



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY

ماجستير القانون الرقمي

LAW 601
أسس القانون الرقمي

المحاضرة الثالثة
الأمن السيبراني

Prepared
by Dr. Ahmed Elkhoully

محاور المحاضرة



1- أهمية دراسة الأمن السيبراني 2- ماهية الأمن السيبراني

3- التطور التاريخي للإنترنت و الأمن السيبراني 4- الأمن السيبراني و مواجهة الجريمة السيبرانية .

في إطار ما سلف من موضوعات تعرضنا فيها بالشرح و التفصيل للحاسوب و الانترنت ، ثم تطرقنا إلى الحديث عن الفضاء السيبراني و حدود سيادة الدول . أما في المحاضرة الراهنة فنكمل عقد محاور مقرر أسس القانون الرقمي فنتناول موضوع « الأمن السيبراني » ؛ كأحد أهم تلك المحاور ؛ وعليه نخوض في تلك المحاضرة في البحث عن ماهية الأمن السيبراني ؛ من خلال تحديد تعريفه ، و علاقته بالفضاء السيبراني ، و الجريمة السيبرانية . وكذا نتعرض لسبل مجابهة الجرائم السيبرانية ؛ من خلال تحديد أهداف الأمن السيبراني ، ووضع استراتيجية للأمن السيبراني ، و الحديث عن الاتفاقيات الدولية و العربية التي وضعت للتعاون الدول في مجال مكافحة الجرائم السيبرانية .

ولعل موضوع هذه المحاضرة يرتبط بتنظيم روابط القانون العام المتعلقة بالقوانين الجنائية الداخلية ؛ فيما يتعلق بتنظيم الجريمة السيبرانية كأحدى مسائل التجريم و العقاب .

ومن الأهمية أن نذكر بخطورة الجرائم السيبرانية ؛ لما تشكله من آثار بالغة على اقتصاديات الدول لفقدان الثقة في قدرتها على حماية مقدراتها ، ومن ناحية أخرى ما تشكله من آثار بالغة على النفس البشرية التي تتعرض لتداعيات تلك الجريمة القاسية على نحو ما سيتبين عند الخوض في غمار الجرائم السيبرانية . « والأمن السيبراني » واستراتيجيته السليمة هو السبيل الأوحى للخروج من مخاطر الجرائم السيبرانية .

تهدف هذه المحاضرة إلى الوقوف على ماهية الأمن السيبراني من الناحية القانونية ، وعلاقته بالجريمة السيبرانية ؛ و الأهداف الاستراتيجية للأمن السيبراني . فضلاً عن تحديد سبل مجابهة الجريمة السيبرانية .

أولاً: مقدمة

لمواكبة العصر الحديث وما حدث فيه من ثورة معلوماتية في جميع المجالات ، اتجهت غالبية الدول إلى نظام التحول الرقمي و تطبيقه على مرافقها العامة و الاستراتيجية و كذلك العسكرية . الأمر الذي قد يتسبب في أضرار جسيمة للدول حال عدم اتخاذها الإجراءات التي تؤمن فضاءها الإلكتروني و تحول دون اختراق أنظمتها الالكترونية و تضمن إحكام السيطرة على أمنها السيبراني.

أدت علاقة الفضاء السيبراني بعمل المنشآت الحيوية داخل الدول سواء أكانت مدنية أو عسكرية لقابلية تعرضها لهجوم سواء عن طريق استهدافها كوسيط وحامل للخدمات أو بشلل عمل أنظمتها المعلوماتية ، ويكون من شأنه التأثير على القيام بوظيفتها ومن ثم فإن التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة ونفوذ استراتيجية بالغة الأهمية سواء في زمن السلم أو الحرب. وتكمن خطورة حروب الإنترنت والشبكات في كون العالم أصبح يعتمد أكثر فأكثر على الفضاء الإلكتروني لا سيما في البنى التحتية المعلوماتية العسكرية والمصرفية والحكومية إضافة إلى المؤسسات والشركات العامة والخاصة. ولا شك أن ازدياد الهجمات الالكترونية والتي نشهد جزءا بسيطاً منها اليوم يرتبط أيضا بازدياد هذا الاعتماد على شبكات الكمبيوتر والإنترنت في البنية التحتية الوطنية الأساسية، وهو ما يعني إمكانية تطور الهجمات الالكترونية اليوم لتصبح سلاحا حاسما في النزاعات بين الدول في المستقبل علما بان أبعاد مفهوم الحرب الالكترونية لا تزال غير مفهومة لدى شريحة واسعة من المراقبين حتى العامة . ومن المتوقع أن تصبح الحرب الإلكترونية نموذجا تسعى إليه العديد من الجهات نظرا للخصائص العديدة التي تنطوي عليها.

مع بداية القرن العشرين برزت الثورة المعلوماتية، نتيجة التقدم العلمي التكنولوجي التقني استخدام الحاسب الآلي والأنظمة والشبكات العاملة عليه، وبالتالي ظهرت معها الجرائم الإلكترونية منذ نشأة الأجهزة الإلكترونية الحديثة وحتى وقتنا هذا، وصاحبت هذه الجرائم أيضاً ظهور البيانات والمعلومات والمستندات الإلكترونية بأشكالها وأنواعها المختلفة مثل العقود والشيكات والتوقيعات والسجلات الإلكترونية.

وأدى التطور والانفتاح التكنولوجي الذي نعيشه اليوم مع الأنظمة الإلكترونية إلى تزايد الاعتماد على هذه التكنولوجيات في التنمية الاقتصادية والاجتماعية، إلا أن الانفتاح جعلها عرضة للتعديات والأنشطة الإجرامية من قبل مخترقي الشبكات، لذلك من الضروري وضع الأطر القانونية والتنظيمية والإجرائية لمواجهة المخاطر السيبرانية وتوعية المؤسسات والأفراد حول المخاطر وآثارها على أعمالهم وحياتهم الشخصية .

ثانياً : أهمية دراسة الأمن السيبراني

تأتي أهمية موضوع هذه المحاضرة بسبب تعاظم استخدام الفضاء الإلكتروني سواء عن طريق شبكة الإنترنت أو الشبكات الأخرى واتجاه أغلبية الدول إلى التحول الرقمي . ومن هنا فإن جميع الإجراءات الحكومية سواء في التعامل مع الأفراد أو الهيئات أو الشركات الخاصة أو أسلوب التحكم في مرافقها أو الاحتفاظ بملفاتها أو إدارتها لأذرعها تأتي من خلال شبكة الإنترنت أو شبكات مغلقة تتحكم فيها الدولة ومؤمنة. إلا إن هذا التحول الرقمي كما أنه يأتي بإيجابيات عدة من سهولة ويسر وعدالة في التعاملات مما يؤثر إيجابياً في عدم ضياع الوقت وكذا إتخاذ قرارات سليمة بناء على معلومات لولا وجود هذه الشبكات ما كنا تحصلنا عليها بهذه الغزارة والجودة.

إلا انه يمكن أن يأتي بأمور سلبية عن طريق المفسدين الذين يتخذون من مواطن الضعف في هذه الشبكات منفذا لهم للدخول الى هذه الشبكات والعبث بها وارتكاب جرائم قد تصل لحد القتل في بعض الأحيان والحصول على معلومات أو أموال مما يضر بالفرد والدولة وتهتز ثقة الأفراد في أسلوب حكوماتهم في التعامل مع هذه الشبكات مما قد يزعزع استقرار الدول وحكوماتها ؛ ومن هنا وجب على جميع الدول اتخاذ الكثير من الإجراءات لحماية فضاءها الإلكتروني ومن ثم حماية مصالحها ومصالح مواطنيها.

