مجلة
البوصلة الرقمية

المجلة الليبية لقانون الانترنت

تصدر عن إدارة مكافحة جرائم تقنية المعلومات
جهاز المباحث الجنائية / وزارة الداخلية الليبية

العدد الأول
مارس 2025

The Digital Compass

Libyan Journal of CyberLaw

2025 March/001

إدارة مكافحة جرائم تقنية المعلومات

مجلة البوصلة الرقمية
المجلة الليبية لقانون الانترنت

السنة الاولى
2025

صَدَرَت هذه المجلة بموجب:

قرار رئيس جهاز المباحث الجنائية رقم (214) لسنة 2025
بشأن إنشاء مجلة علمية دورية متخصصة.

قرار مدير إدارة المطبوعات والمصنفات الفنية رقم (07) لسنة 2025
بشأن الإذن بإصدار مجلة علمية إلكترونية.

رقم الايداع القانوني / 294 - 2025 دار الكتب الوطنية

تصدر عن إدارة مكافحة جرائم تقنية المعلومات
جهاز المباحث الجنائية / وزارة الداخلية الليبية

تمت طباعة هذا العدد بدعم من المؤسسة الليبية للتقنية

مشرف عام المجلة:
اللواء محمود عاشور العجيلي

رئيس تحرير المجلة:
اللواء صلاح الدين مصطفى بن سليمان

مدير التحرير:
د. محمد عبد الرحمن الفيتوري

مستشار المجلة:
د. عمر محمد بن يونس

رئيس الهيئة العلمية:
أ. فرج بشير برنوص

منسق التحرير:
أبوبكر محمد الهنشيري

تنفيذ وإخراج:
أيمن سليمان الشتيوي

المحتويات

لواء محمود عاشور العجيلي
رئيس جهاز المباحث الجنائية
المشرف العام للمجلة

يسعدنا ويشرفنا أن نقدّم لقرائنا الكرام العدد الأول من مجلة البوصلة الرقمية التي تصدر عن جهاز المباحث الجنائية كمنبر معرفي متخصص في قضايا قانون الإنترنت والجرائم الإفتراضية بهدف تعزيز الوعي القانوني والتقني حول التحديات التي يفرضها العصر الرقمي.

لقد أصبحت الجرائم الافتراضية اليوم واحدة من أخطر التهديدات التي تواجه الأفراد والمجتمعات والدول، حيث تتجاوز آثارها الحدود الجغرافية لتصل إلى كل بيت ومؤسسة. فمع التطور المتسارع في تكنولوجيا المعلومات والاتصالات، نشهد تزايدًا في أشكال الاحتيال الإلكتروني، واختراق البيانات، والابتزاز الرقمي، ونشر الشائعات، وتهديد الأمن السيبراني، مما يجعل الحاجة إلى مكافحتها ضرورة ملحّة تتطلب تعاونًا وثيقًا بين الأجهزة الأمنية، والجهات التشريعية، والمجتمع المدني.

إن إطلاق هذه المجلة يأتي في إطار التزامنا بمواكبة المستجدات في هذا المجال، وتقديم منصة علمية وتوعوية تساهم في نشر المعرفة القانونية والتقنية، وتسليط الضوء على أحدث التطورات في مكافحة الجرائم الإفتراضية، سواء من خلال التحليل القانوني، أو الدراسات المتخصصة، أو استعراض الجهود الوطنية والدولية في هذا المضمار.

نأمل أن تكون مجلة البوصلة الرقمية دليلًا لكل من يسعى إلى فهم الواقع الرقمي الجديد بكل تفاصيله وأبعاده، وأن تشكل إضافة نوعية في مجال تعزيز الأمن السيبراني، وتوفير بيئة رقمية أكثر أمانًا واستقرارًا.

ختامًا، نتوجه بالشكر والتقدير لكل من ساهم في إصدار هذا العدد، ونوجه الدعوة إلى كافة الباحثين والمتخصصين والمهتمين لإثراء صفحات الأعداد القادمة. فالمعرفة هي سلاحنا الأقوى في مواجهة تحديات العصر الرقمي.

إعداد لواء صلاح الدين مصطفى بن سليمان
مدير إدارة مكافحة جرائم تقنية المعلومات
بجهاز المباحث الجنائية

إدارة مكافحة جرائم تقنية المعلومات بجهاز المباحث الجنائية: بين التحديات والتطلعات

في ظل التحولات الرقمية المتسارعة باتت جرائم تقنية المعلومات من أخطر التحديات التي تهدد الأمن السيبراني والعدالة الجنائية على مستوى العالم. فهذه الجرائم لا تقتصر على اختراق الأنظمة وسرقة البيانات بل تمتد إلى الاحتيال الإلكتروني والتجسس وتهديد البنية التحتية الرقمية للدول. ومع تطور التقنيات تزداد أساليب الجريمة تعقيدًا مما يستلزم استراتيجيات أمنية متقدمة للتصدي لها.

في هذا السياق، تبرز إدارة مكافحة جرائم تقنية المعلومات بجهاز المباحث الجنائية كدرع حامي في هذه المواجهة حيث تسعى إلى بناء منظومة أمنية متكاملة تعتمد على أحدث التقنيات وأساليب التحليل الجنائي الرقمي مع تعزيز التعاون الوطني والدولي من خلال وزارة الداخلية لملاحقة الجناة وحماية الحقوق وتقديم الأدلة الرقمية. وفي هذا المقال، نسلط الضوء على رؤية هذه الإدارة وأهدافها الاستراتيجية والتحديات التي تواجهها بالإضافة إلى استعراض الحلول المستقبلية التي تضمن بيئة رقمية أكثر أمانًا واستقرارًا.

الرؤية: نحو ريادة في مكافحة الجريمة الافتراضية..

تطمح إدارة مكافحة جرائم تقنية المعلومات إلى أن تكون نموذجًا رياديًا في مجال مكافحة الجرائم الافتراضية من خلال تبني أحدث التقنيات وأساليب التحليل الرقمي بما يسهم في تحقيق أعلى مستويات الأمن السيبراني وحماية الأفراد والمؤسسات والدولة من مخاطر الجريمة الافتراضية.

الرسالة: تعزيز الخدمات الأمنية بمنهجية متكاملة

تتمثل رسالة الإدارة في تعزيز الخدمات الأمنية من خلال نهج وقائي واستباقي يعتمد على الرصد المستمر والتحقيق الفعّال في الجرائم الافتراضية مع تعزيز التعاون المحلي والدولي وتطوير الكفاءات البشرية القادرة على مواجهة التحديات المستجدة في عالم الجريمة الافتراضية.

الأهداف الاستراتيجية للإدارة

لتحقيق رسالتها ورؤيتها وضعت الإدارة مجموعة من الأهداف الاستراتيجية من

مكافحة الجرائم الافتراضية: عبر رصد وتحليل الجرائم الافتراضية باستخدام أحدث تقنيات التحليل الجنائي الرقمي.

تعزيز الوعي والتثقيف: نشر الثقافة الأمنية الرقمية بين الأفراد والمؤسسات للحد من مخاطر الجرائم الافتراضية.

تطوير الكوادر البشرية: تأهيل وتدريب الكوادر الأمنية على أحدث الأساليب والتقنيات في مجال التحقيقات الجنائية الرقمية .

تعزيز التعاون المحلي والدولي: إقامة شراكات استراتيجية مع الجهات الأمنية والمؤسسات التقنية لمكافحة الجرائم الافتراضية بشكل أكثر كفاءة.

تحديث البنية التشريعية: المساهمة في تطوير القوانين والتشريعات الخاصة بالجرائم الافتراضية بما يضمن استجابة قانونية أكثر فعالية لمواجهة هذه الجرائم.

التحديات التي تواجه الإدارة.

رغم الجهود الكبيرة التي تبذلها الإدارة فإنها تواجه العديد من التحديات من أبرزها:

التطور السريع في أساليب الجرائم الافتراضية مما يتطلب تحديثًا مستمرًا للوسائل والأدوات المستخدمة في المكافحة.

التحديات القانونية والتشريعية حيث تحتاج القوانين إلى التطوير المستمر لمواكبة طبيعة الجرائم الافتراضية المتغيرة.

التعاون الدولي في مكافحة الجرائم الافتراضية نظرًا للطبيعة العابرة للحدود لهذه الجرائم مما يتطلب تنسيقًا أمنيًا دوليًا مع مختلف الجهات المختصة بما في ذلك مزود الخدمة الخارجي.

نقص الكفاءات المتخصصة إذ يتطلب هذا المجال كوادر بشرية ذات مهارات متقدمة في مجالات الأمن السيبراني والتحليل الرقمي الجنائي.

التطلعات والطموحات المستقبلية

لمواكبة التحديات المتزايدة في عالم الجريمة الافتراضية تسعى الإدارة إلى تحقيق عدة تطلعات استراتيجية من أبرزها:

إطلاق مختبرات جنائية رقمية متطورة تعمل وفق أحدث المعايير العالمية في مجال الأدلة الرقمية والتحقيقات السيبرانية.

تعزيز استخدام تقنيات الذكاء الاصطناعي والتعلم الآلي في رصد الجرائم الافتراضية والتنبؤ بها قبل وقوعها.

توسيع نطاق التعاون الدولي من خلال جهاز المباحث الجنائية وتحت مظلة وزارة الداخلية عبر بناء شراكات استراتيجية مع أجهزة الأمن السيبراني العالمية ومراكز البحث المتخصصة.

تعزيز التشريعات الخاصة بالجرائم الافتراضية لضمان بيئة قانونية رادعة قادرة على مواجهة التطورات السريعة في أساليبها .

الخاتمة

تواجه إدارة مكافحة جرائم تقنية المعلومات بجهاز المباحث الجنائية تحديات متزايدة في ظل التطورات السريعة التي يشهدها عالم الجرائم الافتراضية. ومع ذلك فإن رؤيتها الطموحة ورسالتها الواضحة وأهدافها الاستراتيجية تجعلها في طليعة الجهات المعنية بحماية حقوق الأفراد والمؤسسات ومن خلال تعزيز قدراتها التقنية وتوسيع شراكاتها الدولية وتطوير تشريعاتها فإنها تضع الأسس لمستقبل أكثر أمنًا في الفضاء الرقمي مما يرسّخ دورها كخط دفاع متقدم ضد التهديدات السيبرانية و الجرائم الافتراضية.

مناشط إدارة مكافحة جرائم تقنية المعلومات لسنة 2024م

المهمة	التفاصيل
الشؤون الإدارية :	
عدد الرسائل الواردة	1865
عدد الرسائل الصادرة	2179
مكتب الطب الشرعي الرقمي :	
إجمالي عدد القضايا المنجزة	601 قضية
إجمالي عدد المبرزات الإلكترونية التي تم العمل عليها	188 مبرزة إلكترونية
إجمالي قضايا الصفحات	454 قضية (عدد الصفحات التي تم العمل عليها : 630 صفحة)
قضايا الهواتف	54 قضية (عدد المبرزات التي تم العمل عليها: 86 هاتف)
قضايا كاميرات المراقبة	72 قضية (عدد المبرزات التي تم العمل عليها: 102)
القضايا المستجدة	18 قضية
التجارب الأمنية المميزة	3 تقارير للمشاركة مع الجهات ذات العلاقة
التدريب ورفع الكفاءة:	
التدريب الداخلي	10 دورات
التدريب الخارجي	6 دورات
الاجتماعات وورش العمل	
عدد الاجتماعات	22 اجتماع
عدد ورش العمل	9 ورش
البرامج التوعوية	
برامج مرئية	4 برامج
برامج مسموعة	7 برامج
البروموات التوعوية	7 بروموات
الدعم التقني	
تنفيذ تكليفات ومهام	18 تكليف (صيانة، كشف، ربط شبكات، تنصيب برامج وغيرها)
الدراسات والبحوث	
إعداد ملخصات دراسية	15 ملخصًا دراسيًا حول الجريمة الإلكترونية
حقيبة تدريبية معتمدة	للتوعية في أمن المعلومات والأمن السيبراني
عدد الدورات المقدمة	5 دورات بالإدارة العامة للتدريب

هذا الجدول يعكس جهود الإدارة في مكافحة الجريمة الإلكترونية وتطوير الكفاءات وتعزيز الوعي التقني والأمني.

مصطلحات رقمية

هذا البرنامج هو مبادرة من هذه الإدارة لطرح فكرة توحيد استخدام المصطلحات على الجهات والمؤسسات المختلفة في الدولة الليبية وسوف يتم تعميمه للفائدة. لذلك يرجى التفضل مشكورين بتداول هذه المصطلحات دون تعديل فيها ... والإدارة على استعداد تام لمناقشة كل ما يتعلق بضبط المصطلح... وهي خدمة تؤديها هذه الإدارة بالاستعانة بخبراء قانون الانترنت Cyberlaw. فمن الأهمية بمكان ضبط استخدام المصطلح في المعاملات اليومية ولدى القضاء والجهات الرسمية.

مصطلح الحاسوب والانترنت والعالم الافتراضي

الحاسوب Computer: من وسائل تكنولوجيا المعلومات. ويلزم فهمه على أساس استخدام القضاء المقارن له، فالمصطلح القضائي له يشير الى المعالج Processor تحديدا. والذي يمكن تركيبه في أي جهاز او ملحقات Peripherals كالهاتف النقال او الحاسوب الشخصي او المحمول او الثلاجة او العربة او.. الخ. فهو الذي يتفاعل ويأخذ طابع الحوسبة والرقمية. وعلى هذا النحو يعد المعالج هو المرادف لكلمة حاسوب في مفهوم القضاء المقارن. لذلك عندما يذكر مصطلح الحاسوب فهو يعني ما سلف. اما ما تلى ذلك فهي عبارة عن ملحقات به.

