القانون السوداني الخاص بجرائم المعلوماتية لعام 2007

الدكتورة جنان الخوري
رئيسة القسم الحقوقي في مركز المعلوماتية القانونية في الجامعة اللبنانية

janane-khoury@hotmail.com

مضمون المحاضرة:

- قانون جرائم المعلوماتية للعام 2007 الساري المفعول؛
- أنواع الجرائم التي ينص عليها، مع التعليق عليها، ومقارنتها بالعديد من القوانين الدولية؛
- تطبيق القانون
- واقع المحاولة والمساهمة في هذه الجرائم
- العديد من المقترحات لمكافحة جرائم المعلوماتية في السودان من قبل قضاة الملاحقة، التحقيق وقضاء الحكم...؛
- خاتمة وتوصيات.

مقدمة عامة:

- على الصعيد القانوني، تركت الثورة الإلكترونية بصماتها على الجانب القانوني على الصعيدين المحلي والدولي، وما يتحصّن به هذا الجانب من مبادئ دستورية وقانونية. فإذا كانت الصلاحيات الجزائية الإقليمية، والشخصية، والذاتية (واحتياطاً) العالمية، تتولّى توزيع الاختصاص القضائي لتعقّب المجرمين ومحاكمتهم، فقد توزّعت الجرائم المعلوماتية الإعداد، والتخطيط، والتنفيذ، والاختباء أو الإخفاء في بلد معين أو حتّى في قارة معيّنة، وتبعثر الدليل. ميزةُ هذه الجرائم أنها تقع ولا تُكتَشف، إذا اكتُشِفت فلا يُعرف فاعلها وإذا عُرف تعجز الأدلة عن إدانته؛ مما يُثير في الواقع صعوبات عدّة، تتمثّل الأولى في طريقة الإثبات، ولا سيما إثبات الركن المادي وما يُشكّله هذا الاثبات من أهمية جوهرية لتكوين اقتناع القاضي وفي تحديد الولاية القضائية لأي دولة وحسم مسألة التنازع الايجابي أو السلبي بين الدول. وهذا ما أبرز ظاهرة إجرامية حديثة، أثارت بعض الإشكاليات الموضوعية والإجرائية للجانب القانوني الداخلي والدولي، وما يتحصّن به هذا الجانب من مبادئ دستورية وقانونية.

الإشكالية القانونية المثارة...

1. إشكالية قانونية موضوعية: الركن الإلكتروني

- تستهدف هذه الجرائم معنويات وليس ماديات محسوسة، فالجديد في هذه الجرائم، إضافة عنصر حديث يبرز محل الإعتداء في هذه الظاهرة الإجرامية متمثلاً بمُعطيات الحاسوب على العنصر القانوني والمادي، وهي الكيانات المعنوية ذات القيمة المالية أو القيمة المعنوية البحتة، ولولا هذه الطبيعة المستجدة في الأساس لما كنا أمام ظاهرة مستجدّة برمتها.

2. إشكالية قانونية إجرائية: الدليل الرقمي الجنائي...

لناحية نطاق التفتيش، الضبط، التقصّي الإلكتروني وحجية الدليل الرقمي، ...

- نعالج هذه الإشكاليات القانونية في ضوء القانون السوداني الراهن، محاولين تبيان بعض الثغرات القانونية وبعض المقترحات المرجو اتخاذها.

القانون السوداني: ثماني فصول

- أهم الجرائم التي ينص عليها وهي على التوالي:

- جرائم نظم ووسائط وشبكات المعلومات،
- الجرائم الواقعة على الأموال والبيانات والإتصالات،
- جرائم النظام العام والآداب،
- جرائم الإرهاب والملكية الفكرية،
- جرائم الإتجار بالجنس البشري وبالمخدرات وغسل الأموال.

دخول نظم ووسائط المعلومات المملوكة للغير (م. 4):

- **"كل من يدخل موقعاً أو نظام معلومات دون أن يكون مصرحاً له ويقوم:**
- **بالاطلاع عليه أو نسخه يُعاقب بالسجن مدة لا تتجاوز سنتين أو بالغرامة أو بالعقوبتين معاً،**
- **بإلغاء بيانات او معلومات ملكاً للغير أو حذفها أو تدميرها أو إفشائها أو اتلافها أو تغييرها أو إعادة نشرها أو تغيير تصاميم الموقع أو إلغائه أو شغل عنوانه، يُعاقب بالسجن مدة لا تتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معاً".**