الأمن في الفضاء السيبراني أمر اهتمت به الدول في كل مكان في العالم، بغض النظر عن مدى تواجدهم في هذا الفضاء، مما يعنى ارتباط أمن المعلومات ارتباطاً عضوياً بالأمن القومي في معظم دول العالم، ذلك أن الاعتداء على البنى التحتية المهمة منها الاتصالات الأنظمة الإلكترونية يمكن أن يؤثر على كل الدول في منطقة جغرافية معينة، المؤثر بدوره المباشر على مصالح الدولة المعنية بالفضاء السيبراني ، والتي تشكل بنيتها التحتية للاتصالات والمعلومات جزءاً من تركيبة البنية التحتية للفضاء السيبراني .

لذا احتل الاهتمام بأمن المعلومات المراكز الأولى في اهتمامات واضعي السياسات العامة في أغلب الدول، وعلى كل المستويات سواء الإقليمية أو المحلية، فالدولة لأنها المنتج الأكبر للبيانات والمعلومات العامة والخاصة، هي المعنية بالأمن السيبراني ، كما أنها المتحكمة في وضع النظم والقواعد التي تحدد الضوابط والحدود.

ثالثاً : التطور التاريخي للإنترنت و الأمن السيبراني

ويرجع إنشاء الإنترنت في بادئ الأمر في الستينيات من القرن الماضي نتاجاً لمشروع حكومي أمريكي سمي بالآربانت ARPANET ؛ وكان ذلك بهدف تأمين شبكة اتصال خاصة لا يمكن إتلافها أو تدميرها في حال حدوث عمليات تخريب أو نشوب حرب مفاجئة، وعهدت وزارة الدفاع بهذه المهمة إلى وكالة مشاريع الأبحاث المتقدمة القادرة على مقاومة الكوارث والاستمرار في العمل في حالة حدوث هجوم، وكانت هذه الشبكة تربط أربعة حاسبات آلية ضخمة فيما بينها لغرض التجربة .

و في ١٩ ديسمبر عام ١٩٦٨ م تبنت الجمعية العامة للأمم المتحدة في اجتماعها توصيات المؤتمر الأول لحقوق الإنسان المنعقد في طهران عام ١٩٦٨ والخاص بالآتي:

- (1) دراسة أثر التقدم التكنولوجي على حقوق الإنسان .
 - (2) ضرورة احترام الحياة الخاصة في مواجهة التقدم التكنولوجي .
 - (3) حماية حقوق الأفراد وحررياتهم من خطر التعدي عليها .
- أما فيما يتعلق بتبادل المعلومات بين الحاسبات بعضها البعض فقد طالبت وكالة الأبحاث المتقدمة التابعة لوزارة الدفاع الأمريكية عام ١٩٦٩ ببرتوكول للاتصالات مستقل عن أنظمة الاتصالات الأخرى لمشيدي هذه الأنظمة عن طريق حزم المعلومات ، وفي عام ١٩٧٠ تم ربط أربع جامعات أمريكية بشبكة واحدة .

وفي نهاية عام ١٩٧٠ م تم استخدام أول بروتوكول وهو x25 لربط الحاسبات الآلية التي تعمل بلغات مختلفة ببعضها البعض ، وبذات العام استخدم مصطلح الاختراق للمرة الأولى وكان التركيز على البرمجية الاستثنائية التي يمتلكها المتسلل. وفي نهاية عام ١٩٧٢ م ابتكر الباحثان BOB KAHN & VINTON CERF بروتوكول (IP / TCP) الذي تم اعتماده رسميًا ؛ ليحل محل البروتوكول السابق ، وفي عام ١٩٧٧ م أبدت منظمة التعاون الإقتصادي والتنمية اهتمامها بالمشكلات التي أثارته نظم المعلومات في الحياة الاقتصادية، وبدأ الاهتمام أيضًا بحماية الخصوصية من التهديد المعلوماتي، وأنتج هذا الاهتمام عدة قواعد لحماية البيانات الشخصية .

وفي عام ١٩٨٣ ، رأت وزارة الدفاع الأمريكية فصل الشق العسكري (milnet) عن الشبكة ، وقامت الهيئة القومية للعلوم بإنشاء شبكة NSFNET لتوصيل خمسة حاسبات تعمل بسرعة فائقة لتحل محل الأنظمة السابقة ؛ وذلك لخدمة مركز البحوث الأمريكية .

وفي أواخر الثمانينات من القرن العشرين تم اختراع شبكة الويب العالمية في جنيف بسويسرا في مختبرات CERN ، وتعني مركز الدراسات والبحوث النووية، وهي منشأة عالمية للفيزياء التجريبية والنظرية ، ويرجع الفضل في ذلك لشاب يبلغ من العمر أربعة وثلاثين عامًا يُدعى TIM BERNERSLEE ، وذلك بسبب صعوبة عثوره على المواد البحثية الخاصة به، فصمم لغة جديدة تسمى HTML ؛ وهي لغة ترميز النص التشعبي مصممة ، لمساعدة أجهزة الكمبيوتر على التحدث مع غيرها ومشاركة البيانات بشكل أفضل.

(ويمكننا القول أن لغة (HTML) هي اختصار لجملة Hyper Text Markup Language ؛ وتستخدم هذه اللغة في التنقل بين صفحات الويب العالمية بشرط توصيلها بشبكة الإنترنت ، فهي تسمح بالتجوال داخل المُتصفحات الموصولة "بالشبكة" ، ومن أشهر برامج المتصفحات هي برنامج INTERNET EX PLOER ، وبرنامج OPERA ، وبرنامج Chrome ، وبرنامج Mozilla Firefox .

وفي عام ١٩٩٤ م أوصى المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات في البرازيل والخاص بجرائم الحاسب الآلي والإنترنت بضرورة إدخال الدول بعض التعديلات على قوانينها الجنائية الداخلية .

وإدراكًا بعمق التغيرات التي أحدثتها تكنولوجيا المعلومات والعولمة الخاصة بالكمبيوتر وبمخاطر استخدام الشبكات في ارتكاب جرائم سيبرانية ، وأهمية التعاون الدولي بين الدول والقطاع الخاص ، اعتمد الاتحاد الأوروبي عام ٢٠٠١ ، اتفاقية دولية خاصة بمكافحة الجرائم الالكترونية « اتفاقية بودابست الأوروبية » .

وفي شهر مايو من عام ٢٠٠٥ ، قام الاتحاد الأوروبي بالتوسع في خطة العمل بشأن شبكة إنترنت أكثر أمانًا (safer internet plus) عن الفترة من عام ٢٠٠٥-٢٠٠٨ م ؛ وذلك لتعزيز الإستخدام الآمن لشبكة الإنترنت وما يقترن بها من تكنولوجيا حديثة لاسيما المواد غير القانونية .

وفي تقرير صادر عن الاتحاد الدولي للاتصالات (ITU) عام 2018 أشار إلى أن هناك أكثر من نصف سكان العالم موصولون بالإنترنت ، ففي البلدان المتقدمة هناك أربعة أفراد من بين كل خمسة أفراد موصولون بالإنترنت .