ومن الأهمية بمكان القول بان الترجمة العربية لمصطلح الكومبيوتر Computer الى حاسوب هي من اعمال مجمع اللغة العربية.

انترنت Internet: فهي عبرة عن وسيلة او إدارة تواصلية بين الحواسيب والشبكات دون اعتبار للحدود الدولية. حيث يلزم فهم الانترنت على أساس انها تقنية لها مهام محددة فهي أساسا تنقل من يتصل بها الى العالم الافتراضي. تنقله من العالم المادي الذي يعيش فيه ماديا الى عالم البيانات والمعلومات والبرمجة والنشاط التقني. فهي وسيلة مواصلات تحديدا. ولكن لا يعني مدلولها أكثر من ذلك فلا يفهم مدلول الانترنت على انها وسيلة كما لو كانت مثل السكين في جريمة القتل.. اذ يجب ان تفسر في إطار تكنولوجيا المعلومات لا أكثر. فهي ليست وسيلة جنائية وانما وسيلة تقنية معلومات تحديدا.

العالم الافتراضي cyberspace: وهو ذلك العالم المتواجد في حلقة التواصل الكبرى بين الحواسيب والشبكات. وهو مناط التعامل واليه تنقلنا الانترنت. وهناك العديد من الترجمات الخاطئة التي تأخذ الطابع الإعلامي مثل الفضاء الالكتروني او العالم الالكتروني او الترجمة الحرفية الخاطئة مثل السيبراني او.... الخ وهذه كلها ترجمات خاطئة.. لان هذا المصطلح من ابتكار الادب المعلومات/ الخيال العلمي. وكان اول ورود له في رواية الحالم الجديد Neuromancer للأديب الكندي الأمريكي William Jibson عام 1984 والتي استمد منها القضاء المقارن المصطلحات.. ورصدها كأساس لأحكامه.

فهناك في العالم الافتراضي يتم كل شيء، هناك البرمجة وهناك تبادل البيانات وهناك يتم التفاعل مع التقنية والتحول الرقمي يتم بالانتقال اليه. كل شيء هناك وحوله يدور العالم المعاصر. كل شيء هناك. حتى وان تصادف ان تخلف المصطلح العربي فنقول الانترنت او عبر الانترنت.. فهذه استخدامات إعلامية لا تفيد الدقة ولا تنتمي الى المصطلح الدقيق.

وصف العالم الافتراضي

Describing_Cyberspace

By Beer Sijpesteijn,

s0201162 for Technology and Social Order

مقدمة Introduction

يتناول هذا المقال مسألة تعريف وماهية «العالم الإفتراضي cyberspace». وهذا هو صراحة شيء مختلف ثم «التعامل مع تعريف العالم الإفتراضي». كما سنجادل أكثر في هذا المقال، والرغبة في التوصل إلى تعريف (في حالتنا) العالم الإفتراضي بالفعل ينقل ضمنا مجموعة من الافتراضات المسبقة لما قد يكون العالم الإفتراضي.

هذه هي الافتراضات الإفتراضية ontological presuppositions حول العلاقة بين التكنولوجيا والمجتمع، حول الطبيعة مقابل الثقافة والإنسان مقابل غير الإنسان. ومن أطروحتنا أن مثل هذه الثنائيات المفترضة تأتي بنتائج عكسية في محاولة لوصف (كبديل أكثر تواضعا لـ «تعريف») الظاهرة التي نشير إليها عادة باسم العالم الإفتراضي.

وعلى العكس من ذلك، نقترح الاقتراب من وصف العالم الإفتراضي من منظور التهجين perspective of hybridity، بما يتماشى مع ما يسميه أندروز بيكرينغ Andrews Pickering علم الوجود الحادث بالفعل ontology of becoming. في تحليلنا لخطاب تعريف العالم الإفتراضي، حيث نركز على كيفية تصارع الاستراتيجيين العسكريين والمشرعين مع هذا الموضوع.

مكان الميلاد في الخيال العلمي Born in science fiction

1980s, and The term cyberspace originates from science fiction works from the became widely known via William Gibson's novel Neuromancer, where it was described as follows:

مصطلح العالم الإفتراضي ينبع من أعمال الخيال العلمي science fiction وجد في ثمانينات القرن العشرين، وأصبح معروفا على نطاق واسع عن طريق رواية وليام جيبسون William Gibson «الحالم الجديد Neuromancer»، حيث وصفه على النحو التالي:

«العالم الإفتراضي. هو هلوسة جماعية consensual hallucination تعاني يوميا من قبل المليارات من المشغلين الشرعيين legitimate operators، في كل أمة، من قبل الأطفال ممن تم تعليمهم مفاهيم الرياضيات mathematical concepts... والتصوير البياني للبيانات المستخلصة من بنوك كل حاسوب في النظام البشري. تعقيد غير متصور Unthinkable complexity. وخطوط ضوء تتراوح في لا مساحة non-space في العقل، وقواطع clusters وكوكبات constellations من البيانات».

على الرغم من أن جيبسون ذكر في وقت لاحق أن الكلمة لم يكن لها أي معنى حقيقي بالنسبة له وأنه ينظر إليها بدلا من الكلمة الطنانة buzzword، فقد تم التقاط العالم الإفتراضي وككلمة ذات علاقة ناشئة من الإنترنت، اذ سرعان ما تصبح مصطلحا اجتماعيا لائقا household term. في الوقت الحاضر، والعالم الإفتراضي وغيرها من المصطلحات الافتراضية هي جزء من المفردات اليومية لدينا، ولكن تماما مثل وليم جيبسون قبل ثلاثين عاما، والناس (بما في ذلك العديد من

العلماء والمشرعين وهلم جرا) لديهم صعوبات difficulties في وصف «المعنى الحقيقي» لذلك. ففي العقيدة العسكرية military doctrine المعاصرة، على سبيل المثال، يعتبر العالم الإفتراضي الحيز الخامس fifth domain الذي يمكن أن تقع فيه الحرب، بعد الفضاء البري land والبحري sea والجوي air والفضاء «العادي» 'regular' space'. وبما أن أحد خصائص الجيش characteristics of the military هو محاولة أن يكون واضحا في السيطرة على كل ما يقوم به، فقد كان يحاول التقاط جوهر العالم الإفتراضي أيضا.

وقد أصدر البنتاغون Pentagon على مر السنين ما لا يقل عن اثني عشر تعريفا مختلفا لما يعتقد أنه العالم الإفتراضي. وفي كل مرة كانت هناك أسباب لرفض التعريف السائد prevailing definition. في بعض الأحيان لأن التعريف كان ضيقًا narrow جدًا ولم يتضمن جوانب يجب أن تشملها، في أحيان أخرى لأنه كان واسعًا جدًا ويشمل كل شيء من أجهزة الحاسوب والصواريخ إلى الضوء من الشمس. ومن المفارقات أنه مهما كان العالم الإفتراضي الذي قد ينطوي عليه، فإن جذوره تقع في ARPANET، التي تمولها ذات وزارة الدفاع الأمريكية.

وفقا لسنجر Singer وفريدمان Friedman، والعالم الإفتراضي هو بيئة المعلومات التي تتعامل مع البيانات الرقمية بطرق مختلفة (النسخ، ونقل، والتخزين،...)، ولكن في الوقت نفسه هو أجهزة الحاسوب وتقنيات الشبكات التي يحدث هذا. لذا فمن ناحية، ان العالم الإفتراضي هو شيء افتراضي virtual، ولكن ليس حصريا، لأنه من ناحية أخرى له جوانب مادية physical aspects. وعلاوة على ذلك، فإن العالم الإفتراضي هو مجال من صنع الإنسان manmade domain (في معارضة لمجالات الحرب domains of warfare الأربعة الأخرى) والأشخاص الذين يقفون وراء أجهزة الحاسوب الخاصة بهم، وتتولى إدارة البنية التحتية هي أيضا جزء مهم من العالم الإفتراضي. وكما قال المؤلفون: «يتم تعريف العالم الإفتراضي من قبل المجال المعرفي بقدر ما يعرف من قبل المادية أو الرقمية». (الصفحة 14).

الجانب التالي الذي يحدده سينغر Singer وفريدمان Friedman، وله أهمية قصوى في هذا المقال، هو أن العالم الإفتراضي يتطور باستمرار. حيث تذكر ثلاث طرق يعتقدون من خلالها أن العالم الإفتراضي يتطور. الطريقة الأولى التي يتطور بها العالم الإفتراضي هي في حجمه وحجمه.

على مدى العقد الماضي past decennia، تطور العالم الإفتراضي من شبكة حاسوب تسيطر عليها وزارة الدفاع الأمريكية بالكامل إلى الوضع الحالي حيث هو نظام اعلى درجة وأكبر وحيث يتصل connect به الناس في جميع أنحاء العالم ويقومون بقطع disconnect أجهزتهم معها باستمرار. ثانيا، تتطور التكنولوجيات التي تشكل العالم الإفتراضي.

For example, until ten years ago it was mostly wired connections, whilst today wireless connections of e.g. smartphones are also omnipresent. Lastly, the politics of cyberspace evolve. Now that SCADA-systems that control infrastructure such as

our energy networks are connected, policy makers look at it much differently than when it was mostly a realm for communication between researchers. This of course is also reflected in the fact that militaries around the world are busy with finding their place and role in cyberspace.

على سبيل المثال، حتى قبل عشر سنوات كانت الاتصالات سلكية wired connections في الغالب، في حين أن الاتصالات اللاسلكية اليوم للهواتف الذكية على سبيل المثال موجودة أيضًا في كل مكان. وأخيراً، تتطور سياسات العالم الإفتراضي. والآن بعد أن تم توصيل أنظمة SCADA التي تتحكم في البنية التحتية مثل شبكات الطاقة لدينا، ينظر واضعو السياسات إلى الأمر بشكل مختلف كثيرًا عما كان عليه عندما كان في الغالب مجالًا للتواصل بين الباحثين. وينعكس هذا بالطبع أيضاً في حقيقة أن الجيوش في جميع أنحاء العالم مشغولة بإيجاد مكانها ودورها في العالم الإفتراضي.

لقد بذلنا الجهد لشرح ما يكتبه سينجر Singer وفريدمان Friedman في فقرة من خمس صفحات مخصصة لتعريف العالم الإفتراضي، لأننا نعتقد أنه يعطينا تلميحات حول السبب في أنه من الصعب جدًا العثور على تعريف مناسب للعالم الإفتراضي، وكذلك حول كيفية التغلب على هذه المشكلة من خلال تغيير نهجنا تجاهها. والفقرة التالية مكرسة لبلورة هذا الموضو

وصف العالم الافتراضي Describing cyberspace

بدأنا هذه الدراسة بتوضيح أن القضية التي نحاول معالجتها هي مسألة «تعريف العالم الإفتراضي». وكما رأينا، فقد أصدر البنتاغون تعريفاً بعد تعريف ولم يكن أي منها مرضياً، ففي موقع مركز التميز للتعاوني الدفاعي الإفتراضي في حلف شمال الأطلسي the NATO Cooperative Cyber Defense Centre of Excellence، نحسب 22 تعريفاً مختلفاً تستخدمه الدول الأعضاء في حلف شمال الأطلسي.

نعتقد أن هذا مؤشر جيد على أن هناك شيء في متناول اليد مع «تعريف العالم الإفتراضي» ووفقا لنا فإن المشكلة لا تكمن في «العالم الإفتراضي»، ولكن في «وضع تعريف defining». وكما أوضح سينغر Singer وفريدمان Friedman، فإن إحدى خصائص العالم الإفتراضي characteristics of cyberspace هي أنه يتطور باستمرار constantly evolves.

هذا يصطدم مع الرغبة في تعريفه، فالعالم الإفتراضي هو أبعد ما يكون عن تحديد definite وشيء محدد وهو ما يحاول اي تعريف التقاطه. حيث نقترح استخدام كلمة «وصف describe» بدلاً من ذلك. وعلى الفور نريد أن نلاحظ أنه ليس في نيتنا أن نلعب لعبة كلمة word game هنا. ومن المسلم به أن «الوصف» قد يبدو ضعيفاً بعض الشيء وغير ملتزم، وقد توجد مصطلحات أفضل. وعارضنا oppose «وضع تعريف defining»، على أساس أن دلالته تحتوي على عنصر معين من عناصر الدوام. باستخدام «وصف describe» نريد أن نفسح المجال لنهج أكثر ديناميكية في التقاط فكرة العالم

الإفتراضي، والتي نعتقد أنها أكثر ملاءمة لهذه الظاهرة.

في نص سينجر Singer وفريدمان Friedman واجهنا جوانب مختلفة من العالم الإفتراضي، وأنها التمييز بين المجال المعرفي والمادي والافتراضي. عوالم مختلفة Different realms، كل مع كل منهما علم الانتولوجيا ontology الخاصة. النظر في ما بايت byte معين (كوحدة من المعلومات unit of information) هو في هذه ontologies.