- عدم الحصول على تصريح بالدخول: السؤال الأساسي هنا: ماذا لو كان مصرّحاً له بالدخول ودخل إلى الموقع وهناك استغلّ حق الدخول وأساء استعماله من خلال الحصول على معلومات خاصة لمصلحته أو لمصلحة غيره؟ لذلك **يقترح تعديل هذه المادة لناحية إضافة هذا الركن لسدّ ثغرة عدم تجريم هذه الحالة.**

- لم تذكُر المادة الرابعة حالة ما اذا كان المتهم قد توصّل بالفعل إلى الإلغاء أو الحذف أو التدمير أو الإفشاء أو الإتلاف. ووفقاً للنظام السعودي المادة 3 يتوافر التجريم وتترتّب المسؤولية الجزائية على عاتق المتهم حتى ولو لم يتمكّن من العبث بالموقع ما دامت نيته من وراء الدخول غير المشروع هي الوصول إلى تحقيق تلك الغاية.

- لا ضرورة هنا لأن يسبّب هذا الدخول أي ضرر للغير لتجريمه، إنما **يُقترح إضافة شرط تسبّب الضرر للمجني عليه لتُشدّد العقوبة.**

دخول المواقع وأنظمة المعلومات من موظف عام (م. 5):

- **"كل موظف عام، يدخل بدون تفويض موقع او نظام معلومات خاص بالجهة التي يعمل بها أو يسهل ذلك للغير، يعاقب بالسجن مدة لا تتجاوز خمس سنوات أو بالغرامة أو بالعقوبتين معاً".**

- ماذا لو دخل الموظف بموجب تفويض إنما أساء حق الدخول؟ (ملاحظة تم تفسيرها أعلاه).
- ماذا لو دخل الموظف العام إلى موقع أو نظام خاص وظيفة أخرى لا يعمل بها؟
- **فيُقترح أنْ تتوسّع المادة لتشمل تجريم الموظف وتشديد عقوبته لدى دخوله إلى أي موقع إلكتروني رسمي سواءً أكان خاصاً بوظيفته أو بوظيفة أخرى.** فالموقع الخاص بالوظيفة العامة عادةً ما يحتوي على معلومات حساسة وأسرار أمنية وطنية وإدارية disseminating secret or sensitive data وأن افشاءها يُسبب خطورة معينة، فهل يكفي معاقبة مرتكبها بغرامة فقط؟

الجرائم الواقعة على الأموال والبيانات والاتصالات (الفصل الثالث):

- الملاحظة الأُولى هي حول مزج جرائم ضد الأموال مع جرائم البيانات والاتصالات communication. فجرائم التعدّي على الأموال متعدّدة (السرقة، الإختلاس، الإحتيال، التزوير، الغش، النصب، الإبتزاز) وتستحق فصلاً مستقلاً.

- **المادة العاشرة: التهديد أو الابتزاز**
- **"كل من يستعمل شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها في تهديد أو ابتزاز شخص آخر لحمله علي القيام بفعل أو الامتناع عنه ولو كان هذا الفعل أو الامتناع مشروعاً ، يعاقب بالسجن مدة لا تتجاوز سنتين أو بالغرامة أو بالعقوبتين معاً ".**

- لا يجوز أن تتساوى العقوبة في حال كان التهديد أو الإبتزاز للقيام بفعل مشروع أو غير مشروع، (فلا يُفترض أنْ تكون عقوبة تهديد موظف بنشر صورة فاضحة له عبر شبكة الإنترنت للقيام بعمله كعقوبة إجباره على إفشاء أسرار وظيفته). **فيُقترح تشديد العقوبة**

الإحتيال أو انتحال صفة غير صحيحة (م. 11):

- **"كل من يتوصل عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب وما في حكمها عن طريق الاحتيال أو استخدام اسم كاذب أو انتحال صفة غير صحيحة ، بغرض الاستيلاء لنفسه أو لغيره على مال أو سند أو توقيع للسند، يعاقب بالسجن مدة لا تتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معاً.**

- هنا يجدر التنويه إلى عبارة "توقيع للسند"، فيُقترح أنْ تشمل توقيع السند إيجابياً (تعهد دفع مبلغ على سبيل المثال)، أو سلبياً (على سبيل المثال توقيع براءة ذمة).

- يقترح شمول سائر أوجه الاحتيال الالكتروني عموماً والتمييز بين مُمتهن وغير ممتهن لناحية العقوبة ولناحية وقوع الضحية في فخ المجرمين، وتجريم من يُسهّل استيلاء الغير على تلك الأموال، كتزويد الغير ببرامج تسهّل أو تسمَح بالاحتيال الالكتروني...

