ورقة عمل

تجربة جمهورية السودان في التحقيق الإلكتروني

إعداد / إسلام تاج السر أحمد

وكيل النيابة

أولاً : مقدمة :

تُعَد التكنولوجيا من أهم أدوات التطور والتنمية ولا شـــك في حاجة الدول لها لتحقيق أهدافها ، لذلك كان من الطبيعي تطورها بإســتمرار لتواكب مســيرة نمو الدول وتطور الحياة بشكل عام .

وبما أن التكنلوجيا شـأنها شـان الكثير من الأشـياء التي تدور آثارها سـلباً أو ايجابياً مع طريقة اســتخدامها ، وفي خضـــم ذلك التطور ظهرت ما تعرف بالجرائم الإلكترونية أو السيبرانية .

ثانياً : الإطار التشريعي :

لعل الســـودان من الدول الســـبَاقة في ســـن القوانين المعنية بالمعاملات والجرائم الإلكترونية حيث تمت إجازة قانوني المعاملات الإلكترونية وجرائم المعلوماتية في العام 2007 ودخلا حيز النفاذ والتطبيق في نفس العام .

ظلت أجهزة إنفاذ القانون طيلة إحدي عشـــر عاماً ومن خلال التطبيق العملي تحدد أوجه القصور وتضع المقترحات والدراسات التي من شأنها أن تجعل التشريعات أكثر مواكبة وتساعد فى مكافحة الجرائم الإلكترونية وكانت ثمرة تلك المجهودات هي قانون مكافحة جرائم المعلوماتية لســـ2018ـنة .

ثالثا : التقنيات المستخدمة في التحقيق الإلكتروني :

مصـــطلح الجريمة الإلكترونية يشـــمل كل المظاهر التقليدية للجريمه مثل الإحتيال ونشـــر مواد ذات محتوى مخل بالآداب العامة وإنتهاك الخصـــوصـــية وخلافه ، إلا أن هذا النوع من الجرائم يختلف عن الجرائم (التقليدية) في أدوات الجريمة وسبل إرتكابها ونطاقها مما يستوجب معه إعتماد تقنيات خاصة للتحري والتحقيق .

وفي هذا الصـدد وبما أن الجرائم الإلكترونيه تتعلق بشـكل كبير بالإجراءات ، لذا لابد من فهمها جيداً وتجنب إجراءها بشـــكل روتيني ، عليه فإن النيابة العامه بالإســـتعانه بجهات التحري الفني (الأدلة الجنائية ، المركز الســـوداني لأمن المعلومات) تعي أهمية الدقة في التحقيق الإلكتروني وتتبع في ذلك ما يلى .

1- معرفة أين يمكن إيجاد الادلة (الحواسيب – البريد الإلكتروني – الصـور الرقمية – الهواتف - ماكينات التصوير ....)
2- معرفة طريقة إخفاء البيانات (مســح البيانات – إســتخدام حاجب لإخفاء العنوان الفيزيائي للجهاز المستخدم – إخفاء بيانات صاحب حساب معين ..) مع توفر الأجهزة التى تســـاعد على معالجة البيانات وإســـتعادة الممحية منها بالإضافة إلي استخدام الأنظمة المناسبة لقهر طرق التخفي .
3- الجـاهزيـة للتعـامـل مع كم هـائـل من المعلومـات وتحليلهـا والتركيز علي المهمة منها .
4- تحديد الأشـياء التي يمكن تعقبها (كمبيوتر الضـحية – دخول الحسـاب – الشخص ساحب المال – كاميرات المراقبة في مكان سحب المال ...) .

رابعاً : الإيجابيات :

1/ وجود قانون جيد ومواكب إلى حد كبير .
2/ إصدار أوامر تأسيس لنيابات متخصصة بالتحقيق الإلكتروني بولايات السودان المختلفة لتسهيل الإجراءات .
3/ وجود كوادر بشـــرية تمتلك التأهيل والخبرة اللازمة لإجراء التحقيق الإلكتروني .

خامساً :التحديات :

1/ تطوير البني التحتيه في مجال الإتصـــالات ، وضـبط تسـجيل شـرائح الإتصالات وبيعها وتداولها .
2/ تعذر حل بعض الجرائم بسـبب ضـعف التعاون بين الدول والشـركات فيسبوك علي سبيل المثال) وما بين الدول مع بعضها .
3/ ضعف التنوير والتحذير فيما يلي الجرائم الإلكترونية .
4/ عدم توفر بعض التقنيات والأنظمه التي تســـاعد علي حفظ الأدلة والتعامل معها (حقائب معنية – The original hashing value – hashing) .
5/ تطور وسئل الجريمة بشكل أسرع من تطور وسائل المكافحة .
6/ وجود بعض الحواجز المجتمعية التي تحول دون إدلاء الضـــحايا بالبيانات التي تساعد في التحقيق لا سيمَا في الجرائم الأخلاقيه .
7/ الجرائم الإلكترونية هي جرائم عابرة للحدود .
8/ ســـهولة إرتكاب الجرائم الإلكترونيه بعيداً عن الرقابه الأمنية ، وإتســـاع نطاق الجريمة وتنامي حجم الضرر منها .
9/ إمكانية إتلاف الأدلة من قبل الجناة .

سادساً : خاتمة :

للحد من إنتشــار الجرائم الإلكترونيه و بالإضــافة إلى الإهتمام بتقنيات التحقيق يجب الإنتباه إلى ما يلى :

1/ تطوير التشريعات وتجويدها حيث أنه في حالة وجود قانون به خلل فإن كل ما يلي ذلك من إجراءات يكون غير صحيح .

2/ لابد من التعاون بين الدول لأن مرتكبي الجرائم أحياناً يكونوا خارج نطاق الإختصاص المعين .

3/ المنظمات الإجرامية تمتلك إمكانيات كبيرة وموارد مالية هائلة ويمكنهم معرفة نقاط الضــعف وإســتغلالها ، عليه لابد من تكريس الإمكانيات والموارد كذلك لمكافحة الجريمة .

4/ تطبيق معايير حماية جيدة ومتطورة .

إسلام تاج السر أحمد الحسن

وكيل النيابة

الخرطوم – السودان