من الناحية المعرفية Cognitively، قد يمثل رسالة كتبتها. فيزيائية Physically، قد يتم تخزينها على قرص صلب داخل الحاسوب في مكان ما، حيث يتم تخزينها عن طريق تكوين حقل مغناطيسي بطريقة معينة. وتقريبا، «داخل الحاسوب»، بل هو مجموعة من 8 بت bits التي يتم تخزينها في عنوان بيانات معينة. ولا يتناول أي من هذه البايتات byte وحدها بالكامل ما يشكله ذلك البايت byte في العالم الإفتراضي. فالعالم الإفتراضي هو، في مصطلحات terminology أندرو بيكرينغ Andrew Pickering (2001)، في منطقة تقاطع هذه العوالم at the zone of intersection of these realms.

عندما نريد أن تعريف define العالم الإفتراضي، نبحث عن تعريف definition يتناسب مع صورتنا لكيفية بناء العالم الإفتراضي. إذا نظرنا إلى الأمر من عالم مادي بحت، فقد نميل إلى النظر إلى العالم الإفتراضي بطريقة حتمية تكنولوجية، على أنه استمرار حتمي للابتكار التكنولوجي الذي ينمو من بعد ARPANET. إذا نظرنا إلى الأمر من عالم معرفي بحت، فقد نميل إلى أن ننظر إلى العالم الإفتراضي على أنه بناء اجتماعي. ونعتقد أن أيا من هذه لا حق في تطوير ظاهرة العالم الإفتراضي.

نعتقد أن فكرة بيكرينغ Pickering عن علم الوجود ontology بأن تصبح أكثر ملاءمة للعالم الإفتراضي. هذا هو السبب بالنسبة لنا استدعاء تعريف سينغر Singer وفريدمان Friedman في تحديد التطور المستمر للعالم الإفتراضي من أهمية قصوى. وقد أعطتنا لمحة عن المكان الذي نتطلع إليه للتغلب على مسألة تعريف العالم الإفتراضي.

وأيا كان شكل العالم الإفتراضي أو شكله في هذه اللحظة، فإنه ليس دائماً. جديد على الانترنت التكنولوجيات سوف تغير ما نقوم به في العالم الإفتراضي، وسلوكنا المتغير بدوره قد تحفز تطوير أو تغيير استخدام تقنيات أخرى. هذه هي الطريقة التي تطور بها العالم الإفتراضي حتى الآن ومن المرجح أن يستمر في التطور. هذا ما يسميه بيكرينغ Pickering رقصة الوكالة بين البشر وغير البشر (الصفحة 6).

وبالتالي وصف العالم الافتراضي! Then describe cyberspace!

فإذا اتبع المرء خط الجدل argumentation في هذا المقال، فقد يتفق على أنه من المنطقي عدم التوصل إلى تعريف دقيق للعالم الإفتراضي، بل وصفها بأنها ظاهرة متطورة في عالم هجين evolving phenomenon in a hybrid world. ولكن ماذا يعني هذا بالضبط إذا كنت أريد أو بحاجة إلى القيام بشيء ما مع العالم الإفتراضي. كيف يحل هذا المشاكل التي يكافح معها الاستراتيجيون العسكريون؟

?How does this solve the problems that military strategists struggle with

دعونا نبقى مع مثال الجيش. وكما رأينا، فإن الاستراتيجيين العسكريين الذين يكافحون مع تعريف العالم الإفتراضي يرجع إلى نهج خاطئ. فالعالم الإفتراضي هو ظاهرة هجينة hybrid phenomenon غير قابلة للتعريف بشكل مرضي في علم الوجود ontology في عالم معين certain realm. هذه هي الإشكالية problematic بالنسبة للجيش، لأنهم متخصصون (عن حق) في السيطرة (لغرض تأمين for the purpose of securing) عالم ما realm، مثل القوات الجوية لا في المجال الجوي. لو كان العالم الإفتراضي قابلاً للتعريف فقط من حيث التكنولوجيات المادية، لكان بإمكان الجيش اتخاذ تدابير تكنولوجية للسيطرة عليه وتأمينه. وقال انه كان يمكن تعريف العالم الإفتراضي بحتة من الناحية المعرفية، ثم كان يمكن إنشاء قوانين وقواعد معينة للسيطرة عليه وتأمينه.

ومع ذلك، فإن كل هذا ليس هو الحال. وتكشف التعريفات المختلفة المقترحة، مثل تلك الواردة في القائمة التي جمعها مركز التميز الدفاعي الإلكتروني التعاوني لحلف شمال الأطلسي by NATO Cooperative Cyber Defense Centre of Excellence، عن افتراضات مسبقة حول كيفية السيطرة على العالم الإفتراضي وتأمينه.

ما هو أكثر من ذلك، والرغبة بالفعل في تحديد (لا يزال في هذه الطريقة الدائمة) العالم الإفتراضي يكشف ضمنا عن الافتراضات المسبقة لما هو عليه. الآن بعد أن رأينا أن التعريف لا يعمل، ونحن (في casu الجيش) يجب أن تذهب كل في طريق العودة وإيجاد نهج جديد للوفاء بواجبهم، وتعديلها للوجود. وهو خارج نطاق هذا المقال كيفية القيام بذلك بالضبط، لكنه جزء من ما يدعو بيكرينغ Pickering سياسة أن تصبح والتلميح واحد انه يعطي ما يلي: «إذا كنا نعرف أننا نعيش في عالم من البشر human و غير البشر nonhuman الذين يصبحون مستجدات غير متوقعة unexpectable novelties سطح باستمرار، [...] وينبغي أن نحاول بدلا من ذلك أن نكون على ضوء سياسي politically light على أقدامنا، مستجيبين لما يظهر في الوقت المناسب». (الصفحة 15).

خاتمة Conclusion

ومن خلال أخذ المكافحة من الاستراتيجيين العسكريين كمثال، قدمنا مسألة تعريف العالم الإفتراضي. استخدمنا سينجر Singer وفريدمان Friedman لتوضيح أين تظهر الصعوبات، ولكن أيضًا لإيجاد اتجاه لحل المشكلة. من خلال الإشارة إلى نظريات أندرو بيكرينغ Andrew Pickering، جادلنا بأن «وضع تعريف defining» لا يتطابق مع علم الوجود الذي يصبح يناسب العالم الإفتراضي بشكل جيد. بدلا من ذلك، فمن الأفضل أن «تصف describe » الهجين hybridity من العالم الإفتراضي وضبط في المستقبل طريقة نهج التحديات المتعلقة بالعالم الإفتراضي وفقا لذلك.

وكملاحظة أخيرة، نود أن نشير إلى أنه إذا أعجب المرء بحججنا بشأن وصف العالم الإفتراضي، فقد يكتسب المرء إلى حد متواضع أيضا بعض التقدير الجديد للوصف الأصلي للعالم الإفتراضي الذي انتقده ويليام غيبسون William Gibson نفسه في وقت لاحق.

(نظرية الحق عبر الانترنت)

د. عمر محمد بن يونس
مستشار موسوعة التشريعات العربية
(جينيس للأرقام القياسية 1999- كتاب 2002- ص. 156)
رئيس الجمعية العربية لقانون الانترنت

خلفية :

هذه سلسلة الحقوق والحريات والالتزامات الرقمية تتناول موضوع ربط الرقمية كمنهج بنظرية الحق في الدراسات القانونية. وهي النظرية التي يتم تدريسها في مناهج السنة الأولى (الى جوار نظرية القانون) في كليات الحقوق والشريعة وبعض الكليات الاخرى لأنها تمثل بداية علاقة الطالب بالقانون المدني خاصة وبنظرية القانون ككل، وهي عادة ما تأخذ تسمية (المدخل الى دراسة القانون) او (المدخل الى الدراسات القانونية) في جزئين (نظرية القانون- نظرية الحق) وتشكل عماد فهم الطالب للدراسات القانونية قاطبة، وبدون الاهتمام بهذه المادة لن يكون لدينا طلاب وبالتالي رجال قانون في المستقبل على درجة ووعي بأهمية دورهم كحراس للنظام القانوني. وهذه السلسلة تستهدف البحث في مدى إمكانية تطوير نظرية الحق ونظرية القانون لكي تتواءم كل منهما مع التطورات الرقمية الحادثة في عالمنا المعاصر. فقد كان العدد الأول في هذه السلسلة يتناول دور الفقه المقارن (المؤتمر الإقليمي الأول نحو مجتمع معلومات أكثر عدالة- عمان/ الأردن 2004) والعدد الثاني يتناول المباديء الكبرى للحكومة الالكترونية (المؤتمر الرابع للحكومة الالكترونية شرم الشيخ/ مصر 2005) والعدد الثالث موضوع هذا البحث يتناول موضوع القانون الوطني الامريكي (المؤتمر الأول لأمن المعلومات مسقط/ سلطنة عمان 2005) وهو القانون الذي أثار الحيرة واجتهد الفقه في بحثه فكان فقها حائرا أكثر من كونه فقها يضع الحلول. لذلك رأينا متابعة منا لموضوع القانون الوطني الامريكي ضرورة طرح مفهومه بهدف التعريف به في هذه السلسلة ولكي يكون هذا البحث معينا أكاديميا على الطرح بشكل أكثر تجاوبا مع هذا القانون الذي أثار حفيظة الجميع.

(1)

دور الفقه المقارن

يتضمن الطرح في هذه الورقة رؤية الفقه المقارن لموضوع حقوق الانسان الرقمية والتي يجب أن تكون ذات طابع مميز عن تلك المادية، وهو تمييز عرضي من طبيعة جوهرية الا أنه ليس تمييزا جذريا، والجوهرية هنا يجب أن تفهم على أن الاختلاف قائم في النهاية. فالمسافة بين حقوق الانسان المادية وتلك الرقمية هي ذات المسافة القائمة بين العالم المادي الذي ورثته الثورة الصناعية، وبين العالم الرقمي الذي سوف ترثه الثورة الرقمية. ونحن إذ نعترف بوجود الثورة الصناعية ونتائجها الايجابية والسلبية خلال نيف ومائتي عام حتى الآن، فإننا نقر بأن الثورة الرقمية لها طابعها الخاص بها والذي يميزها عن غيرها، وبالتالي يجب الآخذ في الاعتبار النتائج الايجابية والسلبية لهذه الثورة الجديدة مع بناء فكر مميز وناضج نابع منها دون محاولة خلق تزاوج أولي بين هاتين الثورتين. فالأساس هو الفصل التام بينهما ثم بعد ذلك نتناول أوجه الاتفاق والخلاف بينهما، ودون ذلك سوف نقع في مأزق المزج بين الاثنتين وبما يؤدي الى سيطرة احداهما الأكثر نضجا (حقوق الانسان المادية) على الأخرى الأقل خبرة في هذا الاطار (حقوق الانسان الرقمية).

ففي إطار الحقوق والحريات الرقمية، يحاول الفقه جاهدا جمع شتاتها بما يقابلها من التزامات في شكل يبرر طابعها المصلحي عبر الانترنت ، والذي يسعى القانون الى المحافظة عليها. على أن هذه المحاولات لا زالت في طور التكوين ، اذ ليس من السهولة وضع تصنيف لمثل هذه الحقوق والحريات ويبدو ذلك – بشكل واضح – في العشوائية التي عليها عملية التصنيف.

– الحقوق والحريات والالتزامات الرقمية: لقد نشأ عن تداول موضوع الحقوق والالتزامات، وبالتالي الحريات، أن وجد موضوعا جديدا بدأ مع المحاولات الأولى للفقه حين تعرض لحقوق الملكية الفكرية ودراسة مشاكل النسخ وإعادة النشر رقميا فيما يعرف بادارة (حماية) الحقوق الرقمية **Digital rights Management DRM**[1]، تلك الحقوق أطلق عليها الحقوق الرقمية **Digital Rights** ويشمل ذلك شرط مستقبل التكنولوجيا **Future Technology Clause**. ولقد كان منبت هذه الفكرة أساسا هو ظهور شبكة المعلومات الدولية **World Wide Web** او

[1] **Robin Jeweler - CRS Report for Congress Received through the CRS Web Copyright Law: Digital Rights Management Legislation, Congressional Research Service ˜ The Library of Congress, May 28, 2004 " Digital Rights Management (DRM) refers to the technology that copyright owners use to protect digital media.".**

الويب **Web** على يد مهندس الاتصالات الانجليزي **Tim Burners Lee** في عام **1991** ، حيث بدا التأثر واضحا في رصد قوة النشر عبر الويب.

لقد شرع الفقه بداية في محاولة وضع تصنيف للحقوق التي يشملها موضوع الملكية الفكرية بإعتبارها "تلك الحقوق التي تتضمن الحق في وضع المصنف الأدبي،

1. عبر قاعدة بيانات اتصالية بنظام استردادي.
2. في كل او بعض اسطوانة ممغنطة مضغوطة.
3. في كل او بعض اسطوانة فيديو رقمية.
4. عبر الانترنت.
5. عبر موقع في شبكة المعلومات الدولية.
6. عبر نشرة الكترونية مثلما هو الحال في تلك الخدمات مثل امريكا او لاين او كومبيو سيرف او بروديجي[1].

ويضاف الى التصنيف السالف شرط مستقبل التكنولوجيا كنوع من الشمولية والذي يسمح باضافة حقوق جديدة الى القائمة السالفة بالإضافة الى أن إقراره في العقد يسمح لأحد المتعاقدين بالنشر الإلكتروني وهو شرط نجده في المرحلة المعاصرة في عقود الصحافة الحرة.

واذا كان ذلك هو المرادف الأولي للحقوق الالكترونية او الرقمية فإن ذلك لا يعفي من القول بأن هناك محاولات لعرض مفهوم أوسع للحقوق والحريات والالتزامات عبر الانترنت يشمل ما هو أوسع مدى من حصر الحقوق الرقمية في اطار حقوق الملكية الفكرية.