المادة الثانية عشرة: الحصول على أرقام أو بيانات بطاقات الإئتمان:

- **"كل من يستخدم شبكة المعلومات أو أحد أجهزة الحاسوب وما في حكمها للوصول إلى أرقام أو بيانات للبطاقات الائتمانية أو ما في حكمها بقصد استخدامها في الحصول على بيانات الغير أو أمواله أو ما تتيحه تلك البيانات أو الأرقام من خدمات ، يُعاقب بالسجن مدة لا تتجاوز خمس سنوات أو بالغرامة أو بالعقوبتين معاً."**

- تستحقّ أن تكون تحت عنوان فصل مستقل يشمل "البطاقات المصرفية والنقود الإلكتروني".

- **ماذا عن سرقة هذه البطاقات الإئتمانية credit card theft مادياً من دون إمكان استعمالها (عدول خارجي، استحالة مادية)؟**
- **ماذا عن تقليد بطاقة مصرفية الكترونياً؟ أو تزوير بطاقة مصرفية الكترونياً؟ او إستعمالها use of forged credit cardفي ما بعد (وهنا الضرر الفعلي والجسيم ربما)؟ أو عدم إمكانية استعمالها؟**
- **ما هو وضع من يقبل الإيفاء ببطاقة مصرفية مُقلّدة أو مُزوّرة أو مسروقة accepting payment through a counterfeit credit card؟ أليس شريكاً في هذه الجريمة؟**
- **بالنسبة إلى "البطاقات الإئتمانية"، الأفضل النص على "البطاقات المصرفية"عموماً أو بيانات البنوك على غرار ما ينص عليه القانون الإماراتي، لا سيما في العصر الحالي حيث تتعدّد أنواع هذه البطاقات وأشكالها (الشيك الالكتروني electronic cheque، الصراف الآلي ATM، بطاقات الدفع أو بطاقات السحب Debit or credit card، "بطاقة شامخ الذكية المستخدمة في السودان)، وإن لم تكن منتشرة بشكلٍ واسع في السودان، فبالطبع سيكثر استعمالها في المستقبل نظراً إلى الاتجاه الدولي والإقليمي والمحلي إلى المعاملات المصرفية الإلكترونية.**
- **يُقترح إضافة "تزوير النقود الإلكترونية"** Cyber money forgery وجريمة "تزوير النقود الكترونياً.
- **يُقترح تجريم التجسس على بيانات البنوك**

الإخلال بالنظام العام والآداب (م. 14)

- **كل من ينتج أو يعد أو يهيئ أو يرسل أو يخزّن أو يروّج عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها، أي محتوى مخلّ بالحياء أو النظام العام أو الآداب، يُعاقب بالسجن مدة لا تتجاوز خمس سنوات أو بالغرامة أو بالعقوبتين معاً.**
- **كل من يوفر أو يسهّل عمداً أو بإهمال عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها للوصول لمحتوى مخلّ بالحياء أو منافٍ للنظام العام أو الآداب، يُعاقب بالسجن مدة لا تتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معاً.**
- **إذا وُجه الفعل المشار إليه في البندين (1) و(2) إلى حدث يعاقب مرتكبها بالسجن مدة لا تتجاوز سبع سنوات أو بالغرامة أو بالعقوبتين معاً"**

- هناك غياب لفعل "الحيازة" أي حيازة المحتوى المذكور، فهل أنّ مصطلح "يخزّن" يتضمّنه؟ الأفضل ومنعاً للقياس أنْ ينص صراحة على "حيازة أي محتوى مُخلّ بالنظام العام. " وهنا **يُقترح ألّا تكون العقوبة مُرتفعة** لأن الضرر منحصر بالشخص الحائز والذي يعبّر عن سُلوك مُنحرف وغير سليم له إنّما لم يُسبّب أي ضرر للغير.
- أهمية ضبط معيار النظام العام والآداب العامة وتعريف المكان العام والزي الفاضح (لأن القانون الجنائي السوداني وهو القانون العام بالنسبة إلى القانون الراهن ينص على ضبط هذا المعيار).
- كما **يُقترح أنْ تكون عقوبة من ينشُر ويوزّع ويروّج أشدّ من عقوبة من ينتُج ويُهيئ ويعدّ،** لأنّ الضرر الجسيم والفعلي من المواد الإباحية لا يتأتى إلّا عبر نشرها وخدش شعور الرأي العام.