إن التطور التكنولوجي الخاص بتوفر الإنترنت وانتشاره عبر الأجهزة المتنقلة – أو النقالة - ، وذلك توازيا مع توافر حزمة الإنترنت العريضة قليلة التكلفة عبر تلك الأجهزة؛ أدى إلى تزايد عدد المستخدمين للإنترنت، وأيضا زيادة الاعتماد على هذا النوع من التكنولوجيا في التنمية الاجتماعية والاقتصادية، غير أن ما يميز شبكة الإنترنت والفضاء السيبراني – بشكل عام – هو الانفتاح، وهذه الميزة جعلتها عرضة للنشاط الإجرامي وتعيدياته، الأمر الذي جعل مستخدم الفضاء السيبراني يتعرضون للانتهاكات من قبل مخترقي الشبكات . وهذا ما دعى إلى ضرورة وضع أطر إجرائية لمواجهة تلك المخاطر السيبرانية، ونشر الوعي الخاص بخطورة هذه التعديات على مستوى الأفراد والمؤسسات، وأثارها السلبية على أعمالهم.

ومن الخطوات الجيدة التي اتخذت في شأن الأمن السيبراني هو استحداث الاتحاد وهو الدولي للاتصالات التابع للأمم المتحدة مؤشر عالمي للأمن السيبراني (GCI) وهو اختصار لـ GLOBAL CYBER SECURITY INDEX، و ذلك لتحديد مدي تطور الدول في مجال الأمن السيبراني .

رابعاً: ماهية الأمن السيبراني

تمهيد و تقسيم :

مع تراجع مبادئ الأخلاق و ضعف البيئة القانونية الحاكمة للمجال الافتراضي أصبحت معايير الأمن من أهم متطلبات المعاملات الالكترونية ؛ حيث ظهرت العديد من الآثار السلبية للاقتصاد الرقمي على بيئة الأعمال ، خصوصاً فيما يتعلق بالأمن ، حيث ظهرت الجرائم الالكترونية و الغش التجاري و انتهاك الخصوصية و سرية المعلومات .

فضلاً عن ذلك فإن المستثمرين في أي دولة في العالم إذا لم يجدوا من الأنظمة و القوانين ما يواجهه الجرائم السيبرانية التي تقوض الصناعات المعلوماتية ، و إذا لم يجدوا دعماً من الدولة ، و حضوراً لأجهزتها لتنفيذ تلك الأنظمة و القوانين ؛ فإنهم يبدلون واجهتهم للاستثمار و التطوير في مكان آخر ، وهو ما يؤثر بالسلب على الاقتصاد .

3

تعريف الأمن السيبراني

خصائص الأمن السيبراني

المصطلحات المرتبطة بالأمن السيبراني

الأمن السيبراني و الجريمة السيبرانية

3

تعريف الأمن السيبراني

وتوجد صعوبة لإيجاد تعريف شامل للأمن السيبراني ؛ باعتباره مصطلح متغير ينظم و يجمع كافة الموارد و العمليات و الهياكل المستخدمة لحماية الفضاء الالكتروني و الأنظمة التي تدعم الفضاء الالكتروني من الأحداث التي تتماشى بحكم القانون مع حقوق الملكية الفعلية .

هنالك عدد من التعاريف الوطنية والدولية لمصطلح "الأمن السيبراني". يُقصد من مصطلح "الأمن السيبراني" وصف مجموعة الأدوات والسياسات والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وآليات الضمان والتقنيات التي يمكن استخدامها في حماية توفر وسلامة وسرية الأصول في البنى التحتية الموصولة التابعة للحكومة والمنظمات الخاصة والمواطنين، وتشمل هذه الأصول أجهزة الحوسبة الموصولة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات والبيانات في البيئة السيبرانية.

وتعددت تعريفات الأمن السيبراني، حيث عرفه فريق العمل المشترك المعني بتعليم الأمن السيبراني في جامعة جورج واشنطن أنه نظام قائم على الحوسبة يشمل التكنولوجيا والأشخاص والمعلومات والعمليات المؤكدة ، ويشمل إنشاء وتشغيل وتحليل واختبار أنظمة الكمبيوتر الآمنة . إنها دورة دراسة متعددة التخصصات ، بما في ذلك الجوانب القانونية والسياسية والعوامل البشرية والأخلاق وإدارة المخاطر .

- وقد عرف الاتحاد الدولي للاتصالات (ITU) الأمن السيبراني في تقرير صادر عام 2010 أنه مجموعة من المهمات ، مثل تجميع وسائل و سياسات و إجراءات أمنية ومبادئ توجيهية وأساليب إدارة المخاطر ، و تدريبات و ممارسات و تقنيات تستخدم لحماية البيئة السيبرانية والمؤسسات والمستخدمين .
- بينما عرفتة جامعة أوكسفورد في ورقة بحثية لها في عام 2014 بأنه حالة الحماية من الاستخدام الإجرامي أو غير المصرح به للبيانات الالكترونية ، أو الإجراءات المتخذة لتحقيق ذلك .
- وعرفه البعض أنه عبارة عن مجموع الوسائل التقنية والإدارية التي يتم القيام بها لمنع الاستخدام غير المشروع ، وسوء الاستغلال للمعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها . بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات الشخصية ولحماية المواطنين من المخاطر في الفضاء السيبراني " .
- وقيل أيضاً في تعريفه أنه فن ضمان وجود واستمرارية مجتمع المعلومات لدولة ما ، وضمان وحماية المعلومات والمجموعات والبنية التحتية الحيوية في الفضاء السيبراني.

خصائص و سمات الأمن السيبراني :

يتميز الأمن السيبراني بعدة سمات ومن أهمها :

- ١: الأمن السيبراني ليس مسار عمل لمرة واحدة ؛ إنما هو عملية مستمرة ويحتوي على آليات دفاع مبتكرة لكونه يواجه التهديدات التي تقع على الأنظمة والشبكات وغيرها .
- ٢: يعمل على خلق نظام بيئي سيبراني آمن وإنشاء نظام موثوق به .
- ٣: يقوم بعملية وقائية رقابية مسبقة بهدف البحث عن المخاطر والعمل على حلها وسد الثغرات .
- ٤: يعمل على الدفاع اللاحق والذي يتمثل في قاعدة إرجاع الوضع إلى ما كان عليه .
- ٥: يوفر خاصية التنبيه إلى وجود خطأ أو إساءة استخدام الشبكات التي تعرض البيانات والمعلومات إلى الخطر من داخل المؤسسات وأيضاً تغطية المخاطر الخارجية ومراقبة التهديدات .

المصطلحات المرتبطة بالأمن السيبراني

يتبع الأمن السيبراني نهجاً محدداً يتكون من عدة طبقات للحماية تثبت في أجهزة الحاسب أو الشبكات أو البرامج أو البيانات التي ينوي المستخدم حمايتها . وتوجد مجموعة من المصطلحات ترتبط بالأمن السيبراني نذكر منها :

الفضاء السيبراني (Cyber Space):

عبارة عن بيئة تفاعلية رقمية تشتمل عناصر مادية و غير مادية مكونة من مجموعة من الأجهزة الرقمية و أنظمة الشبكات و البرمجيات ، و المستخدمين سواء مشغلين أو مستعملين .

الردع السيبراني (Cyber Deterrence) :

يعرف على أنه منع الأعمال الضارة ضد الأصول الوطنية في الفضاء الرقمي و الأصول التي تدعم العمليات الفضائية.

الهجمات السيبرانية (Cyber Attacks) :

وهو أي فعل يقوض من قدرات ووظائف شبكة الحاسوب لغرض شخصي أو سياسي من خلال استغلال نقطة ضعف معينة تمكن المهاجم من التلاعب بالنظام . و قيل أيضاً أنه أي نوع من أنواع الأنشطة الخبيثة التي تسعى إلى الوصول بشكل غير مشروع إلى المعلومات أو جمع موارد النظم المعلوماتية ، أو تعطيلها أو منعها أو تحطيمها أو تدميرها .

