اعرف حقك وقانونك
KNOW YOUR LEGAL RIGHT

التصنيف القانوني لجرائم الابتزاز الإلكتروني

القاضي أنيس صالح جمعان

محامي عام أول في النيابة العامة اليمن عدن

إصدار منصة اعرف حقك وقانونك

النسخة الإلكترونية

المحتويات :

أولاً: المقدمة :

▪ إن جرائم الكمبيوتر والإنترنت أو مايسمى Cyber Crimes بشكل عام، وجرائم الإبتزاز الإلكتروني (Cyber-extortion) خاصة هي ظواهر إجرامية تقرع أجراس الخطر لتنبه مجتمعنا عن حجم المخاطر والخسائر التي يمكن أن تنجم عنها، وتعتبر جرائم الإبتزاز الإلكتروني أنها جرائم ذكية تنشأ وتحدث في بيئة إلكترونية أو بمعنى أدق رقمية، يقترفها أشخاص مرتفعي الذكاء ويمتلكون أدوات المعرفة التقنية، مما يسبب خسائر لأفراد المجتمع خاصة النساء، إذا كانت مجتمعاتنا العربية لم تتأثر بشكل كبير من مثل هذه الظواهر الإجرامية، كونها مستحدثة ودخيلة على قيمنا الإسلامي، إلا أن هناك دولاً عربية كثيرة أضحت مهتمة بتلك الظواهر، ومفهومها القانوني، وسمات المجرم المعلوماتي، والمتمثل بإنه هو شخص يختلف عن المجرم العادي فلا يمكن أن يكون هذا الشخص جاهلاً للتقنيات الحديثة المعلوماتية.

ثانياً: مفهوم جرائم الإبتزاز القانوني :

▪الإبتزاز في اللغة هو القيام بالتهديد من قبل شخص معين بمحاولة كشف المعلومات عن شخص معين أو أرتكاب بعض التهديدات التي بموجبها يمكن أن تدمر سمعة شخص آخر إن لم يقم ببعض الطلبات، وبالرجوع إلى معجم المعاني الجامع ستجد أن الإبتزاز هو الحصول على المال أو المنافع من شخص تحت التَّهديد بفضح بعض أسراره أو غير ذلك، أما قاموس المعاني يعتبر الإبتزاز هو الحصول على المال أو المنافع من شخص تحت التَّهديد بفضح بعض أسراره أو غير ذلك.

▪أما أصطلاحاً: الإبتزاز و الاستبزاز مفهومين لهما نفس المعنى تقريباً، وهو القيام بالتهديد بكشف معلومات معينة عن شخص، أو فعل شيء لتدمير الشخص الذي يتم تهديده، في حالة لم يستجب لمطالب ممارس الإبتزاز، حيث غالباً ما تكون المعلومات المستخدمة في عملية الإبتزاز ذات طبيعة محرجة للضحية، و يمكن أن تؤدي في بعض الأحيان إلى تدمير حياته الاجتماعية، هذا عن الإبتزاز عموماً، والإبتزاز الإلكتروني هو مصطلح يتكون من كلمتين، الأولى (الإبتزاز) ومعناه اللغوي الحصول على المال أوالمنافع من شخص تحت التهديد بفضح بعض أسراره أو غيرها، أما الكلمة الثانية (الإلكترونية) أي حصول فعل الإبتزاز بإستعمال وسائل ووسائط إلكتررنية وغيرها، ومع تطور التقنية ظهرت العديد من المشكلات التي تتعلق بها، حيث لم نجد في السنوات الماضية أي من تلك المشكلات إلا بتطور التكنولوجيا وأرتباطها بحياة الناس، حيث أصبحت حسابات التواصل الاجتماعي والبريد الإلكتروني والمواقع الإلكترونية معرضة بشكل ما للسرقات وعمليات الإبتزاز والحصول على معلومات في غاية الخصوصية وإمكانية حفظها والـتهديد بها، وقد سبق لإحدى الصحف الأمريكية نيويورك تايمز أن أشارت إلى أنه من بين كل ١٠٠ شخص يستخدم الإنترنت، يتعرض واحد منهم للإبتزاز الإلكتروني وبعدة طرق، سواء عبر تسجيل صوتي أو فيديو أو صور أو حتى رسائل مكتوبة، وفي مثل هذه الحالات، وخوفاً من الفضيحة في مجتمعاتنا العربية المحافظة، يتصرف الشباب بتلبية مطالب هؤلاء المبتزين دون اللجوء إلى طلب المساعدة من أهاليهم، أو الجهات الأمنية، الأمر الذي يحقق مطالب المبتزين أحياناً، بل يؤدي ببعض الذين وقعوا في هذا الفخ إلى التفكير في الانتحار أو إيذاء النفس أو التعرض للإضطرابات النفسية.