المادة السادسة عشرة: انتهاك المعتقدات الدينية او حرمة الحياة الخاصة

- **"كل من ينتهك أو يسئ أي من المعتقدات الدينية أو حرمة الحياة الخاصة عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها، يُعاقب بالسجن مدة لا تتجاوز ثلاث سنوات أو بالغرامة أو بالعقوبتين معاً."**
- **أضف أنّه يقترح أن تجمع "حرمة الحياة الخاصة مع المادة التالية رقم 17 حول "إشانة السمعة".**
- كما أنْ مصطلح " حرمة الحياة الخاصة" شامل، بمعنى آخر إذا كان من المُسلّم به تجريم نشر صور غير مُباحة أو غير أخلاقية، فهل يقصد المشرّع السوداني تجريم نشر صور عائلية ولو كانت مشروعة ولا يشوبها أي شائبة؟ إنما تمّ نشرها من دون أخذ رأي العائلة؟ فالحق في الحياة الخاصة أحد أهم الحقوق التي تنص عليها المواثيق الدولية والدساتير والقوانين المحلية (ففي أذهان العديد أنّ عملاً كهذا غير مجرم ومشروع، ويختلف مفهومه بحسب الزمان والمكان حتى في الدول العربية في العصر الحالي).

- **يُقترح تجريم نشر أي صور أو معلومة أو بيانات أو مستندات من دون إذن اصحابها حتى ولو كانت شرعيّة، بحيث تختلف العقوبة وتُشدّد في حال كانت هذه المُحتويات غير شرعيّة أو سريّة** (بالطبع بإستثناء حكم قضائي او إذن الفرد).

- **تجريم إفشاء معلومات ذات طابع شخصي dissemination of personal data أو سري من دون إذن اصحابها، أو إذن المراجع الرسمية أو القضائية المختصّة، سواء عن قصد أو عن إهمال مع تشديد العقوبة في الحالة الأولى (اي عن قصد)، وفي حالة تم الإفشاء من قبل الشخص المسؤول أو الموظف العام.**

- **تجريم عدم استجابة المُجرم criminal للمجني عليه victim لإلغاء المعلومات المنشورة والتي تطال حياته الخاصة أو معلومات شخصية.**

الفصل الخامس: جرائم الإرهاب والملكية الفكرية

- **المادة الثامنة عشرة: إنشاء أو نشر المواقع للجماعات الارهابية:**

- "كل من ينشئ أو ينشر أو يستخدم موقعاً على شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها لجماعة إرهابية تحت أي مسمي لتسهيل الاتصال بقياداتها أو أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع المواد الحارقة أو المتفجرة أو أية أدوات تستخدم في الأعمال الإرهابية، يُعاقب بالسجن مدة لا تتجاوز سبع سنوات أو بالغرامة أو بالعقوبتين معاً."

اهمية تجريم سائر الجرائم الدولية:

- **يُقترح تجريم "تنفيذ العمليات الإرهابية بوسائل معلوماتية حديثة"**، (فالمادة الراهنة تجرم مرحلة الإعداد وإنشاء الموقع والنشر) إنما التساؤل ماذا عن استخدام نظام معلوماتي في تفجير قطاع للاتصالات أو للنقل الجوي أو المصارف (على سبيل المثال إسقاط طائرة عبر التحكّم بنظام سيرها).

- تجريم الإعداد أو التحريض على ارتكاب الجرائم الدولية بوسائل معلوماتية وهي: جريمة الإبادة الجماعية (والتفرقة أو النعرات العنصرية والعرقية أو المذهبية أو بحسب اللون)؛ وجرائم التحريض أو المساعدة بوسيلة إلكترونية على ارتكاب جرائم ضد الإنسانية crimes against humanity؛ أيضاً جرائم الحرب؛ جريمة العدوان: تجريم كل الوسائل المعلوماتية لإرتكابها على سبيل المثال لا الحصر: النشر، التوزيع، التهديد، التعدّي، تبرير هكذا جرائم تحت أية ذريعة، لا سيما أنّ المعلوماتية تسمح بوصول هكذا معلومات إلى الأسرة البشرية بأكملها وليس على نطاق محدّد.