الجريمة السيبرانية (Cyber Crime) :

مجموعة من الأفعال و الأعمال غير القانونية التي تتم عبر معدات أو أجهزة الكترونية عبر شبكة الانترنت ، و تتطلب حكماً خاصاً بتقنيات الحاسوب و نظم المعلومات لارتكابها أو التحقيق فيها أو مقاضاة فاعليها .

الجريمة السيبرانية كتهديد للأمن السيبراني

يرتبط الأمن السيبراني بالجريمة السيبرانية التي هي أساس الأمن المعلوماتي الذي يعمل على مكافحتها، وهي عبارة عن جرائم ذكية تنشأ في البيئة الإلكترونية أو الافتراضية، حيث يقوم بها أفراد أو منظمات لديهم درجة عالية من الذكاء ويمتلكون المعرفة والتقنية، مما يتسبب في خسائر فادحة للمجتمع.

كما أدى ظهور الجرائم السيبرانية كنمط جديد من أنماط الجريمة إلى توجيه المجتمع الدولي للتعاون من أجل تصد دماغ لتلك الجرائم التي لها بالغ الأثر السلبي، حيث تعتمد أغلب المجتمعات على تقنيات الاتصالات والمعلومات، ومع ذلك الاعتماد المستمر تصاحبه مخاطر ناشئة ومحتملة تهدد تلك الشبكات، وتؤثر بالسلب على البنية التحتية للمعلومات الوطنية الحساسة، وخاصة المعلومات الشخصية والأمن الفكري.

أدى التقدم العلمي والتقني في مجال الاتصالات وظهور شبكة الإنترنت وتضخمها وامتدادها إلى كل أقاليم الدول تقريباً إلى تنوع وتعدد الأنشطة الإجرامية التي ترتكب من خلالها وعبر عدة دول.

ومن ثم يستلزم الأمر الوقوف على ماهية الجريمة السيبرانية وخصائصها ؛ حتى نتمكن من الوقوف على أهداف الأمن السيبراني و استراتيجيات الأمن السيبراني المثلى .

3

تعريف الجريمة السيبرانية

خصائص الجريمة السيبرانية



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

www.esu.ac.ae

تعريف الجريمة السيبرانية

لقد حاولت عدة أعمال أكاديمية تعريف "الجريمة السيبرانية"، وفي هذا الصدد، لم يبد التشريع الوطني اهتماماً إزاء وجود تعريف دقيق للكلمة. وفي دراسة مجراة بمعرفة مكتب الأمم المتحدة المعني بالمخدرات و الجريمة في عام 2014 ، وجد أن عدداً من الدول أشارت إلى ما يقرب من 211 مادة من مواد التشريع الوطني، فأقل من 2 في المائة استعملت كلمة "جريمة سيبرانية" في عنوان التشريع أو في نطاق الأحكام التشريعية. ومن المسميات الأكثر شيوعاً، إلى حد ما، في التشريعات؛ " جرائم الحاسوب"، " الاتصالات الإلكترونية"، " تكنولوجيا المعلومات"، أو " جرائم التكنولوجيا المتقدمة".

فمن الناحية العملية، قننت العديد من هذه التشريعات جرائم جنائية والتي تم تضمينها في مفهوم الجريمة السيبرانية، مثل النفاذ غير المشروع إلى نظام حاسوبي، أو التدخل في النظم الحاسوبية أو البيانات الحاسوبية. فإذا استخدم التشريع مصطلح "جريمة سيبرانية" بشكل محدد في عنوان أحد القوانين أو الفصول مثل: "قانون الجريمة السيبرانية" (فنادراً ما يشتمل الفصل التعريفي في التشريع على تعريف لكلمة "جريمة سيبرانية". وعندما تم إدراج مصطلح "جريمة سيبرانية" كتعريف قانوني، فالنهج الشائع قد دأب على تعريفها بـ " الجرائم المشار إليها في هذا القانون".

ومن ضمن الجهود نحو وضع تعريف للجريمة السيبرانية ، ما ورد بالقانون العربي النموذجي في شأن مكافحة جرائم الحاسوب و الانترنت الذي صيغ في جامعة الدول العربية بين مجلس وزراء الداخلية العرب و مجلس وزراء العدل العرب في 22 مايو 2003 ، حيث عرف الجريمة الالكترونية في المادة الأولى منه أنه كل فعل مؤثم يتم ارتكابه عبر أي وسيط الكتروني .

3

ثمة سؤال يطرح حول إن كان من الممكن تحديد أهداف أو سمات أو أسلوب الجريمة السيبرانية، بدلا من تحديدها استنادا إلى قائمة من أفعال فردية من الجريمة السيبرانية؟ وعلى النحو المذكور أعلاه، فإن مثالا على هذا النهج يمكن أن نجده في اتفاقية دول الكومنولث المستقلة، حيث تصف "الجريمة المتعلقة بالمعلومات الحاسوبية" بأنها "فعل إجرامي هدفه المعلومات الحاسوبية". بينما تصف اتفاقية منظمة شنغهاي للتعاون على نطاق أوسع "جرائم المعلومات" بأنها "استخدام موارد المعلومات و)أو(التأثير عليها في الفضاء المعلوماتي لأهداف غير مشروعة". أما اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية – وعلى الرغم من عدم تعريفها للمصطلحات – فإنها تستخدم عناوين تجريم واسعة، تشتمل على "جرائم ضد سرية، وسلامة، وتوافر البيانات والأنظمة الحاسوبية"، و "جرائم ذات صلة بالحاسوب"، و "جرائم ذات صلة بالمحتوى". أما مشروع قانون الاتحاد الأفريقي، فيستخدم على نحو مشابه عناوين تجريم تميز بين "جرائم خاصة بتكنولوجيات المعلومات والاتصال" و "جرائم ذات تكييف قانوني محلها تكنولوجيات المعلومات والاتصال". وابتناء على ما تقدم، فإن تلك المواثيق الدولية قد أفصحت عن إمكانية تحديد الجريمة السيبرانية من خلال وضع قائمة بالأفعال التي تشكل جرائم سيبرانية.

3

الأفعال التي تشكل الجريمة السيبرانية

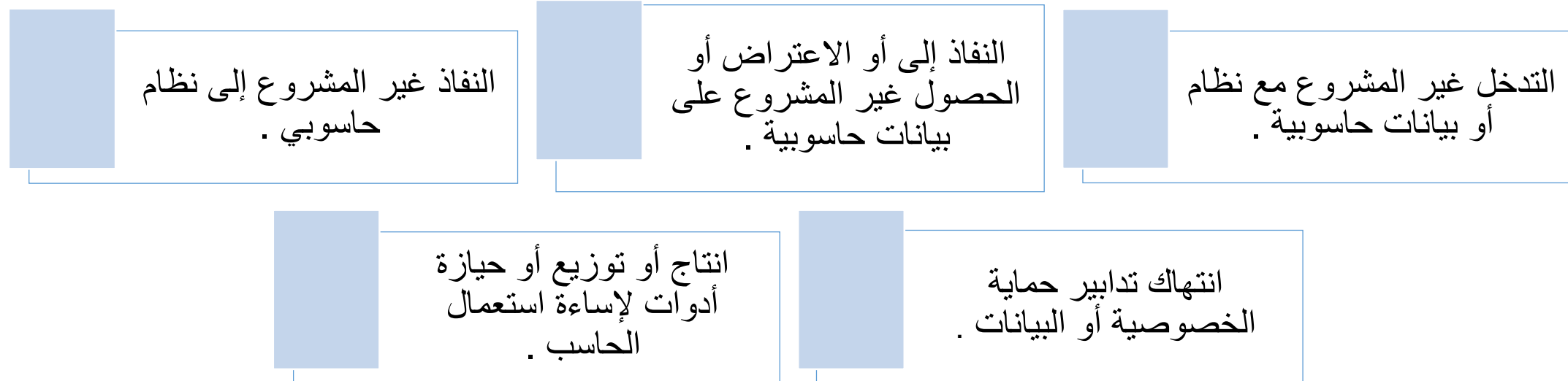
أفعال ضد سرية و نزاهة وتوافر البيانات أو
النظم الحاسوبية