▪يعتبر الإبتزاز الإلكتروني أحد أكبر المخاطر التي تواجه مستخدمي شبكة الإنترنت والأجهزة الذكية ممن لا يمتلكون أي معرفة عن أمن المعلومات، فقد يؤدي الإبتزاز الإلكتروني إلى حدوث مشاكل تؤثر على الوضع النفسي للشخص الذي يتم إبتزازه وخاصة في مجتمعاتنا وبسبب عاداتنا وتقاليدنا، ومع التطور التكنولوجي السريع الذي وصلت إليه غالبية بلدان العالم العربي والغربي، أصبح بإمكان أي شخص وهو جالس في منزله الحصول على مايريد، فبكبسة زر واحدة يمكننا تصفح مئات المواقع الإخبارية وآلاف المتاجر الإلكترونية، وغيرها العديد من مواقع التواصل الإجتماعي التي بات يستخدمها الصغير قبل الكبير، ومن هنا بدأت مشاكل الإنترنت تزداد وذلك بسبب استغلال بعض العصابات الإلكترونية هذه الحسابات وأستبزاز أصحابها بهدف جمع الأموال، والأطفال هم الفئة الكبيرة المستهدفة لهذه العصابات.

▪غالباً تبدأ عملية الإبتزاز عن طريق إقامة علاقة صداقة مع الشخص المستهدف، ثم يتم الانتقال إلى مرحلة التواصل عن طريق برامج المحادثات المرئية (Video conferencing)، ليقوم بعد ذلك المبتز بإستدراج الضحية وتسجيل المحادثة التي تحتوي على محتوى مسيء وفاضح للضحية، ثم يقوم أخيراً بتهديده وإبتزازه بطلب تحويل مبالغ مالية أو تسريب معلومات سرية، وقد تصل درجة الإبتزاز في بعض الحالات إلى إسناد أوامر مخلة بالشرف والأعراف والتقاليد مستغلاً بذلك إستسلام الضحية وجهله بالأساليب المتبعة للتعامل مع مثل هذه الحالات. ▪أنه مع التطور الضخم في مجال التقنيات الإلكترونية تظهر في كل يوم وسيلة جديدة للتحايل على الضحايا وإبتزازهم، لكن غالباً تبدأ العملية عن طريق إقامة علاقة صداقة مع الشخص المستهدف، ثم يتم الانتقال إلى مرحلة التواصل عن طريق برامج المحادثات المرئية، ليقوم بعد ذلك المبتز باستدراج الضحية وتسجيل المحادثة التي تحتوي على محتوى مسيء وفاضح للضحية، ثم يقوم أخيراً بتهديده وإبتزازه بطلب تحويل مبالغ مالية أو تسريب معلومات سرية، وقد تصل درجة الإبتزاز في بعض الحالات إلى إسناد أوامر مخلة بالشرف والأعراف والتقاليد مستغلاً بذلك إستسلام الضحية وجهله بالأساليب المتبعة للتعامل مع مثل هذه الحالات، أو قد يقوم المبتز بتوجيه دعوة أو إرسال رابط معين إلى الضحية كدعوة صداقة وعند الضغط على هذا الرابط يقوم بتحميل برامج أو فيروسات من شأنها أن تضع ثغرات في النظام الإلكتروني للجهاز المستخدم عند الضحية يقوم من خلالها المبتز بالولوج إلى جهاز الضحية وتصويره أو نقل صور أو معلومات من جهازه ويقوم بتهديده بنشرها أو تسريبها أو التصرف فيها بأي صورة تؤدي بالضحية إلى تلبية مطالب المبتز.