ومن بين هذه المحاولات كانت محاولة الاستراليالاستاذ **Peter Mere** [1] في عام **1996** حيث قام بتقسيم هذه الحقوق الى خمسة أقسام هي حقوق الاتصال[2] والحق في الخصوصية[3] وحق

---

[1] **(RICH) Lloyd L. – Legal articles, Who controls e-rights- the writer or publisher ? p.1, 1997 – available online in dec. 1997, at http://www.publaw.com/1articles.htm : e-rights may currently include the right to place a literary work : 1 - in an online database retrieval system ; 2 - in whole or in part, on cd-rom (computer disk – read only memory) ; 3 - in whole or in part, on a DVD (digital video disk) ; 4 - on the internet ; 5 - on a website on the world wide web ; and 6 - on an electronic bulletin board services such as america on line, compuserve and prodigy.**

التقاضي[4] والحق في الدخول[5] والحق في ادارة النظم[6]. على أن هذه المحاولة لم تذهب الى أبعد من ذلك، فحين التعرض للالتزامات فرض الاستاذ **Mere** منطق القاعدة الاخلاقية **Ethics** بحيث تعد الواجهة الأخرى للحقوق.

---

[1] **A Bill of Electronic Rights and Ethics, Version 0.23 (1996) Author: Peter Merel, available online in Sep. 2004 at http://www.efa.org.au/Publish/ere.html**

[2] **Rights of Communication**
0.0 The right to accept any information from any source.
0.1 The right of every person to control and license intellectual property invested in their own original expressions, but not in algorithms nor other properties of mathematics.
0.2 The right to transmit any information to any person, as limited only by intellectual property rights.
0.3 The right to publish any information in any unmoderated forum, and to submit any information to any moderated forum, as limited only by intellectual property rights.

[3] **Rights of Privacy**
0.4 The right of every person to refuse to disclose any information they originate or receive.
0.5 The right of every person to encrypt, decrypt or transform in any way any information they originate or receive.
0.6 The right of every person to refuse to disclose the identities of the originators of information they transmit or receive.
0.7 The right to monitor others only with their prior consent.
0.8 The right to ignore information of any nature.

[4] **Rights of Jurisdiction**
0.9 The right of every person to abide only by those laws and regulations that apply at their physical location.
0.10 The right to seek legal recourse against the originators of actions and expressions that cause damages, but not against any intermediary person, organisation or medium.

[5] **Rights of Access**
0.11 The right of access to any information in the public domain, restricted only by cost.
0.12 The right of every person to access any report, record, policy, regulation or law that may apply to them, or which has been created in whole or in part by their representatives or their agents, as limited only by the Rights of Privacy.

[6] **Rights of Administration**
0.13 The right, as moderator of a moderated forum, to observe and enforce the charter of that forum.

على أن أهم محاولة في اطار الكشف عن الحقوق والحريات والالتزامات الالكترونية هي تلك التي قام برصدها الأستاذ الألماني **Herburt Burkert** (أستاذ قانون الاتصالات بجامعة سانت جالن بسويسرا) تضمنه بحثه المقدم الى مؤتمر روما **(8 / 9 – 5 – 1998)** حول تأمين حماية الشخصية **Il garante per la protezione dei dati personali**[1]. لقد قام هذا التصنيف على أساس التمييز بين الحقوق الاتصالية الشاملة وتلك الاستثنائية ويقابل هذه وتلك التزامات في شكل مسئوليات **Responsabilities**. وفيما يلي ملخص لتصنيف الاستاذ **Herburt Burkert**.

أولا : شمولية الحق في الاتصال **Rights to communicational inclusion** :

وتشمل هذه الحقوق أربعة أنواع هي على التوالي:

1– الحق في الدخول الى وسائل الاتصالات **The right of access to the means of communication**. ولهذا الحق أكثر من مظهر يتمثل في امكانية المشاركة في الأنشطة المتعددة للانترنت من ترفيهية واجتماعية وثقافية، وبالجملة المشاركة في بيئة الاتصالات بالكامل **Total communication environment** ويسمح هذا الحق باستخدام ادوات الدخول الى وسائل الاتصالات بشكل عام. وهذا الحق مستوحى من القيمة الكبيرة البارزة في تعدد وسائل الاتصال واختلافها عبر الانترنت[2].

0.14 The right, as administrator of a system, to deny participation in that system to any person for any reason, as limited by contractual obligations.
0.15 The right, as parent or legal guardian of a minor, to control the information made available to that minor.

[1] (BURKERT) Herbert - Rights & responsibilities presentation at the internet . - conf. on internet & privecy - which rules ? ROMC May 8 1998 . p . 1 - available online in mars 2000 at :
http://www.gmd.de/people/herbert.burkert/rom.htm

[2] Rikke Frank Jørgensen- Internet and Freedom of expression- EUROPEAN MASTER DEGREE IN HUMAN RIGHTS AND DEMOCRATIZATION 2000-2001 RAOUL WALLENBERG INSTITUTE – SAYS ". Internet facilitates bi-directional communication, where users are both speakers and listeners and allows for a variety of different communication

2 – الحق الشخصي الذاتي في الاتصال The right to communicational personality. والفكرة الأولية في هذا الحق الشامل **Inclusion** أنه في بيئة الاتصالات الشاملة فإن الاتصالات التي تجرى إنما هي نسخة مطابقة او أنها صورتنا المنقولة على وجه الدقة **Communicate as a medial replicas of ourselves** فنحن نتعامل تجاريا ونخاطب السلطات المدنية، فنحن نمارس الحقوق المدنية حتى في اتصالاتنا مع الأقرباء والعائلة والأصدقاء. ويعد البريد الالكتروني والتوقيع الالكتروني مثالا هنا على التعامل بأشخاصنا في البيئة الاتصالية. ومثل هذا الحق يعد من الحقوق الشاملة التي لا يجوز مصادرتها **Inalienable** او حذفها من البيئة الاتصالية الكاملة. إن الأثر الشامل للانترنت على مثل هذا الحق هو ضرورة توافق التشريع مع استخدام هذا الحق وبما يتفق أيضا مع البيئة الاتصالية الشاملة فاستخدام التوقيع الالكتروني مثلا إنما هو تطبيق لتعاملاتنا الالكترونية. ويجب أن يفهم التوقيع الالكتروني هنا على أساس يتسع لأبعد من مجرد مقارنته بالتوقيع المادي، فاذا كان الفرد يملك توقيعه باستخدام اليد والقلم او الختم فإنه في البيئة الاتصالية الشاملة يمكن استخدام العين والبصمة و...الخ.

3 – الحق في الدخول الى المعلومات The right of access to information. إن البيئة الاتصالية الشاملة ليست غاية في ذاتها وإنما لها غرض وغاية تتمثل في امكانية الحصول على المعلومات المبتغاة، ومن ثم فهي وسيلة او أداة تواصلية بين الشبكات دون اعتبار للحدود الدولية[1].

---

methods. The most common functions can be grouped into six categories (Ibid:7-11, modified).

- **One-to-one communication (such as e-mail or chat)**
- **One-to-many communication (such as listserv or chat)**
- **Many-to-many communication (such as newsgroups or chat)**
- **Real time remote computer utilization (such as telnet)**
- **Information retrieval (such as ftp, gopher and world wide web)**
- **Publishing information (world wide web)".**

[1] Rikke Frank Jørgensen- op cit, SAYS "And Internet does bear promising features for strengthening pluralism and empowering civil society. Here are a few practical examples to illustrate:

- **Easier to get your message out: Through e-mail and websites, human rights organisations in Egypt and the Palestinian territories can disseminate**

information more effectively than before, despite modest resources and limited access to local media (HRW 1999:17).

- New means for suppressed media: When Radio B92 in Belgrade was closed by the authorities, the station put its programming on the Internet using a Dutch Service Provider. Radio Free Europe, Voice of America and Deutche Welle picked up the station and broadcasted it back into Serbia. In response to this, the government allowed the station back on the air (GILC 1998:C).
- Easier to "meet and discuss": Citizens of Arab countries have been able to debate with Israelis in chat rooms at a time when it was difficult for them to have face-to-face contact, telephone conversations, and postal correspondence, due to travel restrictions and the absence of phone or mail links between many Arab countries and Israel (HRW 1999:18).
- Harder for governments to censor information: The China News Digest (www.cnd.org) makes available news from non-official sources. While the Chinese government sometimes blocks the site, users in China have found ways to access it (GILC 1998:B).
- Easier to find information, for instance from a specific minority group: An Arab Gay and Lesbian website (www.glas.org) caters to people who, in many Arab countries, have few places to obtain information pertaining to their sexual orientation (HRW 1999:19).
- Easier access to public information, for instance new laws, decision making and so on: Through the European Unions website (europa.eu.int) the public can gain access to all EU publications in several languages.
- Easier access to global information: For Indian children in the Chiapas region in Mexico, a few computers with Internet access have meant access to a "global library" of information.
- Mobilising civil society: The McSpotlight site (www.mcspotlight.org) is created to provide information on the "McLibel" trial, against MacDonald and other multinational corporations. The site is a new way of mobilising consumers worldwide and has received some of the most extensive press coverage ever given to a website (Liberty 1998:263).".

وهذا الحق من طبيعة شاملة يتوافق مع فكرة حرية التجول المعلوماتي التي قررها المشرع المقارن مثلما هو الشأن في التشريع الفرنسي (القانون رقم **19 / 1978**) الذي تنص المادة الاولى منه في صدرها على الحرية المعلوماتية وامكانية اتاحة المعلومات لكل مواطن(!)، وإن كان المشرع الفرنسي يضيق من هذا الحق لكي يشمله باملواطنة فقط وهو في هذا يتعارض مع مدلول الحق بربطه بالجنسية. لذلك فإن مصطلح الدخول **Access** سوف يكتسب مضمونه تعريفا موسعا، إذ سوف يشمل المضمون المعلوماتي المقنع لطالب المعلومة.

4 – الحق في المشاركة الاتصالية The right to communicational participation.

إن حقوق المعلوماتية في البيئة الاتصالية الشاملة يجب أن يقودنا الى حقوق المشاركة فيها[1]، ثم إن هذه الحقوق بما تتضمنه من معلومات واتصالات ومشاركة ينبغي أن تندمج في مفهوم حقوق المواطنة. فالحق في المشاركة الاتصالية يتطلب تأقلم تقنية ادوات المشاركة مع الزمن المعاصر، ولقد بدأت المحاولات الفقهية العربية منذ القدم في فهم آلية التعامل بوسائل الاتصالات الحديثة كما هو الشأن في التعاقد بالمراسلة البريدية والتلغرافية والتليفونية الذي أتخذ منطقه الوظيفي منذ بداية القرن العشرين فقد تفاعل فقه القانون العربي مع هذه الآلية[2].

---

[1] **Rikke Frank Jørgensen- op cit- SAYS "Easier to "meet and discuss": Citizens of Arab countries have been able to debate with Israelis in chat rooms at a time when it was difficult for them to have face-to-face contact, telephone conversations, and postal correspondence, due to travel restrictions and the absence of phone or mail links between many Arab countries and Israel (HRW 1999:18)."!**

[2] **انظر بحث المرحوم الاستاذ سامي أفندي الجريندينى – التعاقد بالمراسلة – مجلة المحامي– نقابة محامي مصر السنة الأولى – 1920. حيث يقول " ثم إنه ليس من المعقول أن يضع القانون حواجز منيعة في سبيل حرية التعاقد فيحدد ويحرم التعاقد بالمكاتبة أو يقلل اعتبارها، كلا بل الأمر بالعكس فإنه يجب تفسير روح التقنين تفسيرًا موافقًا لحرية التجارة وتنشيطها وملاحظة السرعة في التعاقد بالمراسلة تارة وبالتلغراف أخرى وكل هذه أمور لا يمكن أن يتوفر معها شرط وجود صورتين متماثلتين مع كل من المتعاقدين حتى يصح أن يكون عقدًا عرفيًا، وما دام القانون يجيز البيع الشفاهي مثلاً يجوز من باب أولى البيع بالمراسلة. ولا يخفى أن مبدأ القانون التجاري ومبدأ القانون المدني واحد وكل ما في الأمر أن قانون التجارة أوضح بيانًا فيما يخص التعاقد بالكتابة فهو يعتبر مكاتبات التجار رابطة بينهم ويفرض فرضًا محتمًا وجوب أخذ صورة (كوبيا) من كل مراسلة تصدر وما ذلك إلا لجعلها دليلاً من أدلة الإثبات عند مضاهاتها على المراسلات التي ترد فلا نزاع إذًا في أنه يجوز للناس أن يتعاقدوا بالمراسلة كيفما شاؤوا، ولكن هل يجوز ذلك في كل العقود، فإننا إذا قررنا أن المراسلات المتبادلة بين المتعاقدين تحتوي على إيجاب وقبول الفريقين فيجب القول بأن كل عقد يشترط الإيجاب والقبول فقط لصحته كان صحيحًا فيخرج من ذلك العقود الرسمية**

إن الحق في المشاركة الاتصالية يحتاج الى بنية أساسية ترتبط بأهمية الاستمرار في المحافظة على الخدمات العالمية للاتصالات بما يفيد ضرورة تقليص دور الوسيط في تلك البنية الاساسية من الناحية المادية محاولة استظهار العلاقة القانونية بذلك الوسيط، وهي علاقة حتى الآن تصب في مصلحة الوسيط فقط والذي يكاد يصبح المهيمن على الأمور خاصة من حيث بث رؤية امكانية رضاه بافشاء البيانات والمعلومات وبما يعني سيطرته على مسألة الحق في الخصوصية في العالم الرقمي.