المادة التاسعة عشرة: جريمة نشر المصنفات الفكرية:

- **"كل من ينشر دون وجه حق عن طريق شبكه المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها أي مصنفات فكرية أو أدبية أو أبحاث علمية أو ما في حكمها، يُعاقب بالسجن مدة لا تتجاوز سنة أو الغرامة أو بالعقوبتين معاً.«**

- الملاحظة الموضوعية تكمُن في استخدام عبارة "مصنّفات فكرية أو أدبية أو أبحاث علمية"، فلِمَ حصر المُصنّفات في هذه الفئات الثلاث عِلماً أنّ مصطلح "مصنّف" يشمل أي عمل أدبي، مسرحي، موسيقي، لوحة، زخرفة، نحت، تصوير، رسم، حفل، صورة، شريط مسجل، اسطوانة، فيلم سينمائي، برنامج تلفزيوني، عمل إذاعي، لم يسبُق نشره وتمّ تسجيله وفقاً لأحكام القانون السوداني الخاص بحماية حق المؤلف والحقوق المجاورة لعام 1996. **يُقترح على الأقل عطف هذه المادة على القانون المذكور، والنص فقط على مُصطلح "المصنّف" بمفهوم القانون المذكور، وأن يُضاف على النص صراحة تجريم الاعتداء على الملكية الفكرية intellectual property crimes والمُصنّفات الرقمية نظراً لانتشارها بشكل هائل على المواقع الإلكترونية، أو النص عموماً على معاقبة أي فعل اعتداء على أي حق من حقوق المؤلف أو الحقوق المُجاورة المتعلّقة بأي عمل رقمي digital rights.** ماذا بالنسبة إلى نشر "برامج حاسوبية" وتوزيعها من دون إذن صاحبها؟

الفصل السادس: جرائم الإتجار في الجنس البشري والمخدرات وغسل الأموال

- **الإتجار في الجنس البشري (م. 20):**
- **"كل من ينشئ أو ينشر موقعاً على شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها بقصد الإتجار في الجنس البشري أو تسهيل التعامل فيه، يُعاقب بالسجن مدة لا تتجاوز عشر سنوات أو بالغرامة أو بالعقوبتين معاً".**

- ماذا بالنسبة إلى الذي يدخُل إلى موقع موجود أصلاً ويسهّل هذا الإتجار أو يشارك في عملية العرض والطلب؟
- ماذا بالنسبة إلى الإتجار بالأطفال، التحرّش بهم عبر المواقع الإلكترونية؟.
- غياب تشديد العقوبة في حال كانت الضحية أطفالاً أو قاصرين (مراجعة بروتوكول الأمم المتحدة).
- الأهم إلغاء الاختيار بين السجن والغرامة فهذه من أشد الجنايات خطورةً.

المادة الحادية والعشرين: الإتجار او الترويج للمخدرات او المؤثرات العقلية

- **"كل من ينشئ أو ينشر موقعاً على شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها بقصد الإتجار أو الترويج للمخدرات أو المؤثرات العقلية أو ما في حكمها أو يسهل التعامل فيها، يعاقب بالسجن مدة لا تتجاوز عشرين سنة أو بالغرامة أو بالعقوبتين معاً."**

- **يقترح تجريم "تسهيل وترويج المقامرة بوسائل معلوماتية" Facilitating and encouraging online gambingعبر تملّك أو إدارة مشروع مقامرة على الإنترنت Owning and operating a gambling business onlineأو التسهيل أو الترويج أو الدعاية والعرض (من دون إذن أو ترخيص).**

- هناك غياب لتجريم "ترويج الكحول على الإنترنت" providing alcohol to minors onlineولاسيما تحريض القاصرين على تعاطيها وعلى السُكر.

المادة الثانية والعشرون: غسل الأموال

- **"كل من يقوم بعملية غسل الأموال بالتسهيل أو التحويل أو الترويج أو إعادة تدويرها بواسطة شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها ليكسبها الصفة القانونية مع علمه بأنها مستمدة من مصدر غير مشروع يعاقب بالسجن مدة لا تتجاوز عشر سنوات أو بالغرامة أو بالعقوبتين معاً .«**

- يُشترط في هذه المادة أنْ يكون الجاني عالماً بأنّ مصدر الأموال غير شرعي-illegal obtained monies (أي عن قصد). ماذا لو تمّ ذلك عن إهمال وعدم مراعاة القوانين والتعاميم المختصة (أي عن غير قصد)؟ **فيُفترض التعديل لهذه الناحية مع تمييز العقوبة وجعلها أشدّ في حال ارتكاب هذه الجريمة عن قصد.**