ثالثاً: تعريفات الإبتزاز الإلكتروني :

-لقد تنوعت التعريفات مايُسمى بالإبتزاز الإلكتروني أازداد عدد ضحاياه من الذكور والإناث، لكنها تدور حول معنى واحد، ومما عُرف به الإبتزاز الإلكتروني Cyber-extortion الذي لا يختلف كثيراً عن عمليات الإبتزاز الأخرى، وهي:

(١) الإبتزاز الإلكتروني هي عملية تهديد وترهيب للضحية بنشر صور أو مواد فيلمية أو تسريب معلومات سرية تخص الضحية، مقابل دفع مبالغ مالية أو أستغلال الضحية للقيام بأعمال غير مشروعة لصالح المبتزين كالإفصاح بمعلومات سرية خاصة بجهة العمل أو غيرها من الأعمال غير القانونية، وعادة مايتم تصيد الضحايا عن طريق البريد الإلكتروني أو وسائل التواصل الإجتماعي المختلفة (الفيس بوك، تويتر، الواتس أب، وإنستغرام، الأيمو) وغيرها من وسائل التواصل الإجتماعي نظراً لإنتشارها الواسع وإستخدامها الكبير من قبل جميع فئات المجتمع، وتتزايد عمليات الإبتزاز الإلكتروني في ظل تنامي عدد مستخدمي وسائل التواصل الإجتماعي والتسارع المشهود في أعداد برامج المحادثات المختلفة.

(٢) الإبتزاز الإلكتروني هو القيام بالتهديد بكشف معلومات معينة عن شخص، أو فعل شيئ لتدمير الشخص المهدد، إن لم يقم الشخص المهدد بالإستجابة إلى بعض الطلبات، هذه المعلومات تكون عادة محرجة أو ذات طبيعة مدمرة إجتماعياً، وهو بمعنى آخر كثرة المطالب غير المشروعة قانوناً للوصول إلى الهدف الذي رسم له، وغالباً ما يكون هذا الهدف مدمر للحياة الاجتماعية، وهو محاولة الحصول على مكاسب مادية أو معنوية عن طريق الإكراه من شخص أو أشخاص أو حتى مؤسسات ويكون ذالك الإكراه بالتهديد بفضح سر من أسرار المبتز.

رابعاً: وسائل الإبتزاز الإلكتروني :

▪يتم تصيّد ضحايا الإبتزاز الإلكتروني عن طريق الإنترنت بعدة وسائل التواصل الإجتماعي (سوشال ميديا) المنتشرة حالياً يستخدمها الملايين مثل:

(١) الفيس بوك (facebook)

(٢) الواتس أب (whatsapp)

(٣) سكايب (Skype)

(٤) البريد الإلكتروني (E-mail)

(٥) تويتر (Twitter)

(٦) الإنستجرام - انستقرام (Instagram)

(٧) تيلجرام (Telegram)

(٨) اليوتيوب (YouTube)

(٩) السناب شات (Snapchat)

(١٠) الأيمو (imo)

(١١) تيك توك (TikTok)

(١٢) وي شات (WeChat)

(١٣) تمبلر (Tumblr)

(١٤) الفايبر (Fiber)

(١٥) لاين (Line)

(١٦) كيو كيو (QQ)

(١٧) سينا ويبو (Sina Weibo)

▪أو أي وسيلة إلكترونية أخرى جديدة غير معروفة لدى البعض يمكن من خلالها الوصول إلى معلومات سرية أو حساسة عن الضحية.

خامساً: مراحل الإبتزاز الإلكتروني :

(١) تبدأ بعلاقة صداقة مع الشخص المستهدف، ثم تنتقل لمرحلة التواصل عبر برامج المحادثات المرئية.

(٢) المبتز يستدرج الضحية ويسجل أي محتوى مسيء وفاضح، بالنص أو الصوت أو الصورة أو الفيديو.