ثانيا : الحقوق الاتصالية الاستثنائية / حرية الاختيار **The right to communicational exclusion** إن الفكرة الأساسية التي تنطلق منها الحقوق الاتصالية الاستثنائية هي أن الاتصالات ليست من طبيعة اساسية وانما من طبيعة اختيارية. وترتكز نقطة الاختيار هذه على مبدأ حر، أي حرية الاختيار. لذلك تنتفي فكرة الجبر في مسلمات هذه الحقوق. كما تكمن الفكرة الاستثنائية في هذه الحقوق في كونها تعد خروجا عن الغرض من الاتصالات التي تمثل المشاركة **Inclusion** القاعدة العامة فيها.

وتتكون جملة الحقوق الاختيارية فيما يلي:

1 – الحق في الخصوصية **The right to privacy** . ويتضمن هذا الحق مفهوم امكانية البقاء في عزلة بعيدا عن المشاركة مع الغير ، وهو استثناء يجد بقاءه واستمراريته في المثال الواقعي الذي يتكامل برفض التعامل مع المؤسسات التي يتطلب الدخول الى شبكاتها دفع مبالغ مالية. مثل هذه الشبكات إذا لم تتكامل مقومات الدخول اليها فانها تستمر على خصوصيتها.

2 – الحق في الاستعارة **The right to anonymity**. إن الفكرة الأساسية في هذا الحق تنطلق من انه من الصعوبة بمكان – او تجاوزا يعد من المستحيل – فرض قيود رقابية على حركة المعلومات واستخداماتها في البيئة الاتصالية الشاملة، لذا فانه، ووفقا لهذا الحق، فان الضن بالمعلومات الشخصية او اخفاءها يجب قبوله كقاعدة عامة – سيما وإن الشمولية التي عليها الحال في تلك البيئة وحالة التغيير المستمر فيها لا يحتاج فيها الى المعلومات الشخصية . وعليه فإن

فإنها لا يكفي فيها الإيجاب والقبول بل لا بد من وساطة موظف مختص ليكون العقد تامًا صحيحًا، فلا يجوز الرهن العقاري التأميني بالكتابة لأن القانون يقضي أن يكون هذا العقد رسميًا ومثله الهبة.".

شرط موضوع اخفاء الشخصية **Anonymity** واستخدام اسم مستعار **Pseudonym** من الأمور التي يمكن إباحتها بحيث تستبعد كل الشروط المسبقة التي تتعارض مع هذا الاتجاه.

3 – الحق في عدم الظهور **The right to non-availability** . إن هذا الحق يعد احد أهم آثار البيئة الاتصالية الشاملة التي تشبع رغباتنا الانسانية، ذلك انه يبرز أهمية حضورنا ومدى قابلية ظهورنا. في البيئة المذكورة إما أن نكون ظاهرين وإما أن نمتنع عن الظهور (نختفي) دون أدنى تأثير للضغط الاجتماعي كما هو الشأن في البيئة العادية، بل يمكن ايضا عدم الظهور دون أن يكون لذلك عقاب ما. وإن أكثر بروز لهذا الحق حال التعامل الالكتروني من خلال مواقع ليس لها وجود في الواقع المادي وإنما لها وجود في الواقع الالكتروني، وهذه مسألة اثيرت لدى الفقه فنحى جانب منه منحى عدم شرعية تلك المواقع الالكترونية.

4 – حق المستخدم في تقوية موقفه **The right to user empowerment** . ويعني هذا الحق إنه في البيئة الاتصالية الشاملة يمنح الحق للمستخدم في اخراج ذاته عن مضمون المعلومات المتوافرة. إذ مع التنوع الحضاري والثقافي تتصاعد المخاطر، وفي ذات الوقت ازاء أهمية المعلومات فإن الخيار الوحيد باغلاق الجهاز لم يعد خيارا بسيطا. فما نحن بحاجة اليه إنما هو التدريب والقابلية للتطوير على خيارات آلية دفاعية، على سبيل المثال ففي حالة الفلترة او التصفية (التنقية) **filters** فإن مثل هذه المصافي تساعد على حماية الذات ضد العدوان على البريد الالكتروني، وبفضل التأثير الاحتمالي لمثل تلك المصافي أمكن البقاء في اطار الشرعية في ظل حرية الاختيار.

وقبل التطرق الى موضوع الالتزامات او المسئوليات بحسب تصنيف الاستاذ بوركيرت فإنه تجدر الإشارة الى أن عرضه لهذه الحقوق هو عرض متلازم فهذه الحقوق هي حقوق متلازمة ومتلاحقة فلا يمكن استخدام حق دون آخر بل إن استخدام أحد هذه الحقوق يجعل الاخرى او جميعها مستخدمة تلقائيا من قبل المستخدم.

ثالثا : المسئوليات والالتزامات **Responsibility** : وهي كما عددها الاستاذ بوركيرت على النحو التالي:

أ – الالتزامات مرآة الحقوق **Responsibilities as mirror images of rights** . إذا كان الحق يقابله – كقاعدة – التزام في القانون فإن الإخلال بهذا لالتزام يرتب المسئولية ، لذلك كثيرا ما يعبر عن الإخلال بالالتزام بالمسئولية وذلك من منطلق إن الالتزام او المسئوليات إنما هي مرآة الحقوق ككل . فإذا أخذنا في الاعتبار قاعدتي الحقوق المشار اليها فيما سلف في البيئة الاتصالية الشاملة فاننا نكون ازاء خاصية عامة يمتد نطاقها الى الدولة وفي ذات الوقت ذات صلة وثيقة بالعلاقة بين المواطن والدولة **Citizen – state relationship** فتتقابل أفقيا الحقوق والالتزامات بحيث تتولى الدولة التفعيل القانوني للالتزامات و المسئوليات وهو الأمر الذي يترتب عليه تفعيل الحقوق وهذا تحد ضخم لمؤسسات الدولة.

ب – التزامات ومسئوليات جديدة **New responsibility** . إن خلق انعكاس للحقوق ويتمثل ذلك في الحريات يترتب عليه ان تتصاعد الى سماء النظم القانونية المعاصرة التزامات ومسئوليات جديدة تتجه الى موقع الصدارة في مجتمعاتنا المعلوماتية، وهى تتجه في صعودها هذا الى ثلاثة مستويات على النحو التالي:

1 – مستوى المسئوليات الصغرى **Micro level responsibilities**. وفي هذا المستوى يؤخذ في الاعتبار دور الفرد، اذ ما هو في تصاعد هنا هو مسئوليته الاتصالية **communicational responsibilities**، مثل مسئولية الصحف التي تطالب بشدة بكل الاخبار القابلة للطباعة. كذلك بتمكين الفرد في المشاركة بمبدأ الواحد للكل – **ONE –TO – ALL**.

2 – مستوى المسئوليات المتوسطة **Mezzo level responsibilities**. ما يتناوله هذا المستوى من المسئوليات هو مدى اخلال الوسيط او المجهز **Provider** بالتزاماته المرتبة لمسئولياته. والواقع أن مسئولية الوسيط هنا ليست من المسئوليات الجديدة وإن كان هناك إجماع أوروبي على ذلك. ولقد لاقى موضوع مسئولية اخلال الوسيط بالتزاماته الاهتمام الكامل ازاء الشك في القدرة على تطوير الانترنت بالاضافة الى ان الوسيط يعد الهدف المتحرك الذي يمكن تحميله المسئولية كذلك، سيما وأن الفاعل – مثالا – قد لا يمكن التعرف عليه كما أنه إذا تم التعرف عليه فإنه ليس من السهولة أن تصل إليه يد العدالة. ولقد لاقى هذا المستوى قبولا كحل ضروري وسريع في مؤتمر بون الدولي **BONN international ministerial conference** المنعقد في

يوليو **1997**. ولقد تأثر بهذا الاتجاه قانون الوسائط المتعددة الالماني **The German multimedia law** وكذلك تقنيين التنظيم الآلي لخدمات الانترنت في ايطاليا **Codice al autoregolamentazione per i serviczi internet**، ولقد تقرر في المؤتمر المذكور:

- ما هو محظور خارج الانترنت هو كذلك عبرها.
- إقرار مسئولية الوسطاء حال الدخول الى الانترنت عبر الاتصال بهم لوجودهم في حالة أدارك إيجابي **positive knowledge** وكذلك حال عدم اتخاذهم موقف ايجابي تجاه العمل غير المشروع مع إمكان قيامهم به.

3 – مستوى المسئوليات الكبرى **Macro level responsibilities**. وفي رأي الاستاذ بوركيرت أن أقوى أنواع المسئوليات هي تلك القابعة في المستوى العالي، ليس فقط بالنسبة للدولة ولكن بالنسبة لكل ذي شأن في قاعدة صناعة التقدم **Rule making progress**، وهي المسئولية الكافية التي تواجه تحدي الجزع **ANXITY**. فهي ليست فقط ذلك التغيير الذي يحدث الجزع. فالقلق او الجزع في البيئة الاتصالية الشاملة هو جزع من نوع متميز يحمل في مضمونه تحدي الاتصالات لقيمنا ومعتقداتنا وأصالتنا وشخصيتنا. لذلك فإن أهم فريضة ينبغي علينا دراستها وتعلمها في البيئة الاتصالية الكاملة هي القدرة على تعزيز تحدي الاتصالات وذلك لحماية التحدي في شخصيتنا الانسانية.

تلك كانت رؤية الاستاذ "هيربرت بوركيرت" في تصنيف الحقوق والحريات والالتزامات الرقمية، وهي محاولة ذات تأثير كبير حتى الآن في الوسط القانوني الاروبي باعتبارها أولى المحاولات التي اعترفت بالبيئة الشاملة او الكاملة للانترنت. ولقد لقيت محاولته هذه نجاحا نسبيا، لاسيما من الزاوية الجدلية، حيث إنها رؤيا تتجاوب مع التحول الحادث في الفترة المعاصرة، من العصر الصناعي الى عصر المعلوماتية والاتصالات، ومن ثم يتناول الحديث حقوقا تجري في هذا الإطار، وقد يكون مناسبا القول بأن بعض أنواع الحقوق التي نشأت في فترات سابقة لم تعد مقبولة في هذا العصر على الرغم من أن فكرة الحقوق لا زالت في تصنيفاتها المعاصرة تصارع من اجل كينونتها ووجودها. ولكن المشكلة التي تقابل كل محاولة لتصنيف الحقوق والالتزامات والحريات هي لزوم استمداد تفسير قبولها من الشريعة الكبرى في الدولة او حتى المجتمع المعلوماتي ودون ذلك يكون من

الصعوبة بمكان البحث في منطق تصنيف لها، إذ يظل مثل هذا التصنيف مصاحبا لواقع عملي تحديدا ليس له أساس من النظرية[1].

وفيما يلي نعرض لبعض أنواع الحقوق التي صادفت مشكلات في إطار الانترنت.

– الحق في الخصوصية: فإذا تأملنا الإطار العام للحماية المدنية فإن الحق في الخصوصية يقف على قمة الهرم هنا ، إذ يقف التشريع المقارن بالمرصاد لكل محاولة للعدوان على هذا الحق عبر الانترنت . ففي الولايات المتحدة الأمريكية وقف قانون خصوصية الاتصالات الالكترونية **1986** **The e - communications privacy act** بالمرصاد لادارة البحرية الأمريكية في قضية **Timothy R. McVeigh** وتتمثل وقائع هذه القضية في أن المدعو **McVeigh** كان عضوا بالبحرية الأمريكية وبدأت أزمته **Ordeal** عندما قام بارسال رسالة الكترونية عابثة الى متطوع بالبحرية عبر بريده الالكتروني من خلال شركة **AOL** وقد اتخذ لنفسه اسم **BOYSRCH** معرفا اسمه **TIM** ومهنته العسكرية وحالته الاجتماعية لوطي **GAY** ، فما كان من المتطوع سوى ان ابلغ ادارة البحرية بهذه المعلومات التي شرعت في التحقيق عبر شركة **AOL** فقامت الشركة المذكورة باعلان الاسم الحقيقي لـ .. **McVeigh** بشكل ودي واتخذت ادارة البحرية الاجراءات الادارية لاقالة **McVeigh** إلا أن المحكمة الابتدائية لكولومبيا قضت بالغاء تلك الاجراءات الادارية واعادة **McVeigh** الى سابق عمله لما في تلك الاجراءات من مخالفة لقانون خصوصية الاتصالات الالكترونية **1986** الذي يحظر على الحكومة الفيدرالية الحصول على معلومات عن

---

[1] أنظر طعن دستوري مصري رقم 106 لسنة 19 ق. جلسة 1 / 1 / 2000 (المحامي – مصر ع. 1 لسنة 2001 ص. 291) حيث جاء في هذا الطعن " إنه من المقرر إن السلطة التي يملكها المشرّع في مجال تنظيم الحقوق، حدها قواعد الدستور التي تبين تخوم الدائرة التي لا يجوز اقتحامها، وبما ينال من الحق محل الحماية او يؤثر في محتواه ، ذلك إن لكل حق دائرة يعمل فيها و لا يتنفس الا من خلالها ، فلا يجوز تنظيمه إلا فيما وراء حدودها الخارجية ، فإذا اقتحمها المشرّع كان ذلك أدعى الى مصادرة الحق او تقييده ". كما قضت ذات المحكمة في الطعن الدستوري رقم 163 لسنة 20 ق. جلسة 5 / 8 / 2000 (السابق ص. 367) بأنه "وحيث إن الأصل في سلطة المشرّع في موضوع تنظيم الحقوق ، أنها سلطة تقديرية ما لم يقيد الدستور ممارستها بضوابط تحد من انطلاقها ، وتعتبر تخوما لها لا يجوز اقتحامها او تخطيها. وكان الدستور إذ يعهد الى أي من السلطتين التشريعية والتنفيذية بتنظيم موضوع معين، فإن القواعد القانونية التي تصدر عن أيتهما في هذا النطاق لا يجوز أن تنال من الحقوق التي كفل الدستور أصلها سواء بنقضها او انتقاصها عن أطرافها ، وإلا كان ذلك عدوانا على مجالاتها الحيوية من خلال إهدارها او تهميشها".

