونية مما قد يؤثر على الحكم الصادر في تلك القضية.

4- **توعية العاملين في منظومة العدالة الجزائية:** من واقع البحث في هذه القضية توصلنا الى ان هناك عدم اتفاق الى حد ما على تعريف الجريمة الالكترونية في منظومة العدالة الجزائية كجهاز الشرطة والادعاء العام والمحاكم بكافة مراحلها المختلفة وحتى هيئة الدفاع، ونعود مرة اخرى لنقول ان سبب عدم وجود قانون مستقل ينظم الجريمة الالكترونية هوالسبب الأول، وعليه يجب اتخاذ الاجراءات الصحيحة في توعية العاملين في تلك المنظومة لتحقيق عدالة أفضل.

عليه، و في ختام ورقة العمل هذة نقدم لكم خلاصة ما حصلنا عليه من توصيات ومقترحات من واقع الزيارات الميدانية لمنظومة العدالة الجزائية في سلطنة عمان:

1- إن على الحكومة أن تشرع قوانين جديدة وتدعم الأجهزة الخاصة التي تتعامل مع جرائم الفضاء الحاسوبي ومن أجل أن تقوم بذلك عليها أن تراجع القوانين القائمة بهدف تعديل ما يمكن تعديله ثم تشريع ما لم يسبق وجوده. حيث أن مما يشجع المجرمين على ارتكاب الجرائم هو أن القوانين السائدة ليست واضحة في تعلقها بجرائم الفضاء الحاسوبي وان المقدرة على تطبيقها ليست صارمة.
2- من المهم بمكان تثقيف المحققين بأمور الحاسوب والشبكة ونظم المعلومات، حتى يمكن لهم جمع الأدلة الرقمية المطلوبة لتوجيه التهم. وقد لا يكون هذا العمل يسيرا حيث أنه يعني ثقافة فوق العادية في أجهزة الشرطة والتحقيقات.
3- المختبرات الجنائية في حاجة إلى المزيد من المحققين مع تقنيات متقدمة بالإضافة إلى المعرفة القانونية الصحيحة التي تمكنهم من جمع الأدلة الرقمية المهمة لتتم الملاحقة الملاحقة القانونية بنجاح.

4- توعية المواطن وتثقيفه بمفهوم الجريمة الالكترونية وما يترتب عليه من من نتائج عند التعامل مع التكنلوجيا الحديثة. فقليل من الناس يعرف ان نشر الفايروس على الشبكة هو جريمة لا تقل في الخطورة والعقوبة عن أي جريمة تخريب. كما يجب أن يعلم المواطن بأن التلبيغ عن تلك الجرائم ضروري للحد منها. وقد يكون من الحكمة أن يشمل أي تشريع جديد ضمانات للمحافظة على سرية وهوية الشخص الذي يبلغ عن اية جريمة مما قد يشجع على مبادرته للتبليغ.

5- التوعية الأمنية لأفراد المجتمع بخطورة هذه النوعية من الجرائم في مختلف وسائل الإعلام، وكذلك تبصيرهم بأي ظواهر جرمية تظهر على الساحة، وذلك بهدف وقايتهم من الوقوع في براثن هذه الجرائم.

6- دور المؤسسة التعليمية في هذه التوعية حيث ان تثقيف الطالب في أمور الحاسوب يجب ان تتضمن إفهامه بما يمكن له عمله ولا يمكن عمله وذلك وفق القوانين والقواعد الأخلاقية لإستعمال الحاسوب والشبكة.

7- العلماء والخبراء بحاجة إلى الاستمرار في البحث و الدراسة حول الأسباب التي تؤدي إلى ارتكاب الجريمة الالكترونية ومعرفة طرق الوقاية.

8- تعزيز أواصر التعاون والتنسيق المستمر بين مختلف الجهات الرسمية، والقطاع الخاص المعنية في هذا الاتجاه بهدف توحيد الجهود المبذولة.

9- الإستفادة من تجارب و توصيات البلدان المختلفة في التصدي لأساليب وطرق ارتكاب هذه القضايا لتعزيز الوسائل والإجراءات المطبقة في المكافحة والقضاء عليها.

10- تشكيل لجنة وطنية لمكافحة الجرائم الإلكترونية تختص بوضع السياسات العامة.

11- عمل ورش عمل مكثفة لمنظومة العدالة الجزائية بكافة تفرعاتها لفهم التعاملات الاكترونية الحديثة لتقليل الفجوة بين السلك القضائي و الفني خصوصاً اننا جميعاً متفقون بالطفرة التكنلوجية القادمة على مجتمعاتنا العربية.

إعـــداد:

المهندس/	الخبير القانوني/
أحمد بن سالم بن حمود السيابي	عبدالحق عبدالجبار العاني
رئيس قسم الصيانة و الشبكات	الخبير القانوني بمكتب معالي وزير العدل