(٣) المبتز يهدد ضحيته مقابل مبالغ مالية أو تسريب معلومات سرية، وقد تصل درجة الإبتزاز إلى مطالب مخلة بالشرف.

سادساً: طرق إختراق حسابات المبتَز :

(١) محاولة سرقة الحسابات الخاصة بالمبتَز سواء من خلال إرسال بعض الروابط الإحتيالية على البريد الإلكتروني الخاص به أو موقع التواصل الإجتماعي من خلال الرسائل.

(٢) إرسال بعض المواقع المجهولة التي تثير فضول المبتَز من أجل سرقة البيانات الخاصة بك من خلالها.

(٣) محاولة الوصول إلى الصور والفيديوهات الشخصية من خلال المراسلة أو سرقتها من خلال حساباتك على مواقع التواصل الاجتماعي.

(٤) طلب التحدث إليك عبر الواتس أب أو ماسنجر الفيس بوك أو الأيمو أو سكايب أو غيره من وسائل التواصل الإجتماعي من أجل محاولة إجترارك للإبتزاز من خلال عرض فيديو يخيل للمستخدم أنه مباشر بل هو فيديو مسجل مسبقاً، وهذا الأجترار من خلال فتح الكاميرا الخاصة بالمبتَز وبالتالي محاولة التقاط الفيديوهات والصور له المخلة الفاضحة المخلة بالحياء دون علم منه.

سابعاً: طرق التعامل مع الابتزاز الإلكتروني :

(١) قطع التواصل مع الشخص المبتز مهما كانت الضغوطات شديدة، ولا تحاول شتم المبتز أو تهديده كي لا تصبح غايته إنتقامية.

(٢) عدم الأنصياع للمبتز ولا تقوم بتحويل أي أموال له، أو الإفصاح عن رقم بطاقة البنك، لأن المبتز بالنهاية هو لص ومجرم وسيستمر بطلب الأموال إذا شعر بضعفك من المرة الأولى.

(٣) تجنب المشادات مع المبتز وعدم تهديده بالشرطة، و الإبلاغ الفوري للجهات المختصة الشرطة أو لوحدة الجرائم الإلكترونية التابعة لبلدك إن وجدت، التي ستقوم بفتح تحقيق بذلك.

(٤) الإبلاغ الفوري للجهات المختصة لإدارات وسائل التواصل (الفيس بوك او اليوتيوب أو تويتر) وغيره من وسائل التواصل الإجتماعي المرئية لحدفه في حال تم تسجيل فيديو فاضح لك، أو لاحد أفراد عائلتك أو تم دبلجته وتهديدك به.

(٥) إغلاق جميع حسابات التواصل الإجتماعي و البريد الإلكتروني وجميع وسائل الاتصال على الإنترنت، كما يجب إغلاق الهاتف نهائياً حتى لا يستطيع الشخص المبتز الوصول إليك.

(٦) عدم تتبع الشخص المبتز إلا في حالة لديكم الخبرة الكافية بالأدوات التكنولوجية أو محترفاً في أمور التتبع الإلكتروني.

(٧) إبلاغ الأشخاص القريبين منك (الأبوين والأخوة والأصدقاء) بما حدث لك من المبتز، وفي حالة تعرض الفتيات للإبتزاز فمن الأفضل إخبار الأهل بذلك سريعاً وذلك للتصرف مع المبتَز.

(٨) عدم اللجوء وطلب المساعدة من أشخاص آخرين ليقوموا بإختراق حساب المبتز وذلك للأسباب التالية:-

(أ) المبتز في الغالب يكون تابعاً لعصابة كبيرة ولديهم معرفة كافية ووافية بأساليب الاختراق.

(ب) المبتز لديه حسابات وهمية أخرى، وبالتالي إختراق أي من هذه الحسابات لن يؤثر عليه وسيعمل على إنشاء حسابات وهمية جديدة لإبتزازك من جديد.

(ج) تعريض الأشخاص الذي قاموا بمساعدتك في إختراق حسابات الشخص المبتز في مشاكل وبالتالي تعرضهم للخطر.