- اللافت أن هذه المادة لا تُجرّم "المجرم الأساسي والأصلي"، أي صاحب الأموال غير الشرعية، فهي موجّهة فقط إلى من يسهّل ويروّج ويدوّر هذه الأموال، **فيُفترض التعديل أيضاً لهذه الناحية وإضافة "كل من يقوم بعملية غسل الأموال أو تسهيلها أو ترويجها أو تدويرها" لأن المجرم الأساسي يكون عرضة للملاحقة بجرائم أخرى كالسرقة والاحتيال.**

الفصل السابع: أحكام عامة

- **المادة الثالثة والعشرون: التحريض أو الإتفاق أو الإشتراك**
- "يُعدّ مرتكباً جريمة التحريض كل من حرّض أو ساعد أو اتفق أو اشترك مع الغير على ارتكاب جريمة من الجرائم المنصوص عليها في هذا القانون، وإن لم تقع الجريمة يعاقب بنصف العقوبة المقررة لها.
- إذا وقعت الجريمة نتيجة لذلك التحريض يعاقب المحرض بذات العقوبة المقررة لها."

- **المادة الرابعة والعشرون: الشروع**
- "يُعدّ مرتكباً جريمة الشروع كل من شرع في ارتكاب جريمة من الجرائم المنصوص عليها في هذا القانون ويعاقب بنصف العقوبة المقررة لها ."

المادة الخامسة والعشرون: المصادرة:

- "مع عدم الإخلال بحقوق غير حسنى النية، يجب على المحكمة في جميع الأحوال أن تحكم **بمصادرة الأجهزة أو البرامج أو الوسائط المستخدمة في ارتكاب** أي من الجرائم المنصوص عليها في هذا القانون أو الأموال المتحصلة منها، كما يجب **إغلاق المحل** أو المشروع الذي ارتكبت فيه أي من الجرائم الواردة في هذا القانون إذا ما ارتكبت الجريمة بعلم مالكه، وذلك للمدة التي تراها المحكمة مناسبة.«

- **المادة السادسة والعشرون: إبعاد الأجنبي**

الفصل الثامن: إجراءات تنفيذ القانون

- هو الفصل الأهم في هذا القانون لناحية القواعد الإجرائية التي تتعلّق بالضابطة العدلية المختصة، حُجية الدليل الرقمي، التقصّي الإلكتروني، التفتيش والضبط، الإختصاص القضائي وأصول المحاكمات الجزائية.

- **المادة الثامنة والعشرون: المحكمة المختصة**
- "ينشئ رئيس القضاء وفقاً لقانون الهيئة القضائية لسنة 1986 محكمة خاصة للجرائم المنصوص عليها في هذا القانون".
- إلا أنّ المحكمة الناظرة في قضايا جرائم المعلوماتية في السودان هي محكمة ضمن اختصاص محكمة الملكية الفكرية.
-
- **المادة التاسعة والعشرون: النيابة المختصة**
- "تُنشأ بموجب أحكام قانون تنظيم وزارة العدل لسنة 1983 نيابة متخصصة لجرائم المعلوماتية."
-
- أيضاً النيابة العامة المختصة حالياً في السودان هي النيابة العامة ضمن نيابة التحقيق الجنائي.
-
- **المادة الثلاثون: الشرطة المختصة**
- "تُنشأ بموجب أحكام قانون شرطة السودان لسنة 2007 المتخصصة لجرائم المعلوماتية
- الملاحظة عينها بالنسبة إلى الشرطة والتي تُعتبر جزءاً من شرطة المباحث المركزية.
-

جانب الحوكمة القانونية لجرائم المعلوماتية:

- **يُقترح إنشاء محاكم ونيابة عامة وضوابطة عدلية متخصصة في قضايا جرائم المعلوماتية بشكلٍ مستقلٍ عن سائر الأجهزة وفي مجمّع واحد،** مع تدريب وتخصّص المسؤولين وسائر العاملين فيها.
- على مستوى جهاز الشرطة القضائية، لا شك أن خصوصية وطبيعة الجريمة المعلوماتية بمختلف صورها المجرّمة وبتطبيقاتها المجرّمة، تفرُض على جهاز الشرطة القضائية اتباع التقنيات العلمية والتكنولوجية للبحث والتحرّي، واستجماع الأدلة والإثباتات المتعلقة سواء بشخص الفاعل أو بطبيعة الفعل المرتكب وحدوده، وإن كان هذا لا يقلّل من أهمية وسائل الإثبات التقليدية كالإعتراف أو التفتيش أو الحجوزات وغيرهما.