أفعال متعلقة بالحاسوب تهدف إلى كسب
شخصي أو مالي أو إضرار

أفعال متعلقة بمحتوى الحاسب



1- أفعال ضد سرية و نزاهة وتوافر البيانات أو النظم الحاسوبية



2- أفعال متعلقة بالحاسوب تهدف إلى كسب شخصي أو مالى أو إضرار

- الاحتيال أو التزوير المتعلق بالحاسب .
- جرائم الهوية المتعلقة بالحاسوب.
- جرائم حقوق الطباعة و العلامة التجارية المتعلقة بالحاسوب .
- إرسال أو التحكم في إرسال البريد الالكتروني الطفيلي .
- الأفعال المسببة لأذى شخصي و المتعلقة بالحاسوب .
- إغواء أو استمالة الأطفال لأغراض جنسية من خلال الحاسوب .

3- أفعال متعلقة بمحتوى الحاسوب

الأفعال المرتكبة بواسطة الحاسوب و المنظوية على خطاب كراهية .

انتاج أو توزيع أو حيازة مواد إباحية متعلقة بالأطفال بواسطة الحاسوب .

أعمال دعم جرائم الإرهاب بواسطة الحاسوب .

خصائص الجريمة السيبرانية

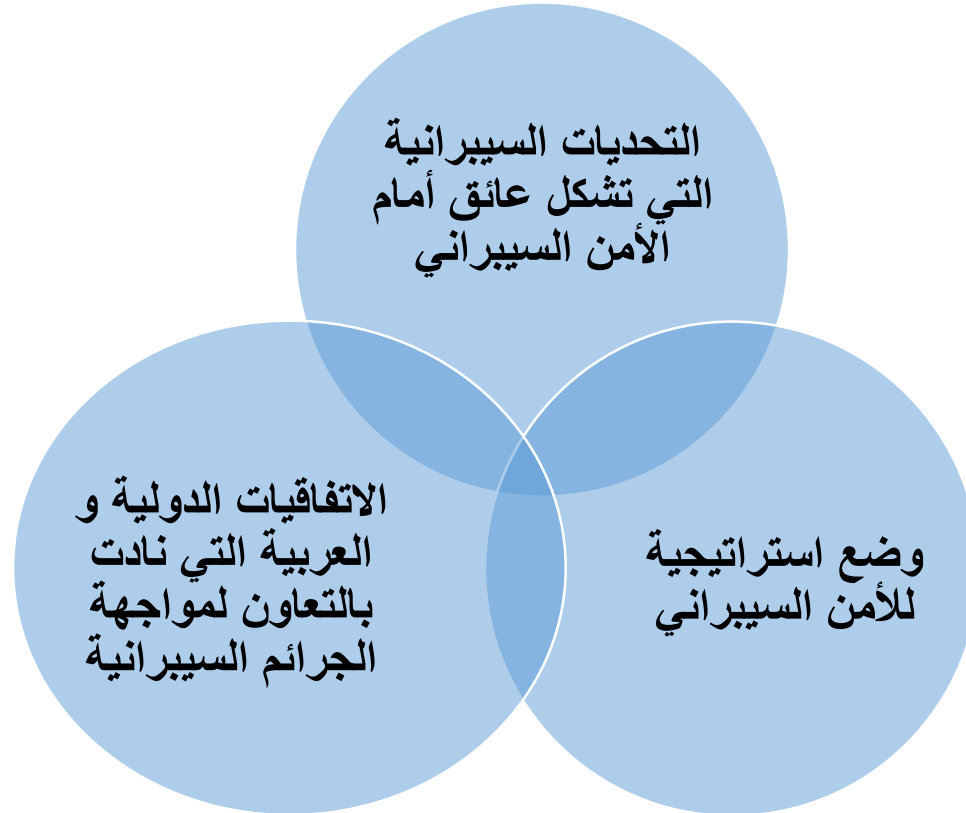
الجريمة السيبرانية هي امتداد طبيعي لنمو أجهزة الكمبيوتر، وقد نمت الجريمة السيبرانية بشكل هائل على مدى العقدين الماضيين، وتطورت الجريمة من قضية ثانوية إلى ظاهرة عالمية، مما يؤثر على أعداد غير مسبوقة من الأفراد وتسبب الملايين من حالات الإيذاء في كل عام، ومن آثار هذه الجرائم السيبرانية تتراوح الخسارة المالية بالمليارات وخسارة الكثير من الوقت في سرقة الهوية والاحتيال، وتسبب في الاضطراب العاطفي المرتبط بالقلق، والاكتئاب، أو حتى الأفكار الانتحارية .

وتتميز الجريمة السيبرانية بطائفة من الخصائص التي جعلتها متفردة فهي صورتها عن باقي الجرائم الأخرى، بالنظر إلى مجموعة المعطيات الخاصة بها بالدرجة الأولى، سواء معن ناحية أداء ارتكابها أو مرتكبيها، أو حتى كيفية إثباتها ومعاينتها. وتتمثل تلك المعطيات فيما يلي:

1 - إن طبيعة الجرائم السيبرانية وتمييزها عن الجرائم التقليدية يرجع إلى البيئة التي ترتكب فيها الجريمة وهي الأداة أو الوسيلة التي استخدمها الجاني في ارتكاب فعله غير المشروع، وتتطلب توفر معرفة أو حد أدنى من الثقافة التقنية لدى الجاني، وهي لا تخرج عن كونها سلوك إجرامي جرمه القانون، وتتجه إرادة الجاني إليه، رغم وجود نص قانوني يجرم السلوك.

- 2- الجريمة الإلكترونية ذات بعد دولي، عابرة للحدود، فهي تتجاوز الحدود الجغرافية بسبب تنفيذها عبر الشبكة المعلوماتية، وهو ما يثير في كثير من الأحيان تحديات قانونية فنية، بل سياسية بشأن مواجهتها، لاسيما فيما يتعلق بإجراءات الملاحقة الجنائية.
- 3- صعوبة الكشف عن مرتكب الجريمة السيبرانية إلا بأساليب أمنية وتقنية عالية.

خامساً: الأمن السيبراني و مواجهة الجريمة السيبرانية



التحديات السيبرانية التي تشكل عائق أمام الأمن السيبراني

- 1- سهولة محو الدليل أو تدميره .
- 2- انتشار كوفيد 19
- 3- الأخطاء البشرية للموظفين بالشركات
- 4- التطبيقات الضارة
- 5- كثرة برامج التجسس و الثغرات الأمنية
- 6- استخدام المخترقين شبكات WIFI
- 7- البريد الالكتروني العشوائي
- 8- التهديد و الابتزاز
- 9- الإيهام بالجوائز
- 10- جرائم الملكية الفكرية

خطوات تحديد أهداف الأمن السيبراني

الهدف الاستراتيجي للأمن السيبراني هو حماية الفضاء السيبراني ؛ يهدف الأمن السيبراني بشكل عام إلى مواجهة الجرائم السيبرانية ومخاطرها، ويهدف إلى تعزيز الثقة في البنى التحتية للاتصالات والمعلومات وتطبيقاتها وخدماتها في جميع المجالات والقطاعات، والعمل على تأمينها من خطر الاختراق، وذلك تحقيقاً لبيئة رقمية تتصف بالأمان.