مستخدمي الانترنت إلا إذا : – (أ) حصلت على امر تفتيش **Warrant** وفقا لقانون الإجـراءات الجنائية الفيدرالي **Federal rules of criminal procedure** او قانون معادل له ، او (ب) حصولها على مذكرة أولية للوسيط **Online subscriber** ثم بعد ذلك تلجأ للقضاء والحصول على أذن للكشف على المعلومات محل التساؤل[1].

واذا تأملنا المسألة من أبعاد أخرى فإننا نجد أن التفسيرات الفقهية والقضائية لقانون تخزين الاتصالات **The Stored Communications Act** الفيدرالي الأمريكي أبعاده في الاختلاف بين خدمة الاتصالات الالكترونية **Electronic Communications Services ECS** وبين خدمة الاتصال عن بعد **Remote Communications Services RCS** .

وفـي فرنسـا تعـد قضـية **Gubler** (ينـاير **1996**) مـن القضـايا الشـهيرة فـي اطـار الحـق فـي الخصوصية، ولقد أدان القضاء الفرنسي العدوان على الحياة الخاصة لعائلة الرئيس الفرنسي السابق فرنسوا ميتران لقيام طبيبـه الخـاص الـدكتور **Gubler** مـع الصـحفي **Gonod** بنشـر مذكراتـه كشف فيها عن أسرار مرض الرئيس السابق، ولقد تمت مصادرة الكتاب إلا أن مالك مقهى انترنت في مدينة **BESANCON** نشر تلك المذكرات على الانترنت دون موافقة من عائلة الرئيس السابق فلحقته الادانة القضائية وتم اغلاق المنشأة ومصادرة موقع الانترنت المذكور إلا إن النشر كان قد تم.

علـى أن الغريـب فـي اطـار الحـق فـي الخصوصـية إن دولا عديـدة لـم تكـن تعتـرف بـه مثـل القـانون الانجليزي، ولدى الفقه الانجليزي إن مصطلح الخصوصية **Privacy** ليس مصطلحا قانونيا بل وغير معروف أيضا كقيمة انسانية **Human value** حتى إنه في قضية **Prince Albert v. Strange** (عام **1849**) تم إقرار مصطلح الشخصية المحصنة **Invidate personality** حين تنـاول موضوع حق المـدعي **Plaintiff** فـي الملكيـة. ويمكن القول اجمـالا إنـه فـي القـانون الانجليزي وباستثناء قانون البث لسنة **1990** **The Broadcasting act** الذي حل محله القانون الصادر في عام **1996** فإنه فليس هناك مكان لمصطلح الحق في الخصوصية.

[1] **Eric J. Sinrod – Barak D.Jolish, controlling chaos: the emerging law of privecy and speech in cyberspace, op-cit p. 5.**

– حقوق الملكية الفكرية: ظلت حقوق الملكية الفكرية الشغل الشاغل للمشرع المقارن وعلى المستويين الدولي والمحلي وإن كان الوضع الدولي لها قد أخذ المجرى الطبيعي للحماية لاسبقيته على التشريع المحلي ، فمنذ اتفاقية برن لحماية الأعمال الفكرية في **9 / 9 / 1866** وموضوع امتداد هذه الحماية الى الحقوق الالكترونية يصنف على أساس أهمية الموضوع. وقلد حسمت اتفاقية الجات/التريبس عام **1994** هذا الموضوع تماما كأول اتفاقية دولية تقوم بفرض التزام على الدول كافة في ضرورة شمول منتجات الحوسبة والرقمية بحقوق الملكية الفكرية، ومن ذلك مثلا برامج برمجيات الحاسوب وقواعد البيانات (انظر المادة **10** والملحق الأول / ثالثا).

ومن الدول – في التشريع المقارن – ما يجعل هذا الموضوع – لأهميته في المحافظة على التطور العلمي – يرقى الى مستوى الحقوق الدستورية[1]. فالمادة **8/1** من الدستور الأمريكي تنص على أنه: –

"To promote the progress of science and useful arts, by securing for limited times to authors & inventors the exclusive right in their respective writings & discoveries".

ويعد قانون النسخ الأمريكي لسنة **The Copyright act 1976** من التشريعات التي اخذت في الاعتبار موضوع التقنية الحديثة للاتصالات. فقد توقع الكونجرس في عام اصداره كل التغيرات التي سوف تحدثها التكنولوجيا وكحد ادنى أخذ في الاعتبار المستجدات التكنولوجية والاعلام ولقد تضمن النص في القسم **(C /201)** التعامل مع الاعمال الجماعية **Collective works** بحيث لم يضع اية قيود على الاعلام والنشر **Media** وهو ما جعل المحاكم الأمريكية ترى في هذا النص امكانية واسعة للانطباق على قواعد البيانات عبر الانترنت وكذلك الاقراص المضغوطة[2]. الا أن التفعيل الأكثر حدة لحقوق الملكية الفكرية الرقمية كان بعد ظهور تشريع **Digital Millennium Copyright Act DMCA** في عام **1998** ومعه تشريع منع العدوان الالكتروني **The Non – E Theft Act** .

ولقد ترتب على دخول حقوق الملكية الفكرية في دائرة الحقوق الرقمية أن اتسعت دائرة عقود التأليف والنشر لتشمل حقوقا جديدة مثلما هو الحال في شرط منح الحقوق **The grant right clause**

---

[1] **Losey R.C – Practical & legal protection of computer database p. 2. available online in march 2000 at http://www.uplink.com.au/lawlibrary/document/docs/doc32.htm**

[2] **Lloyd Rich – op-cit at 3.**

وشرط مستقبل التكنولوجيا **The future technology clause** وبمقتضاها يمنح المؤلف الناشر الحق في التداول الالكتروني لمؤلفه[1].

ففي قضية **Tasini V. NewyorkTimes Co.** عرض على المحكمة الفيدرالية سؤالا مقتضاه هل يجوز للناشر القيام بالتداول الالكتروني لاعمال الصحفيين المستقلين **Freelance** كوضعها على الانترنت او في اسطوانات مضغوطة **CD-ROM**؟

كان القضاء الأمريكي قبل هذه القضية يعتبر وضع المقالات والمؤلفات عبر الانترنت او على أقراص مضغوطة نوعا من الحفظ لها **Archiving the articles** ولكن بعد هذه القضية أخذ القضاء اتجاها جديدا: فقد ذهب القضاء الى إن الناشرين لا يكونون منتهكين لحقوق النسخ إذا أعادوا نشر مقالات الصحافيين المستقلين عبر الانترنت حتى على الرغم من إن هؤلاء الصحفيين لم يمنحوا الناشرين حقوقا الكترونية، ولا يكون من حق الصحفيين منع الناشرين من القيام بهذا العمل وانما يكون لهم الحق في مقابل مالي فقط. ولقد برر القضاء الأمريكي هذا الحكم بإن إعادة نشر مثل هذه المقالات الكترونيا انما هو ممارسة لحق قانوني للناشرين في المراجعة الشاملة لمجموعة الاعمال **Collective works** التي قاموا بنشرها[2] في الوقت الذي لا يجوز فيه حجب حقوق هؤلاء الصحفيين. ولقد كان أهم مرتكزات هذا الحكم هو ما قرره قانون النسخ الأمريكي في القسم **(201 / D – 1)** من "أن مالك حقوق النسخ يجوز له نقل ملكيتها كليا او جزئيا وبأي شكل من أشكال نقل الملكية او بطريق عملي قانوني"[3]. كذلك ما قرره القسم **(201 / D – 2)** من أن "أيا من حقوق النسخ ، بما في ذلك تسويات حقوق النسخ، بما في ذلك تقسيم أي من هذه الحقوق ... يمكن

---

[1] **Lloyd L.Rich, Legal articles, op-cit at 1.**

[2] **Id at 2.**

هذا ولقد عرفت المادة (27) م قانون القانون رقم 9 لسنة 1968 بشأن حماية حق المؤلف في ليبيا (ج . ر . ع 10. في 30 / 3 / 1968) المصنف الجماعي بأنه " المصنف الجماعي هو المصنف الذي يشترك في وضعه جماعة بتوجيه شخص طبيعي او اعتباري يتكفل بنشره تحت ادارته ويندمج عمل المشتركين فيه في الهدف العام الذي قصد اليه هذا الشخص الطبيعي او المعنوي بحيث لا يمكن فصل عمل كل من المشتركين وتمييزه على حده. ويعتبر الشخص الطبيعي او الاعتباري الذي وجه الى ابتكار هذا المصنف ونظمه مؤلفا ويكون له وحده الحق في مباشرة حقوق المؤلف " . (موسوعة التشريعات العربية – محمد ابوبكر بن يونس – ليبيا ، ملكية فكرية) .

[3] **"The ownership of a copyright may be transferred in whole or in part by any means of conveyance or by operation of law "**

نقلها ... ويمكن أن تكون محلا لملكية منفصلة عن بعضها البعض"[1] حيث يعد من قبل الحقوق المطلقة للناشرين **Exclusive rights** والذي قررته المحكمة حق العرض **Display right** دون حاجة الى موافقة مسبقة من قبل المؤلف، إذ إن حق العرض التكنولوجي ليس منفصلا عن العرض العادي وذلك وفقا لما هو مقرر في قانون النسخ[2].

وفي فرنسا قضت المحكمة الابتدائية العليا / باريس في **14 / 8 / 1996** بعدم جواز وضع أغنية على صفحة طالبين دون الحصول على موافقة مسبقة على ذلك من قبل مالكي الأغنية (قضية **BREL ET SARDOU**)[3].

وفي إطار النشر الصحفي فقد قررت المحكمة الابتدائية/باريس في **1999/4/14** (في قضية جريدة الفيجارو **LE FIGARO**) أن النشر الجماعي **Une oeuvre collective** من حق الجريدة. على أنه لا يمتد هذا الحق الى النشر الفردي عبر الانترنت مميزة بذلك العمل الجماعي وبين النشر الفردي الذي يستلزم الحصول على الموافقة المسبقة من الصحفي. ولقد أيدت محكمة استئناف باريس هذا الحكم في حكمها الصادر بتاريخ **10 / 5 / 2000** مقررة لزوم الحصول على موافقة الصحفي حال وجود نشر فردي عبر الانترنت كما لو كان النشر عبر شبكة **Minitel**[4] . وان كانت المحكمة قد جانبها الصواب في تشبيه الانترنت بالميناتل لكون الأخير شبكة خاصة بفرنسا فقط وتعمل بنظام الخطوط المغلقة وليست كالانترنت مفتوحة وتتصف بالعالمية[5].

وفي مصر وضع المشرع تعديلين للقانون رقم **35** لسنة **1954** بشأن حقوق المؤلف (القانون رقم **38** لسنة **1992** والقانون رقم **29** لسنة **1994**) فالقانون المصري في تعديل **1992** اضاف برمجيات الحاسوب لتأخذ حظها من الحماية متجها في ذلك الاتجاه التقني الانساني ومتخذا سلوك المعلوماتية كهدف انساني. على أن الامر كان متعلقا ببرمجيات الحاسوب آنذاك ولم يكن يقصد الانترنت وسوف تبرز المفارقة بين الاثنين حال تعرضنا لجرائم العدوان على الملكية الفكرية

---

[1] " Any of exclusive right, compromised in a copyright, including any subdivision of any rights … may be transferred … and owned separatly".

[2] Rich op –cit at 3

[3] Available on line in mars 2000 at http://www.juriscom.net/dauteur.htm

[4] Available on line in mars 2000 at http://www.legalis.net/jnet/2000/actualite_os-2000.htm

[5] J. Heut, la commerce electronic, op-cit at 4.

فيما بعد وما يهمنا هنا أن المشرع المصري أصدر القانون رقم **82** لسنة **2002** بشأن حماية الملكية الفكرية والقانون رقم **10** لسنة **2003** بشأن تنظيم الاتصالات في محاولة أولية لتطوير آليات التعامل مع الانترنت والمجتمع المعلوماتي ككل.

ولا ينطبق ذات الأمر على التشريع الليبي الذي تحوي موسوعته التشريعية تشريعا قديما هو القانون رقم **9** لسنة **1968** بشأن حماية حق المؤلف الذي لم يتطرق الى فكرة المصنفات الرقمية على الاطلاق حتى الآن. على أن قانون الاستثمار الليبي رقم **5** لسنة **1997** المعدل بالقانون رقم **7** لسنة **2003** تضمن حيثيات تشير الى امكانية تطوير التعامل مع موضوعات في إطار نظام الملكية الفكرية بصورة حديثة مثل العلامة التجارية وبراءات الاختراع والتراخيص ولكن مع ذلك لم يتم ربطها بالرقمية مباشرة.