آليات نطاق التفتيش والضبط في دعاوى جرائم المعلوماتية:

- لا بدّ من الإعتراف بصعوبة وسائل الإثبات والتفتيش وصعوبة الوصول إلى الأدلة أو لغياب الاعتراف القانوني بطبيعة الأدلة المتعلقة بهذه الجرائم، وصعوبة الوصول إلى مرتكب الجريمة أو كشفه نظراً الى سهولة إتلاف الأدلة من الجناة، مما يوجد مشكلة قانونية لرجال الشرطة والقضاء الذين لا يملكون أحياناً الخبرة التقنية الكافية، من حيث مدى قبولها، وحجيتها والمعايير المتطلبة لاعتمادها إزاء هذا الاختراع الذي ينقل ويحرّف ويعبث بالمعلومات عبر نبضات إلكترونية، أو حتى اتصال هاتفي واستحالة اكتشافها أحياناً.
- إنما يجدر التنبه لعدم الخطأ في التفتيش والضبط الالكترونيين مما يؤدي إلى عدم كشف الجريمة، أو ضبط الأدلة ومعرفة الفاعل، ولا سيما أن المجرمين الموهوبين ربما يخدعون أفضل الخبراء. وهو أمر متوقع الحصول في أي تفتيش للفضاء الالكتروني أو لنظام معلوماتي وعموماً للعالم الافتراضي مما يثير العديد من المحاذير.

مقترحات للتحقيق الأولي:

- تكوين مجموعة من المحقّقين المتخصّصين في ميدان جرائم المعلوماتية ويتم إلحاقهم بجهاز الشرطة، بهدف دعم القدرات العملية الميدانية للشرطة القضائية وتعزيزها؛
- إحداث وحدة تقصّي آثار الجرائم المعلوماتية؛...
- إنشاء مختبرات لتحليل ومعالجة الآثار الرقمية؛
- اعتماد "الإثبات الإلكتروني" و"الدليل الرقمي الجنائي»؛
- استعانة قضاء الملاحقة والتحقيق والحكم بالخبرة التقنية؛

اثناء المحاكمات...

- على المحكمة أن تبني حكمها أو قرارها على حجج تُعرَض أثناء الجلسات وتُناقش شفهياً أمامها وفي حضور جميع الأطراف، بما فيها الحجج والأدلّة المستمدة من الحاسوب كالوثائق المعلوماتية والأشرطة الممغنطة والمصغرات الفيلمية، أو ببيانات معروضة على شاشة الحاسوب أو معطيات مستخرجة منه أو بتقارير تقنية منجزة من الشرطة التقنية والعلمية أو من مُختبرات استغلال الآثار الإلكترونية أو من غير ذلك من الوحدات والخلايا الأمنية المختصة في التحريّ والتثبّت من ارتكاب الجرائم المعلوماتية، أو تعلّق الأمر بوسائل إثبات تقليديّة، وأن تضمّن حكمها جميع الأسباب الواقعية والقانونية التي ينبني عليها، وإذا ارتأت أنّ الإثبات غير قائم تقرّر عدم إدانة المتهم وتحكم بالبراءة.

مقترحات للمحاكمة...

- أهمية مراعاة الخصوصية واحترام الحياة الخاصة، وحفظ السر المهني تحت طائلة العقوبة الجزائية، فيما يتعلّق بالمجرم المعلوماتي أو ضحايا المعلوماتية في معرض التفتيش أو ضبط الحاسوب أو الدخول إلى البريد الإلكتروني أو المواقع الإلكترونية الخاصة بهم، فيُفترض أن تتمتّع بحرمة المنزل الخاصة نفسها أثناء تفتيشه أو ضبطه.

- للمتهم بجريمة معلوماتية الحق في طلب الخبرة المقابلة للخبرة المُستند عليها قرار اتهامه، والحق في عدم إجراء أي عمليات تفتيش الحاسوب، أو ضبطه، أو حجزه أو توقيف برنامجه المعلوماتي أو بريده الإلكتروني إلا بحضور من يمثله قانوناً.

- ولكي لا يفوّت القضاء السوداني فرصة الإفادة من "الشهادة"، يُقترح توفير حماية خاصة "للشاهد المعلوماتي"، لئلا يوضع موضع تساؤل عن أمور خاصة، أو موضع استهجان من المجرم أو الضحية إذا لم يشهد لمصلحة أحدهما.