يعد إنشاء قدرة وطنية لإدارة الحوادث مهمة طويلة الأجل تبدأ بإنشاء مجموعة فرق وطنية للاستجابة لحوادث الأنظمة الإلكترونية منها تحديد أو إنشاء قدرات وطنية لفرقة Cyber Incident Response Team ووضع آليات داخل الحكومة الوطنية للتنسيق بين القطاعين المدني والحكومي.

ولم تنشأ أغلب الدول العربية هيئة وطنية للأمن السيبراني باستثناء بعض الدول التي بعثت مثل هذه الهيئات بتسميات مختلفة، أما في بعض الدول العربية الأخرى، فنلاحظ إحداث مجالس وهيئات عدة لها دور هام في تحديد الرؤية الإستراتيجية الوطنية للأمن السيبراني وفي وضع البرامج العملية لتحقيقها، تتخذ في بعض الأحيان شكل مجالس، وفي أحيان أخرى شكل هيئات إدارية تابعة لرئاسة الجمهورية أو للوزارة المكلفة بالأمن أو بالدفاع الوطني أو بالعدل، مثلما هو الشأن في مصر المتمثل في المجلس الأعلى للأمن السيبراني التابع لمجلس الوزراء، و الجزائر المتمثل في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، أما في الكويت فتباشر الهيئة العامة للاتصالات وتقنية المعلومات الاختصاص المتعلق بمهام ومسؤوليات الأمن السيبراني وغيرها في مجال حماية البيانات الشخصية.



يقع على عاتق الحكومة إنشاء أو تحديد منظمة وطنية تعمل كجهة اتصال وذلك لضمان حماية الفضاء السيبراني والعمل على حماية البنية التحتية الحيوية للبيانات والمعلومات، تتضمن مهام هذه المنظمة المراقبة والإنذار والاستجابة وجهود التعايش وتيسير التعاون بين الكيانات الحكومية والقطاع الخاص بالإضافة إلى الدوائر الأكاديمية والمجتمع الدولي .

وركزت العديد من الدراسات على المسؤولية الجنائية عن إساءة استخدام وسائل التواصل الاجتماعي وتحديد جرائم الاعتداء على الحياة الخاصة، والسب والقذف، والمسام بالقيم الدينية، و الاعتماد على تحليل قوانين مكافحة جرائم تقنية المعلومات . أظهرت النتائج أن المشرع حرص في كل من عمان والكويت وقطر والإمارات العربية المتحدة على تجريم الآراء التي تؤدي إلى الفتنة بين أفراد المجتمع، أو التي تمس القيم الدينية أو النظام العام في الدولة، كما جرم الاعتداء على الحياة الخاصة والسب والقذف باستخدام وسائل التواصل الاجتماعي، ويتم ذلك من خلال قانون مكافحة جرائم تقنية المعلومات في كل بلد.

وضع استراتيجية وطنية للأمن السيبراني ومكافحة الجرائم السيبرانية

تمهيد :

ليس بإمكان الحلول التقنية وحدها أن تعالج بشكل كاف جميع مشكلات الجريمة الالكترونية و التهديدات الأخرى التي تحيق بالفضاء الالكتروني ، فالأنظمة و التحقيقات و الإجراءات القانونية ضرورية أيضاً . و نظراً إلى قدرة المهاجمين في بلد ما على استهداف الأنظمة في بلد آخر ، فلا بد من وضع آليات تتيح إمكانية التحقيق و المقاضاة دولياً .

تتمثل الخطوة الأولى في هذا الإطار بوضع استراتيجية متكاملة للأمن السيبراني و مكافحة الجرائم السيبرانية، وتتضمن هذه الاستراتيجية نواحي مختلفة، منها التشريعي والتنفيذي والتنظيمي والتثقيفي .
بناء على التجارب الدولية، يوصي بأن تتضمن استراتيجية الأمان السيبراني ومكافحة الجريمة السيبرانية في كل دولة البنود التالية كحد أدنى:

- ١- وضع التشريعات السيبرانية الضرورية وتحديثها.
- ٢- وضع منهجية للاستجابة للحوادث السيبرانية، وبوجه خاص إنشاء مراكز للاستجابة السريعة لطوارئ الحاسوب، ووضع أسس التواصل والتعاون بين هذه المراكز في المنطقة العربية .
- ٣- دعم صناعة البرمجيات والتجهيزات والحلول التقنية الخاصة بالحماية من المخاطر السيبرانية.

- 4- تعزيز الشراكة بين القطاع العام والخاص، وبخاصة فيما يتعلق بحملات التوعية، وتطوير الحلول التقنية، وحفظ معلومات حركة البيانات وبيانات التعريف عن المستخدمين، والتمويل.
- 5 - تشجيع اعتماد الهوية الإلكترونية للمستخدمين على الشبكة، وبوجه خاص عند الدخول إلى الأنظمة ذات الطبيعة الحساسة، كالأنظمة المالية.
- 6- تطوير نظام التبليغ السريع عن الجرائم السيبرانية بحيث يعتمد على السرية ويضمن حقوق المرأة والطفل.
- 7- اعتماد المؤشرات التي تراعي النوع الاجتماعي وتسمح بتقصي مستوى الجريمة السيبرانية، وتحديثها دورياً.
- 8 - التوعية الحثيثة والمستمرة حول الأمن السيبراني والجرائم السيبرانية للمؤسسات والأفراد.
- 9- تعزيز التدريب والتأهيل في مجال الأمن السيبراني، بغية زيادة عدد المتخصصين في هذا المجال.
- 10 - إقرار مبدأ التعاون في محاربة الجرائم السيبرانية ضمن إطار الأمم المتحدة، بغية زيادة تبادل المعلومات بين الأجهزة الرسمية.

بداية، ينبغي على كل دولة العمل على تحديث تشريعاتها، وسن قوانين لتجريم الجرائم السيبرانية؛ فقوانين العقوبات التقليدية ليست صالحة على الدوام الحكم هذه الأفعال الجرمية الجديدة، على الأقل في حالة الأفعال التي تكون فيها المعلوماتية محلاً لا اعتداء. وكذلك ينبغي العمل باستمرار على تحديث التشريعات لمواكبة التطور التقني والأساليب المبتكرة التي يعتمد عليها المجرمون وإعادة النظر في العقوبات وفي ظروف تشديدها وفق ما يظهر من ممارسات إجرامية.

(أ)- اجراء مسح وطني شامل للتشريعات ذات الصلة:

بغية وضع سياسة تشريعية فعالة ومستندة إلى معطيات علمية ودقيقة، ينبغي للدولة القيام بدراسة شاملة وتفصيلية للقوانين الموجودة فيها قبل المسارعة إلى وضع قوانين جديدة .