والحقيقة التي لا مناص من الاعتراف بها هي أن النظام الدولي للنسخ وحقوق المؤلف هو الآن محل مراجعة شاملة وجادة من قبل الأنظمة الوطنية في جميع أنحاء العالم، والسبب الحقيقي وراء هذه المراجعة الشاملة هو قوة الحقوق والحريات والالتزامات الرقمية التي تبشرنا بها ثورة تكنولوجيا المعلومات، حتى أنه يصح القول إن علماء تكنولوجيا المعلومات قادوا التغيير العالمي الحادث الآن. ولذلك فإن الدعوة من قبل رجال القانون ملحة الى النهوض ومجاراة الحضارة في تناولها للموضوعات الانسانية وفي هذا الإطار فإن الدول تحتاج الى الإجابة على السؤال التالي: كيف يمكن تأمين أعمال الفنانين والكتاب والناشرين والموسوعيين وشركات التسجيل ومبرمجي الحاسوب والانترنت من انتهاك أعمالهم في كل مكان، وليس في بلدانهم فقط؟[1]

ومثل هذا التساؤل يشمل أيضا الموقف المعاصر الممثل في الاتفاقيات الجديدة التي دخلت الى حيز النفاذ مع بداية العام **2001** في العديد من بلدان العالم كبرنامج دولي لحماية حقوق الملكية الفكرية وهي كل من اتفاقية العرض واتفاقية حقوق المؤلف.

– مسألة حرية التعبير: تعد حرية التعبير من الموضوعات التي أحتوتها التشريعات الانسانية الكبرى مثل الاعلان العالمي لحقوق الانسان والميثاق الدولي للحقوق المدنية والسياسية واتفاقية الحقوق

[1] **Harry Jarvlepp, An introduction to the law of the internet , part 1, op-cit at 2**

والحريات الامريكية والميثاق الأفريقي لحقوق الانسان والشعوب والاتفاقية الاوروبية لحماية حقوق الانسان وحرياته الأساسية، بالإضافة الى العديد من المواثيق والدساتير الاقليمية.

لكي يمكن تحديد العلاقة بين حرية التعبير ومجتمع المعلومات فإنه يجب تحديد نقطة الانطلاق الأولى التي يبدأ منها البحث، وتتعلق بتحديد او تعريف المعلومة التي تصلح أن تكون مشمولة بحماية القاعدة الدستورية العالمية لحرية التعبير[1].

إن مسألة حرية التعبير التي تصارع في العالم المادي لا يمكن أن تتنقل بذات الرؤية الى العالم الرقمي، ففي العالم المادي توجد العديد من القيود عليها، في حين أنه لا توجد قيود مفروضة على حرية التعبير في العالم الرقمي. وهذه النتيجة أخذت طابع الدستورية الكاملة أمام القضاء الأمريكي (الفيدرالي). فقد انتهت كافة قضايا دعارة الأطفال عبر الانترنت امام القضاء الفيدرالي الأمريكي الى لا شيء، حتى من حيث الاختلاف الحضاري بين المشرع (الفيدرالي والولائي وكذلك القضاء الولائي). فالمسألة الاخلاقية عبر الانترنت أضحت من المشكلات الكبيرة ومحلا لصراع كبير بين القيم واللا قيم. وكان آخر موقف مضاد يتخذه القضاء الفيدرالي هو حكم الدائرة التاسعة الفيدرالية في **2** سبتمبر **2004** في قضية **Gourde** [2] التي تناولت مدى أحقية سلطات الضبط والتحقيق في

---

[1] **Rikke Frank Jørgensen- Internet and Freedom of expression- OP CIT "In January 2001 a Danish public library announced that it had made filtering mandatory on its public computers, in order to block access to pornography and other indecent material for both adults and minors. The library announced that pornography is not information according to the library's definition of information and therefore is not protected as such.".**

[2] **USA, v. MICAH J. GOURDE,9 th Cir. App. No. 03-30262, D.C. No. CR-02-06067-FDB September 2, 2004. "We conclude that this case is much more like Weber than Lacy or Hay. As in Weber, the evidence underlying the search warrant at issue here fails to draw the crucial link between Gourde's having some attenuated connection to child pornography and his actually possessing it. As noted above, the evidence presented to the magistrate included only that Gourde (1) affirmatively subscribed to an internet pornography service that advertised "over one thousand pictures of girls ages 12-17!" and displayed several thumbnail images of girls who at least appeared to be "prepubescent" on the subscription page; (2) had unlimited "access to hundreds of images, including historical postings to the site, which could easily [have been] downloaded during his period of membership" and "would have had to have viewed images of naked prepubescent females with a caption that described them as twelve to seventeen-year-old girls"; and (3) failed to unsubscribe to the site for at least two months. The affidavit also provided expert opinion evidence of the proclivities of child pornography collectors and opined that Gourde's affirmative act of subscribing to**

تفتيش حاسوب منزلي لمجرد أن صاحبه على اتصال بمواقع دعارة أطفال، سواء كان هذا الاتصال في صيغة اشتراك **Membership** في تلك المواقع او كان ذلك من قبل الدخول او اطلاع على تلك المواقع، وحتى مع افتراض منطق أن هناك تخزينا في الحاسوب المنزلي او الخاص لصور من تلك المواقع، فهل يعد ذلك أساس لوجود سبب معقول **Probable Cause** لاستصدار أذن تفتيش؟ ولقد رفضت الدائرة التاسعة الاستئنافية هذا القول وقررت أن مجرد الدخول على مواقع دعارة والاشتراك فيها يمكن أن يكون من قبل حرية التعبير ولكن لا يصلح مطلقا لكي يكون أساسا لاستصدار أذن بتفتيش الحاسوب المنزلي او الخاص ولو كان هناك دخول من قبل هذا الحاسوب على مواقع دعارة أطفال.

والحقيقة إنه يجب فهم موقف القضاء الفيدرالي الأمريكي على أساس بحث نقطة البداية لديه، فالقضاء الفيدرالي الأمريكي ينطلق من فكرة أن الانترنت والعالم الرقمي وبالتالي المجتمع المعلوماتي يعد أرضا حرة في الأساس ولا يمكن نقل القيود التي فرضها الانسان على العالم المادي اليه. وهذا الموقف هو غير موقف المشرع الفيدرالي والولائي وكذلك القضاء الولائي حول هذه النقطة.

أن العرض السالف يثبت أن هناك رؤى للفقه حول حقوق الانسان الرقمية وتميزها عن تلك المادية، ومثل هذا الأمر لا يمكن تجنبه لأي سبب من الأسباب، وهو يحتاج الى موقف ورؤيا فقهية من المتخصصين في حقوق الانسان، خاصة في المرحلة لما بعد العام **1991**. وبالتالي يجب الا تمر رؤيا فقهاء القانون المقارن حول هذه النقطة مرور الكرام. وإذا كانت مسألة الصحة والخلاف في رؤيا فقه المعلوماتية حول الحقوق والحريات والالتزامات الرقمية قائمة، فإن القدر المتيقن الذي لا يختلف عليه أحد هو صحة ودقة ونضوج إبراز فقه المعلوماتية هذا للتمييز بين الحقوق المادية وتلك الرقمية.

Lolitagurls.com and failure to unsubscribe provided a sufficient basis to place Gourde in that “.

(2)

مدخل الى

المباديء الكبرى للحكومة الالكترونية

مقدمة:

الحكومة الالكترونية منهج عمل تقني– انساني يؤدي خدمات جليلة للفرد في كافة مجالات الحياة التي يمكن أن تتصل بتكنولوجيا المعلومات. لذلك يرتبط فهم القيم الصحيحة للحكومة الالكترونية بمدى ما يمكن أن تقدمه للانسان الفرد في كل مكان. وأكثر ما تلتزم به الحكومة الالكترونية كمنهج هو ارتباطها بهدم سلبيات العمل الاداري وبذلك فهي تضع الفلسفة الفردية الاجتماعية في صيغة جديدة قابلة للنقاش والجدل واحياء معالم الانسانية المهدرة التي كانت محلا لوعود واهتمام كافة المواثيق الدولية والمحلية. فالفرد حول العالم في الفترة المعاصرة يتلقى صدمات متتالية تعبر عن مدى الفوارق الكيفية والكمية بين الامم. وهو بحاجة الى قيمه الضائعة التي فقدها أثناء مرحلة الاندماج في عقيدة الدولة التي وصلت معالمها في بعض الدول الى اهدار تلك القيم.

وفي هذه الورقة سوف نعرض للمباديء الكبرى للحكومة الالكترونية. وسوف نتطرق الى هذا الموضوع في صيغة ورقة عمل وصولا الى العرض العام الأولي لتلك المباديء مستهدفا بذلك طرح الفكرة لفقه القانون والسياسة وعلم الاجتماع...الخ. فإرساء مباديء كبرى للحكومة الالكترونية يعني في الحقيقة أن هذه المباديء يمكن أن تجد لها موضعا في الدستور المرن او الجامد. وفي كل الاحوال تجدر الاشارة الى أن المباديء الكبرى للحكومة الالكترونية من طبيعة جامدة لا يمكن اعتبارها مرنة وذلك استنادا الى مصدرها النابع من التقنية، فلم تكشف عنها الحوادث التاريخية او المواقف الانسانية وانما الذي صنع مقدماتها الأولى أفكار تطبيقية لتكنولوجيا المعلومات.

وإذا كانت الكلمات السالفة تطغى عليها النواح المباشرة فإنه يمكن إعادة صياغة قانونية لهذه الكلمات من حيث طرح المفهوم التقني الإنساني للحكومة الالكترونية في شكل ضرورة المطالبة بتطبيق مفاهيم الحكومة الالكترونية في صيغة تعمل على إعادة إحياء المفاهيم الضرورية والإنسانية للفرد. فالفرد اليوم يستطيع انهاء أعماله الادارية دون أن يكون عرضة للمضايقة الوظيفية او التعسف في استعمال او استخدام السلطة وبما يستتبع ذلك القول بإمكانية هذا الفرد انهاء كافة أموره الادارية وفق مبدأ المشروعية وذلك باستخدام منهجية الحكومة الالكترونية.

والآن نأتي الى التساؤل مضمون هذه الورقة: ما هي تلك المباديء الكبرى للحكومة الالكترونية؟

هناك أربعة مباديء يمكن أن تكون نواة حقيقية يتشكل على ضوئها الأسس الكبرى للحكومة الالكترونية:

1. مكافحة الانتقائية في العمل الإداري.
2. إزالة الحواجز (عالم افتراضي واحد).
3. المنهجية الفردية وتطوير القدرات.
4. خلق بيئة حرة فكريا (حرية تجول المعلومة والكشف عن مناطق التفكير والرأي والتعبير).

أولا : مكافحة الانتقائية في العمل الإداري:

من الأهمية بمكان ملاحظة الدلالات العميقة التي تشير الى الحكومة الالكترونية كمصطلح يمكن أن يحقق نجاحا كبيرا في مكافحة عدم انتظام الإدارة ماديا من خلال تنظيمها عبر العالم الافتراضي عموما والانترنت على وجه التخصيص، فيما يعرف بمصطلح.. "ميكنة الإدارة"[1] **L'Administration Electronique**. فهذا المصطلح يفيد ان قدرا من الحرية المتعارف عليها يمكن أن يمارس في المجتمع المعلوماتي/ العالم الافتراضي دون أية قيود ما دام هناك تنظيما يعترف به القانون يشكل منطقا ومعيارا لهذه القيود. ولكي تصبح فكرة الحكومة الالكترونية ناجحة في المجتمع المعلوماتي يجب أن يكون هناك منطقة "لا سياسية خالصة **Non Political Zone**" تعمل من خلالها هذه الحكومة، فضلا عن الاهتمام بالمهام الإدارية في عمل الحكومة هذا. ونجد لهذه المنطقة تطبيقا في قانون الحكومة الالكترونية الفيدرالي الأمريكي المؤرخ **17** ديسمبر **2002** **The Electronic Government Act of** [2] الذي يسعى الى ايجاد هذه المنطقة (اللا سياسية

---

[1] **محمد بن يونس – مستجدات ومتغيرات– مقدمة الاصدار العاشر لموسوعة التشريعات العربية 2000.– انظر كذلك مؤلفنا المجتمع المعلوماتي والحكومة الالكترونية– الطبعة الثانية– دار النهضة العربية القاهرة 2005 ص. 204 وما بعدها.**

[2] **Public Law 107-347, December 17, 2002 (HR 2458), See: http://www.access.gpo.gov**

مع الأخذ في الاعتبار أن أول مشروع لقانون الحكومة الالكترونية في الولايات المتحدة الأمريكية كان قد تقدم به عضـــو مجلـــس الشـــيوخ الأمريكـــي Joseph Lieberman الـــى المجلـــس US Senate في 1 / 5 / 2001 (S.803). ولقد صرح الرئيس الأمريكي بوش الأبن عشية صدور القانون في 17 / 12 / 2002 قائلا:

Today I have signed into law H.R. 2458, the "E-Government Act of 2002." This legislation builds upon my Administration's expanding E-Government initiative by ensuring strong leadership of the information technology activities of Federal agencies, a comprehensive framework for information security standards and programs, and uniform safeguards to protect the confidentiality of information provided by the public for statistical purposes. The Act will also assist in expanding the use of the Internet and computer resources in order to deliver Government services, consistent with the reform principles I outlined on July 10, 2002, for a citizen-centered, results-oriented, and market-based Government. Title II of this Act authorizes agencies to award "share-in-savings" contracts under which contractors share in the savings achieved by agencies through the provision of technologies that improve or accelerate their work. The executive branch shall ensure, consistent with applicable law, that these contracts are operated according to sound fiscal policy and limit authorized waivers for funding of potential termination costs to appropriate circumstances, so as to minimize the financial risk to the Government.