ثامناً: طرق تجنب الوقوع في فخ الإبتزاز الإلكتروني :

(١) تجنب قبول طلب الصداقة من قبل أشخاص غير معروفين.

(٢) تجنب نشر أي صور شخصية أو معلومات شخصية على مواقع التواصل الإجتماعي المختلفة، وذلك حتى لا تتعرض للإبتزاز من قبل مرتكبي الجرائم الإلكترونية.

(٢) عدم الرد والتجاوب على أي محادثة، أو فتح روابط ترد إليك من مصادر غير معروفة.

(٣) تجنب مشاركة معلوماتك الشخصية حتى مع أصدقائك في فضاء الإنترنت (أصدقاء المراسلات).

(٤) رفض طلبات إقامة محادثات الفيديو مع أي شخص، ما لم تكن تربطك به صلة وثيقة.

(٥) عدم الأنجذاب للصور الجميلة والمغرية، وتأكد من شخصية المرسل.

(٦) تجنب تخزين الصور الخاصة بالأفراد على مواقع التواصل الإجتماعي وأجهزة الحاسوب، وتجنّب تحميل أي برنامج مجهول المصدر، مع إستمرارية تحديث برامج الحماية الخاصة بأجهزة الحاسوب ومنها، MCafee, Norton.

(٧) تجنب إستخدام أي برامج مجهولة المصدر، كما يجب تجنب إدخال أي أكواد أو كلمات مرور مجهولة تجنباً للتعرض للقرصنة وسرقة الحسابات المستخدمة.

(٨) تجنب فتح أي رسائل إلكترونية مجهولة، وذلك حتى لا يتم إختراق نظام الحاسوب لديك وسرقة كل ما عليه من معلومات شخصية وحسابات وكلمات المرورو الخاصة بك.

تاسعاً: طرق الحماية من جرائم الإبتزاز الإلكتروني :

(١) التوعية بشكل كبير حول الخصوصية، أي عدم نشر المعلومات الخاصة لهم ولعائلاتهم وأصدقائهم على وسائل التواصل الإجتماعي المختلفة.

(٢) عدم كشف كلمات المرور لأي حساب سواء (كلمة السر) نهائياً، كان حساب مصرفي أو بطاقة إئتمان أو حساب على موقع معين بالإنترنت، كما يجب أيضاً تغييرها بإستمرار

وأختيار كلمات سر صعبة لضمان عدم وقوعها الأيدي الخاطئة، عدم الكشف عنها وتغييرها بشكل مستمر.

(٣) عدم مشاركة الناس حتى المقربين بأسرارهم وصورهم وفيديوهاتهم إن لم تكن مقبولة ضمن المعايير العامة.

(٤) التفكير ملياً قبل إضافة أو قبول طلبات الصداقة، ورفض طلبات الصداقة من الأشخاص غير المعروفين أو غير المقربين.

(٥) التحذير وعدم التفاعل أو الدخول على الروابط والإعلانات التي تتواجد بكثرة على المواقع الإلكترونية، أو المرسلة عبر وسائل التواصل الإجتماعي، فالكثير منها يكون بمثابة مصيدة للإبتزاز الإلكتروني.

(٦) المراقبة والمتابعة والتفتيش لجميع المواقع التي يتصفحها أفراد العائلة والملفات التي يحفظوها على أجهزتهم.

(٧) عدم تصفح المواقع مجهولة المصدر أو غير المشهورة التي يمكن أن تكون مرتبطة ببعض البرامج التي تفتح الكاميرا الخاصة بك من أجل التقاط الصور، أو تكون مرتبطة ببعض الروابط المجهولة التي تسرق البيانات.

(٨) عدم تصفح المواقع الجنسية خاصة على الجهاز الخاص بك، لأن كثيراً من هذه المواقع تسرق بيانات ومعلومات المستخدمين وتجعلهم عرضة للإبتزاز الإلكتروني.

(٩) تثبيت برامج حماية من الفيروسات والإختراقات من أجل الحفاظ على سلامة الجهاز المستخدم وسرية ما به من معلومات، والمواظبة على التحديث الدوري للبرنامج، والحرص على إقتناء النسخ الأصلية من هذه البرامج والمتوفرة في المحلات المختصصة بالبيع لها.