(ب)- تحديث تشريعات الجرائم السيبرانية وايجاد حلول البعض إشكالياتها:

تحتاج التشريعات الوطنية إلى التحديث دورياً خاصة في مكافحة الإشكاليات القانونية الناتجة عن طبيعة الفضاء السيبراني، ومن تلك الإشكاليات، علم وضع تعريف واضح وموحد للجرائم السيبرانية عامة في دولة معينة، حيث يبدو غير ذي أولوية، باعتبار أنه من الأهم وضع تعريفات محددة في التشريع الداخلي لكل جريمة سيبرانية تبين أركانها وعناصرها، تطبيقاً لمبدأ "لا جريمة ولا عقوبة دون نص قانوني". ومن المسلم به أن القواعد القانونية الإجرائية التقليدية في الدول العربية المتعلقة بتنظيم آليات التحقيق في الجرائم الجزائية عاجزة عن حكم قضايا جرائم المعلوماتية نظراً للطبيعة الخاصة لها، فالمعلوماتية تمتاز بالطابع اللامادي والتقني المتخصص وبالقدرة على الزوال بسرعة وباختراق الحدود وبوجود هوية إلكترونية مختلفة عن الهوية الحقيقية وبالقدرة على إحداث أضرار جسيمة عن بعد، فلا بد من تحديث هذه القواعد.

(ت): تنسيق التشريعات بين الدول العربية والاسترشاد بإرشادات الإسكوا للتشريعات السيبرانية:

ينبغي توحيد المقاربة التشريعية بين الدول ، أو على الأقل تنسيقها. كما ينبغي وضع تعاريف موحدة أو متناسقة، للجرائم السيبرانية وكذلك ينبغي وضع سلم متناسق للعقوبات؛ إذ يمكن التغلّت من الملاحقة إذا كانت دولة معينة تجرم فعلا معينا في حينلا تجرمه دولة أخرى. كما أن التعاون بين الأجهزة الرسمية فيما بين الدول لا يكفيلوحده، بل يعتبر إشراك القطاع الخاص ذا أهمية، خاصة الشركات التي توفر التجهيزات والبرامج المعلوماتية وكذلك شركات الاتصالاتإن معظم الدول ترفض التعاون إذاكان الفعل الجرمي المرتكب في دولة أخرى غير مجرم في قانونها الداخلي (التجريم المزدوج)، فالتعاون بين الدول يقتصر على الجرائم المجرمة في جميع هذه الدول. فطالماأن التقنيات المستخدمة في مجال تكنولوجيا المعلومات هي نفسها على مستوى العالم، فمن الأولى أن تكون تعاريف الانتهاكات المستندة إلى هذه التقنيات ذاتها".

كما يمكن للدول الأسترشاد في سن تشريعاتها المتعلقة بالجانب الموضوعي وبقسم من الجانب الإجرائي بإرشادات الإسكوا للتشريعات السيبرانية التي صدرت عام ٢٠١٢، وهي ملائمة للتطبيق في الدول ذات النظام القانوني المبني على القانون اللاتيني، وذلك باعتبار أن هذه الإرشادات مستوحاة من إرشادات الاتحاد الأوروبي والقوانين الفرنسية والأوروبية.

وقد تضمنت إرشادات الإسكوا للتشريعات السيبرانية لعام ٢٠١٢ القواعد الموضوعية المتعلقة بهذه الجرائم، ومنها التعدي على البيانات المعلوماتية، والتعدي على الأنظمة المعلوماتية وإساءة استعمال الأجهزة أو البرامج المعلوماتية، والتعدي على الأموال والمعاملات بوسائل إلكترونية، وجرائم الاستغلال الجنسي للقاصرين بوسائل معلوماتية، والتعدي على الملكية الفكرية للأعمال الرقمية، وجرائم البطاقات المصرفية والنقود الإلكترونية، وجرائم المعلومات الشخصية، وجرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية، والمقامرة وترويج المواد المخدرة بوسائل معلوماتية. وجرائم المعلوماتية ضد الدولة والسلامة العامة، وتشفير المعلومات. ومن ثم فقد تضمن الإرشاد النوع الأول من جرائم المعلوماتية، حيث تكون المعلوماتية موضوع الفعل الجرمي، كالاغتداء على الأنظمة المعلوماتية، وكذلك النوع الثاني من الجرائم المعلوماتية، حيث تكون المعلوماتية هي وسيلة ارتكاب فعل جرمي تقليدي كالاختيال أو السرقة أو السب. ولم ينظم الإرشاد القضايا الإجرائية في التحقيقات القضائية، بل أشار فقط في مادة وحيدة إلى التعاون الدولي في هذا المجال، حيث تنص المادة 56 على أنه على الدول الأعضاء أن تلتزم المعاهدات والاتفاقيات الدولية ذات الطابع الجماعي أو الثنائي المتعلقة بمكافحة الجرائم عموماً، مع مراعاة طبيعة الجرائم السيبرانية، وذلك من حيث تسهيل وتسريع الإجراءات الخاصة بجمع الأدلة وضبطها وتبادل المعلومات حول الجرائم المذكورة وملاحقة مرتكبيها، كما تحرص الدول الأعضاء على التعاون فيما بينها في مجال التحقيقات القضائية في جرائم المعلوماتية، وأعمال رصدها ومكافحتها.

(ث) – الاسترشاد باتفاقية بودابست:

يمكن الاسترشاد بالقواعد الإجرائية الأساسية في مجال تحقيقات جرائم المعلوماتية التي يمكن العودة إليها أيضا في اتفاقية بودابست، حيث تقوم الدول العربية بإدخال مبادئها ضمن أنظمتها القانونية. وتتمحور القواعد الإجرائية حول إعطاء أجهزة التحقيق الصلاحيات التالية:

- إلزام أي شخص يحفظ بيانات معلوماتية، ومنها معلومات حركة البيانات. (Traffic data)
- إلزام مزودي خدمات الاتصال بتزويد أجهزة التحقيق بمعلومات حركة البيانات وبيانات التعريف الشخصية حول أصحاب المواقع الإلكترونية subscriber information التي يستضيفونها، وإلزام أي شخص بتزويدها ببيانات معلوماتية محددة هي بحوزته.
- الوصول إلى أنظمة الحاسوب والمعلومات وضبطها.
- الوصول إلى معلومات حركة البيانات في زمن الإرسال الحقيقي، إما مباشرة أو عن طريق مزودي خدمات الاتصال.
- الوصول إلى محتوى الاتصال أو المعلومات بذاتها content data في زمن الإرسال الحقيقي، إما مباشرة أو عن طريق مزودي خدمات الاتصال.
- إلزام أي شخص لديه معلومات حول طرق عمل نظام معلوماتي والتدابير التقنية لحمايته بالمساعدة على ضبط البيانات أو النظام)
- إعطاء الصلاحية القضائية المحاكم البلد الذي وقع فيه الجرم أو في حال وجود المتهم على أراضي هذا البلد، وعدم إجابة طلب الاسترداد المقدم من بلد أخرج بسبب جنسية المتهم التابع البلد الأول.

ج) إنشاء وحدات متخصصة لتطبيق القانون:

أشارت إرشادات الإسكوا للتشريعات السيبرانية بمادة وحيدة إلى التطويرات البنيوية في الهياكل التنظيمية للسلطات بهدف محاربة جرائم المعلوماتية، عن طريق إنشاء وحدات متخصصة في أجهزة الشرطة التي تتولى التحقيقات الجزائية، حيث تنص المادة 55 على أنه "تحرص الدول الأعضاء على إنشاء وحدة متخصصة في جرائم المعلوماتية في الأجهزة الأمنية المولجة بالتحقيقات القضائية تحت إشراف القضاء، كالضابطة العدلية تتولى هذه الوحدة أعمال التحقيق في هذه الجرائم ورصدها تحت إشراف القضاء. ويتألف الجهاز البشري لهذه الوحدة من عناصر فنية متخصصة ذات كفاءة في مجال المعلوماتية والاتصالات».