خاتمة ومقترحات:

أولاً على الصعيد الموضوعي:

- ضرورة تدخّل المشرّع الجزائي في السودان لتعديل قانون جرائم المعلوماتية الساري المفعول، وتحديثه ضمن ترسانةٍ تشريعيةٍ مُتكاملة؛

- وجوب تشديد عقوبات جرائم المعلوماتية، وجعل البعض منها جنايات وعدم ترك الخيار بين السجن والغرامة؛ وأيضاً أهمية إلغاء الإختيار بين العقوبة البدنية والغرامة في كل الجرائم التي تستحق عقوبة تفوق ثلاث سنوات.

- هناك غياب لجريمة الإخفاق في إبلاغ السلطات أو الإبلاغ الخاطئ عن جرائم المعلوماتية.

- هناك غياب للنص على بعض ظروف التشديد في حالات محددة على سبيل المثال لا الحصر: ارتكاب الجريمة ضمن عصابة منظّمة أو عابرة للحدود، أو من موظف عام، استغلال النفوذ أو السلطة، أو لأصحاب السوابق الإجرامية للمُكررين أو للمُمتهنين.

خاتمة ومقترحات:

- **أيضاً هناك غياب للنص على بعض الأعذار المخففة أو المحلّة لبعض جرائم المعلوماتية، وإعطاء سلطة جوازية للمحكمة لمنح بعض الأسباب التخفيفية، كمبادرة أحد أعضاء العصابة (المجرم النادم) على إبلاغ الدولة حول مؤامرة أو التخطيط الالكتروني لعمليات إرهابية (ويميّز هنا إذا ما تمّ إبلاغ الدولة قبل وقوع المؤامرة أم بعد وقوعها إنما أدّى إلى تعقّب المجرمين وتوقيفهم)**
- **أهمية تجريم "التحريض على القتل"، والتحريض على الانتحار وطريقة التحضير له وهي من الجرائم الرائجة على الإنترنت.**
- **أهمية تجريم الشخص المعنوي كالشركات إذا وقعت إحدى الجرائم المذكورة من مُستخدم يعمل باسمها ولمصلحتها، والنص على حلّها، أو إقفالها وفرض غرامة مالية عليها.**

ثانياً: على صعيد الإجراءات لملاحقة جرائم المعلوماتية

- اعتماد اجراءات التحري، ووسائل التفتيش الالكتروني والضبط الالكتروني؛
- يُفترض أنْ تكون جرائم المعلوماتية من جرائم الحق العام، إلّا في حالة جرائم المعلوماتية الماسة بحرمة الحياة الخاصة.
- أهمية تحقيق حماية جزائية للمعلومات المبرمجة التي تتميّز بالضخامة والتنوّع.
- أهمية توفير حماية لكلمات السر Password من محاولة المُقتحمين التعرّف إليها أو الإتجار بها، مما يُسبّب أضراراً هائلة للشركات وللأفراد.
- التنسيق بين الوزارات المتخصّصة (وزارة العدل ، وزارة الإقتصاد، وزارة الاتصالات، وزارة العلوم والتكنولوجيا، وزارة الداخلية) لمنع التضارب في الصلاحيات والاختصاصات بل التعاون فيما بينها.

ثالثاً: على صعيد التعاون الاقليمي والدولي

- أهمية الاتصالات الشرطية الفاعلة والتعاون القضائي الاقليمي والدولي.
- الأخذ بعين الاعتبار أهمية توفير التجانس في ما بين التشريعات العربية لردم الهوة الرقمية، لتسهيل معاملات المعاملات الإلكترونية electronic transactions ولمكافحة جرائم المعلوماتية.
- دعوة السودان إلى الإسترشاد بإرشادات الأسكوا (لعام 2012)، والقانون العربي الإسترشادي لحماية الملكية الفكرية الذي اعتُمد في مجلس وزراء العدل العرب بقرار رقم 940/د28، وقانون الإمارات العربي الإسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها.
- تشجيع توفير المساعدة التقنية للسودان من خلال الخبرة الفنية، وتطوير مبادرات التعاون التقني، وخبرات وخدمات استشارية، وتدابير ذات صلة بالقطاعات الرقابية والمالية،
- **التوعية وبناء القدرات.**

ختاماً...

- أما عن المستقبل، إذا كانت العولمة والتكنولوجيا تسبّب إشكاليات قانونية حديثة ومعقدة، فإنها توفّر أيضاً فرصاً جديدة للمحقّقين، فيرجو الإفادة منها.