عاشراً: المعالجة التشريعية لجرائم الإبتزاز الإلكتروني في اليمن :

▪بالنسبة للجرائم الإلكترونية ومن ضمنها جرائم الإبتزاز الإلكتروني في اليمن حتى الآن لم يصدر أي قانون ينظمها، وذلك أولاً بسبب إنها لم ترقَ إلى مرحلة الجريمة الإلكترونية المنظمة سابقاً، لازالت في مهدها، وهي جرائم مستحدثة، وثانياً ويرجع ذلك إلى الفراغ التشريعي في اليمن الناتج بسبب الحرب منذ سنوات، وتوقف المجلس التشريعي (مجلس

النواب اليمني) من أنعقاد جلساته، لإقرار قانون تقنية المعلومات وغيره من القوانين، لذلك يتم معاقبة المتهمين في هذه الجرائم عن طريق القياس بالجرائم المماثلة في القانون رقم ١٢ لسنة ١٩٩٤م بشأن الجرائم والعقوبات اليمني الذي تحتوي نصوصه مواد تجرِّم الابتزاز منها المواد (٢٥٦، ٢٥٧)، التي تجرِّما الاعتداء على حرمة الحياة الخاصة، والتهديد بإذاعة الأسرار الخاصة، وجريمة الإبتزاز (٣١٣) الذي حددوا عقوبة جراء تلك الأفعال في التالي:

مادة (٢٥٦): يعاقب بالحبس مدة لا تزيد على سنه أو بالغرامة كل من اعتدى على حرمة الحياة الخاصة وذلك بأن أرتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانونا أو بغير رضاء المجني عليه:

أ- استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أياً كان نوعه محادثات جرت في مكان خاص أو عن طريق الهاتف.

ب- ألتقط أو نقل بجهاز من الأجهزة أياً كان نوعه صورة شخص في مكان خاص.

فإذا صدرت الأفعال المشار إليها في الفقرتين السابقتين أثناء اجتماع على مسمع أو مرأى من الحاضرين في ذلك الاجتماع فإن رضاء هؤلاء يكون مفترضاً.

ويعاقب بالحبس مدة لا تزيد على ثلاث سنوات أو بالغرامة الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتماد على سلطة وظيفته.

ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة كما يحكم بمحو التسجيلات المتحصلة عنها أو إعدامها.

مادة (٢٥٧): يعاقب بالحبس مدة لا تزيد على سنتين أو بالغرامة كل من أذاع أو سهل إذاعة أو أستعمل ولو في غير علانية تسجيلاً أو مستنداً متحصلاً عليه بإحدى الطرق المبينة بالمادة السابقة أو كان ذلك بغير رضاء صاحب الشأن ويعاقب بالحبس مدة لا تزيد على ثلاث سنوات كل من هدد بإفشاء أمر من الأمور التي تم الحصول عليها بإحدى الطرق المشار إليها لحمل شخص على القيام بعمل أو الامتناع عنه ويعاقب بالحبس مدة لا تزيد على خمس سنوات الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتمادا على سلطة وظيفته.

ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة أو تحصل منها كما يحكم بمحو التسجيلات المتحصلة عن الجريمة أو إعدامها.

مادة (٣١٣): يعاقب بالحبس مدة لا تتجاوز خمس سنوات أو بالغرامة كل من يبعث قصداً في نفس شخص الخوف من الإضرار به أو بأي شخص آخر يهمه أمره ويحمله بذلك وبسوء قصد على أن يسلمه أو يسلم أي شخص آخر أي مال أو سند قانوني أو أي شئ يوقع عليه بإمضاء أو ختم يمكن تحويله إلى سند قانوني.

أحدى عشر: التوصيات :

(١) الإسراع في إصدار قانون تقنية المعلومات وذلك لمكافحة الجرائم الإلكترونية، الذي سيوفر الحماية القانونية للإستخدام المشروع للإنترنت وشبكة المعلومات فيها، ومعاقبة مرتكبي الأفعال التي تشكل إعتداء على حقوق مستخدميها من الأشخاص الطبيعية أو المعنوية ومنها جرائم الإبتزاز الإلكتروني.