ومن الأهمية بمكان التنسيق فيما بين الوزارات والهيئات المتخصصة في البلد الواحد من أجل مكافحة الجرائم السيبرانية وخاصة وزارة العدل ووزارة الاقتصاد ووزارة الاتصالات ووزارة الداخلية وذلك بهدف منع التضارب في الصلاحيات والاختصاصات وتعزيز التعاون فيما بينها وتدريب العاملين المعنيين فيها على التشريعات السيبرانية وصولاً إلى التعاون لمكافحة الجرائم السيبرانية. وبهدف التعامل مع خصوصيات المرأة، ينبغي أن تتوفر لدى فرق التحقيق خبرات في التعامل مع الجرائم السيبرانية التي يمكن أن تركز على العنف القائم على النوع الاجتماعي أو العنف ضد المرأة، خاصة عندما تكون الضحية امرأة، إضافة إلى إدخال عناصر نسائية ضمن فرق التحقيق لديها خبرات كافية بالجرائم السيبرانية.

وينبغي أيضا أن يكون لدى أعضاء النيابة العامة خبرة في هذا الموضوع حتى يتمكنوا من ملاحقة المذنبين بارتكاب جرائم سيبرانية ترتبط بالنوع الاجتماعي، دون التأثير على الصحة البدنية والعقلية للضحايا وفي جميع الأحوال، تكمن مهمة النيابة العامة في توجيه المحققين خلال التحقيقات وتحديد الأدلة المعلوماتية المطلوب جمعها لإثبات الوقائع الجرمية وتطوير الآليات والنماذج لمذكرات التفتيش والتوقيف والعمل على توعية الجمهور من الجريمة المعلوماتية وينبغي أن يكون المدعي العام المشرف على هذه التحقيقات مطلعاً على التشريعات السيبرانية وعلى دراية بالتقنيات المعلوماتية .

3

الاتفاقيات الدولية و العربية للتعاون في مجال الجرائم السيبرانية

تعد المعاهدات الدولية والاتفاقيات الإقليمية من أهم صور التعاون بصفة عامة ، وفي مجال مكافحة الجرائم الناتجة عن الهجمات السيبرانية بصفة خاصة ، ومن بين الاتفاقيات الدولية التي تعمل على دعم التعاون الدولي في مجال مكافحة الجرائم السيبرانية ، اتفاقية بودابست لمكافحة الجرائم السيبرانية ، ومن الاتفاقيات الإقليمية ، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

الاتفاقية
العربية
لمكافحة
جرائم تقنية
المعلومات

اتفاقية
بودابست
لمكافحة
الجرائم
السيبرانية

اتفاقية بودابست لمكافحة الجرائم السيبرانية

أبرم مجلس أوروبا اتفاقية مكافحة الجرائم السيبرانية في مدينة بودابست عام ٢٠٠١ إيماناً من دول المجلس بالتغيرات العميقة التي أحدثتها التطورات الرقمية والتقارب والعولمة المستمرة للشبكات المعلوماتية ، وتتكون الاتفاقية من ثماني وأربعون مادة تتعلق بتجريم بعض أشكال الجريمة السيبرانية ووضع قواعد التعاون الدولي بين الدول .

وتعد اتفاقية بودابست الأساس القانوني التقني والإجرائي الأول للتعاون الدولي بين دول العالم بصفة عامة لمواجهة الجرائم السيبرانية وتحقيق الأمن السيبراني .

ونظراً للطابع غير المستقر لأدلة الإثبات الإلكترونية والتي فرضت تحديات أمام التعاون الدولي ، منها صعوبة وصول أجهزة إنفاذ القانون إلى البيانات ، مثل نقاط الاتصال المتاحة على مدار الساعة فيما يتعلق بالتحريات عن الجرائم السيبرانية ، والوصول غير المحدود إلى البيانات الحاسوبية المخزنة ، والطلبات العاجلة للمساعدة المتبادلة .

وبالرغم من أن اتفاقية بودابست تعد من الصكوك الدولية التي تعتمد الكثير من الدول عليها في تعزيز التعاون الدولي إلا أننا بحاجة إلى اتفاقية دولية إضافية تبرز حماية البيانات وغيرها من الضمانات التي تحقق سيادة القانون ، و تعزيز آلية الكشف السريع عن البيانات في حالة الطوارئ ، وتطوير النظام الحالي للإفصاح الطوعي عن البيانات من قبل مقدمي الخدمة ، وتدعيم الفعالية المحدودة للأدلة الإلكترونية المتطيرة .

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

في سبيل تعزيز التعاون بين الدول العربية فيما بينها وتبني سياسة جنائية مشتركة لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ، تم إبرام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي تعد الأساس القانوني للتعاون بين الدول العربية في مجال مكافحة الجرائم السيبرانية .

وقد حثت الاتفاقية العربية على التعاون الدولي بين الدول الأعضاء سواء على المستوى القانوني أو على المستوى القضائي ونبين ذلك من عدة أوجه :

أولاً : من حيث الاختصاص :

ألزمت الاتفاقية الدول الأعضاء بمد اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني من الاتفاقية إذا ارتكبت في إقليم الدولة الطرف أو على متن سفينة أو متن طائرة مسجلة تحت قوانين الدولة الطرف أو إذا ارتكبت من أحد مواطني الدولة ، وإذا ادعت أكثر من دولة بالاختصاص القضائي فيقدم طلب الدولة التي أخلت الجريمة السيبرانية بأمنها.

ثانياً : من حيث تسليم المجرمين :

نصت الاتفاقية على عدة شروط لتسليم المجرمين المرتكبين للجرائم السيبرانية المنصوص عليها في الباب الثاني من أهمها أن تكون الجريمة السيبرانية معاقب عليها في الدولة الطرف بعقوبة لا تقل عن سنة أو بعقوبة أشد إلا إذا وجد اتفاق بين دولتين أو معاهدة أخرى تنظم المسألة فيطبق الاتفاق أو المعاهدة الأخرى .

حثت الاتفاقية الدول الأعضاء على المساعدة المتبادلة : فيما بينها بشأن التحقيقات أو الإجراءات المتعلقة بجرائم تقنية المعلومات

وجمع الأدلة

www.esu.ac.ae
الإلكترونية عن الجرائم .

ثالثاً : بالنسبة للمساعدة المتبادلة :

حثت الاتفاقية الدول الأعضاء على المساعدة المتبادلة : فيما بينها بشأن التحقيقات أو الإجراءات المتعلقة بجرائم تقنية المعلومات وجمع الأدلة الإلكترونية عن الجرائم .
وأن يتم تقديم طلب المساعدة من الدولة الطرف بواسطة الكتابة وفي حالة الاستعجال يتم تقديمه بواسطة البريد الإلكتروني المشفر أو الفاكس مع الحفاظ على عنصر السرية.

وفي مجال التشريعات الداخلية أولت بعض الدول العربية اهتماماً كبيراً بالأمن السيبراني ؛ جعل البعض مثل مصر ينص دستورياً بموجب نص صريح في دستور عام 2014 يشير إلى وجوب الحفاظ على المعلومات و البيانات الالكترونية ؛ إذ جرى نصها على أن أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد و الأمن القومي ، و تلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه ، على النحو الذي ينظمه القانون .
ومن الجدير بالذكر أن بعض الدول العربية قد حققت نجاحاً مدوياً في مجال الأمن السيبراني ؛ حيث حققت المملكة العربية السعودية المركز الثاني عالمياً وفقاً لمؤشر الأمن الرقمي GCI الصادر عن الاتحاد الدولي للاتصالات التابع للأمم المتحدة لمرتين متتاليتين في عامي 2021 ، و 2023.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY

nk You