(٢) الإسراع في إنشاء النيابات والمحاكم المتخصصة في مجال مكافحة الجرائم الإلكترونية والحد منها.

(٣) ضرورة إعداد الكوادر القضائية والأمنية في مجال التحقيق وجمع الأدلة الإلكترونية، وتأهيلهم في مجال مكافحة الجرائم الإلكترونية،

(٤) عقد دورات مكثفة للكوادر البشرية العاملين في حقل التحري والتحقيق، والنظر في تضمين مناهج التحقيق الجنائي في كليات و معاهد تدريب الشرطة موضوعات عن جرائم الإنترنت (تقنية المعلومات) ومنها جرائم الإبتزاز الإلكتروني.

(٥) إنشاء مركز وطني للتقنية والمعلومات لمكافحة الجرائم الإلكترونية، وتزويده بالوسائل الفنية الحديثة، وذلك لمواكبة التطورات المرتبطة بالجريمة الإلكترونية والحرص على تطوير وسائل مكافحتها، ويضم معلومات مكتملة عن أي واقعة ومعلومات عن المدانين والمشتبه بهم، من خلال تطوير طرق ووسائل تتبع مرتكبي الجرائم الإلكترونية بشكل دقيق والإمساك بهم.

(٦) ضرورة نشر الوعي الرقمي بين المستخدمين وكيفية تفادي التعدي على بياناتهم الشخصية في وسائل التواصل الإجتماعي، وتعريفهم بحجم الخطورة التي ترصدهم في حالة عدم أتخاذ الإحتياطات الوقائية اللازمة.

(٧) حث الجامعات القانونية اليمنية للبحث والدراسة في الجرائم المعلوماتية والجرائم عبر الإنترنت (الإلكترونية)، و إدخال مساق الجرائم الإلكترونية كأحد المواد الدراسية فيها.

(٨) دراسة الإتفاقيات الدولية المتعددة المتعلقة في مكافحة الجرائم الإلكترونية، ودراسة إمكانية الإنضمام إليها للإستفادة مما تتيحه هذه الإتفاقيات من تسهيلات في مكافحة هذا النوع من الجرائم على المستوى الداخلي والخارجي.

(٩) تفعيل دور الأسرة ورجال الدين وأجهزة الإعلام والأجهزة التربوية ومراكز الشباب في التوعية القانونية، والتعريف بمدى خطورة الجرائم الإلكترونية بشكل عام، وجرائم الإبتزاز الإلكتروني بشكل خاص، ويتمثل بتوعية الأفراد ونصحهم، فالإعلام له دور هام في التوعية عن مدى خطورة الجرائم الإلكترونية، وكيفية التعامل معها والحماية منها.

(١٠) تشجيع الباحثين اليمنيين بالدعم المعنوي والمادي، لإجراء المزيد من البحوث والدراسات حول الجرائم الإلكترونية المستحدثة ومنها جرائم الإبتزاز الإلكتروني.

(١١) تشجيع الجامعات والمراكز البحثية والإعلامية على تنظيم العديد من الندوات والمؤتمرات التي تعالج تطور الإجرام المعلوماتي، ومنها جرائم الإبتزاز الإلكتروني، وكيفية مكافحتها، والحد من أثارها، ونشرها على نطاق واسع من خلال الصحافة والإعلام المرئي والمسموع، وفي مختلف مواقع التواصل الإجتماعي.

القاضي أنيس صالح جمعان

محامي عام أول في النيابة العامة عدن - كاتب و باحث قانوني

▪تم النشر في مدونة القاضي أنيس جمعان في facebook بتاريخ ١٤ يناير ٢٠٢٠م https://m.facebook.com/story.php?story_fbid=1030279497327838&id=100066819915781&mibextid=Nif5oz

▪نشر في موقع عدن الخبر بتاريخ ١٢ ديسمبر ٢٠٢٣م على الرابط: https://adenkhbr.net/217985