Title III of this Act is the Federal Information Security Management Act of 2002. It is very similar to title X of the Homeland Security Act of 2002, which also bears the name Federal Information Security Management Act of 2002 and which I signed into law on November 25, 2002. I am signing into law the E-Government Act after the enactment of the Homeland Security Act, and there is no indication that the Congress intended the E-Government Act to provide interim provisions that would apply only until the Homeland Security Act took effect. Thus, notwithstanding the delayed effective dates applicable to the Homeland Security Act, the executive branch will construe the E-Government Act as permanently superseding the Homeland Security Act in those instances where both Acts prescribe different amendments to the same provisions of the United States Code.

Finally, the executive branch shall construe and implement the Act in a manner consistent with the President's constitutional authorities to supervise the unitary executive branch and to protect sensitive national security, law enforcement, and foreign relations information. In particular, consistent with my constitutional authorities and section 301(c) of this Act, the executive branch shall construe the Act in a manner that preserves the authorities of the Secretary of Defense, the Director of Central Intelligence, and other agency heads with regard to the operation, control, and management of national security systems.

GEORGE W. BUSH, THE WHITE HOUSE, December 17, 2002.

الخالصة في مجال العمل الاداري والمالي) وبما يترتب على ذلك انتفاء حركة الانتقائية بالكامل، وهي الحركة التي تجعل مبدأ المساواة بين البشر متخلفا عن الوجود، ولقد كانت مسألة الانتقائية هذه محض إزعاج للدورة الرابعة والخمسين للجمعية العامة للأمم المتحدة[1]، حيث اعترفت بكونها نقيض المساواة والحياد والموضوعية فتم اعتبار وجود الانتقائية أمر يتعارض مع حقوق الانسان .

فاذا تقلصت الانتقائية فان المعاملات الانسانية سوف تتشعب من وراء الحكومة الالكترونية فتتخذ بالضرورة الشكل المثالي، فكلما كان مصطلح الحكومة الالكترونية متواجدا كلما كانت الصلاحيات الممنوحة لعضو الانترنت مقيدة بسلسلة طويلة من القيود النفسية والموضوعية، فتبرز هذه القيود من خلال الالتزام بالنظام بداية. ومثل هذا الالتزام يخلق معيارية تتكامل مع الفكر الإنساني، فلا تمضي الاجراءات قدما ما دام هناك خللا في الالتزام المشار اليه. فمثلا من يتوجه الى أحد المواقع بقصد استخراج بطاقة شخصية او جواز سفر يلزمه هنا ملء النماذج بالكامل، فاذا ترك فراغ في أحد البيانات فإن ذلك يترتب عليه عدم إمكانية استخراج هذه البطاقة او غيرها من المستندات التي تسير حياة الانسان. فاذا تقدمنا خطوة الى الأمام فإن ترك فراغات في المثال السالف سوف يمنع الرقم القومي لهذا الشخص من الوجود، كل ذلك محسوبا على الدقة المتناهية التي يكون عليها اتصال الأفراد بالحكومة الالكترونية.

وتبدو الحكومة الالكترونية أكثر حدة على العقل البشري في الزمن المعاصر إذا حاولنا استخدام الإمكانيات الكاملة لتكنولوجيا المعلومات لتحقيقها، ففي هذه الحالة سوف يكون هناك تجاوزا لما هو مقرر حول الحكومة الالكترونية فيبدو الامر كما لو كان الانسان يتناول الخيال!! وسوف تقابل الإمكانيات الكاملة لتكنولوجيا المعلومات بالرفض أيضا، وذلك نظرا لعدم وجود هامش انتقائي فيها على الإطلاق من الناحية الادارية والمالية.

---

[1] قرار الجمعية العامة للأمم المتحدة رقم 54 / 174 المؤرخ 15 / 2 / 2000 بشأن تعزيز إجراءات الأمم المتحدة في ميدان حقوق الانسان بتعزيز التعاون الدولي وأهمية اللانتقائية والحياد والموضوعية – الدورة 54 البند 116 (ب) من جدول الاعمال . وقرارها رقم 56 / 153 المؤرخ 19 / 12 / 2001 – الدورة 56 ، وقرارها رقم 57 / 203 المؤرخ 18 / 12 / 2002 – الدورة 57 . كذلك انظر موقف ليبيا من اللانتقائية منشورا في الملاحق.

ثانيا: إزالة الحواجز (مجتمع معلوماتي واحد):

ماذا يعني مصطلح " إزالة الحواجز "؟

إن استخدام هذا المصطلح يعبر عن القيمة الحقيقة للمجتمع المعلوماتي/العالم الافتراضي، إلا أن هذه القيمة تتخذ في الشكل المادي لها صيغة مثالية، ويبرز ذلك في حركة عاطفية تهدف الى الترويج للانترنت كصيغة اعلانية صحفية وإعلامية. والا ماذا يعني وجود عوائق في العالم المادي تجعل مصطلح إزالة الحواجز قائما في العالم الافتراضي؟

والحقيقة ان مصطلح " ازالة الحواجز " يتخذ بعدا جديدا في التفسير يشير الى امكانية الحصول على المعلومة في المجتمع المعلوماتي طالما وجد لها مكانا في العالم الافتراضي، بمعنى انه قد تم وضعها هناك. ولا يعني مثل هذا المصطلح ازالة الحدود السياسية مثلا بين الدول، فمثل هذه الحدود ليست فرضا سياديا امام كافة البشر، بل ان هناك تقسيمة سياسية تعتمد مبدأ حيازة جواز السفر يمكنها ان تزيل حاجز الحدود امام شخص دون اخر، فمن يملك جواز سفر يوناني مثلا يستطيع الدخول الى فرنسا او بريطانيا ولا توجد حواجز من أية نوع لديه في حين يحتاج جواز السفر العربي الى ما يفيد ازالة هذا الحاجز الموضوع أمامه / التأشيرة.

فالحواجز موجودة في العالم المادي وبما يوحي وجودها وكينونتها هنا بوجود وكينونة تفريد في الجنسية والمواطنة وجوازات السفر.. الخ، وبما يوحي بالسند السياسي لهذا التفريد البشري وجود نوع من إقامة الحواجز العرقية والتمييزية عموما. ومثل هذه الاجراءات المتخذة ضد بعض البشر يمكن استخدام الادوات القضائية لردعها، وليس هناك ما يمنع من تطوير آليات المعاهدات والاتفاقيات الدولية في هذا الإطار في مسمى التمييز والعنصرية والعرق والجنس واللون والدين في مواجهة الحواجز المشار إليها كما هو الحال في اتجاهات التشريع الدولي فيا يتعلق بالعالم الافتراضي (ملحق المعاهدة الاوربية حول الجريمة في العالم الافتراضي).

فاذا قبلنا وجود تفريد بشري في العالم المادي في علاقة الانسان بالحواجز، فانه لا يمكن تصوير العالم الافتراضي على انه يتكون من مجموعة من المجتمعات متعددة المشارب والاتجاهات كما هو

الحال في المجتمع المادي، فهو مجتمع واحد فقط، وبحيث يمكن مناظرته بمجتمع آخر له وجود في الفكر المثالي في العالم المادي وهو "المجتمع الإنساني".

ولا يعني ذلك عدم وجود خلاف في المجتمع المعلوماتي وانما لن يكون سند الخلاف سندا سياسيا مبنيا على قواعد الحدود والحواجز التي تقيمها الدول انطلاقا من مفاهيم سياسية.

فالخلاف يبنى في المجتمع المعلوماتي على أسس الحضارة والانتماء العقائدي الذي يجب أن يجد له محلا في تبادل الفكر والتنوع الثقافي والنشاط الذهني وحركة التاريخ ..الخ، دون أن يكون أساسه نقل الخلافات المتواجدة في العالم المادي الى هناك، ودون أن يكون الأمر متعلقا ببناء سياسي له جذور مادية ممثلا في الدولة. ومثل هذا الأمر انتبهت اليه الأمم المتحدة بنوع من الحذر، لذلك لم تمانع الجمعية العامة للأمم المتحدة في عام **1999** من طرح فكرة "الحوار بين الحضارات" بوسائل من بينها نشر المعلومات وتنظيم الحلقات الدراسية وتنظيم المؤتمرات .. الخ[1]وهذه الوسائل يمكن القيام بها في العالم الافتراضي بكل سهولة.

ويقود هذا المنطق الى ربط عملية ازالة الحواجز بمصطلح آخر يلزم ان يكون هو التفسير الوحيد له، ونعني به " التدفق المعلوماتي" في العالم الافتراضي، والتدفق المعلوماتي يعني صيرورة المعلومة في حالة تواصل مستمر مع المجتمع المعلوماتي لأنها هي الركن الأساسي فيه. وكلما زادت حركة التدفق المعلوماتي كلما كان هناك انسيابية وسهولة في التعامل مع العالم الافتراضي عموما، وتستمر بالتالي حركة التطوير في تكنولوجيا المعلومات. فاذا توقف هذا التدفق المعلوماتي فان العالم الافتراضي يقف عند حدود ما تم تحميله عليه، ومع مرور بعض الوقت ينتهي كل وجود لهذا العالم، وبما يعني في النهاية اقتصاره على القيود التي تفرض عليه. وربما ينطبق عليه مثال مكتبة لم يتم تزويدها بالجديد واقتصرت على الموجود فيها وبما يعني في النهاية ان دورها سوف ينحصر في كونها تمثل نسبيا مرحلة زمنية معينة من الحركة الثقافية.

وهنا نستطيع تخيل فكرة التدفق المعلوماتي على انها تنتمي الى مبدأ الحق في المعرفة، وهو مبدأ تعرفه الحضارة الإسلامية بشكل فائق. فالأمر يبدو هنا كما لو كان هناك إعادة كتابة التاريخ بشكل

---

[1] **قرار الجمعية العامة للأمم المتحدة رقم 45 / 113 المؤرخ 7 / 2 / 2000 بشأن سنة الأمم المتحدة للحوار بين الحضارات ، الدورة 54 ، البند 34 من جدول الاعمال .**

أكثر شمولية، فلن ترتبط الوقائع التاريخية بالمؤشرات السياسية ذات الرؤيا الضيقة وانما بمدى النتيجة التي يمكن أن تحققها معلومة ما.

ثالثا: المنهجية الفردية وتطوير القدرات:

لكي يتم اعداد حلقة متكاملة من التواصل الانساني في العالم الافتراضي يلزم، فضلا عن الاعتراف بوجود المجتمع المعلوماتي والحكومة الإلكترونية، وجود صيغة او تفسير لمصطلح الفردية. ذلك ان الفرد في العالم الافتراضي يتسع لأكثر من مجرد ذلك الذي تعترف به الدولة في سجلاتها، سواء كان من مواطنيها او المقيمين بها. فالفرد في العالم الافتراضي يمكن أن يكون آليا دون تردد، ويعترف المجتمع المعلوماتي بهذه النوعية الجديدة من الأفراد وبما يسمح هنا بإحداث التواصل بين الفرد وبين الآلة وبشكل يطغى على المفهوم التقليدي للآلية.

وبناء عليه لا يحتاج التواصل المعلوماتي الى مجموعة افراد مرتبطين بجنسية معينة حتى ولو كانت هذه المجموعة عبارة عن مجموعة اشقاء في منزل واحد كل أمام حاسوبه الخاص، فالجنسية معيار يفشل في العالم الافتراضي بالضرورة، سيما مع توجهات مكافحة التمييز العنصري في العالم الافتراضي، كما هو الشأن فيما اتفقت عليه الدول الأوربية مع اتفاقية مكافحة الجريمة في العالم الافتراضي الموقعة في بودابست **2001**، حيث قررت، كما أشرنا سابقا، وجوب الأخذ في الاعتبار مكافحة التمييز العنصري في ملحق خاص بالاتفاقية المذكورة، وقد سبق بعض الدول الأوروبية الى القيام بنبذ توجه الجنسية في العالم الافتراضي ووصل الامر بالقضاء البلجيكي الى إدانة البعض بارتكاب جرائم عنصرية حال التحرش فيما يتعلق بالجنسية او بالدين او بالعرق .. الخ، وهو الأمر الذي يوحي بأن اليوم الذي يتم فيه الاستناد الى أحكام القضاء لأجل الحصول على تأشيرة دخول الى دول ترفض منح هذه التأشيرة سوف يصبح ممكنا في ظل مفاهيم تكنولوجيا المعلومات وما سوف تحدثه من تأثير في القيم الاجتماعية.

إذن تحتاج الفردية الى صيغة تفسير جديدة يمكن على ضوئها تحديد الفرد في العالم الافتراضي وبشكل يسمح ببعض المرونة في تقبل الفكرة التقنية، وبحيث تضاف الآلية في تكنولوجيا المعلومات الى كل تفسير لمصطلح الفرد. وهذا يقودنا بالضرورة الى نبذ فكرة الفردية التقليدية التي تقوم على نهج الفكر الخاص الذي يروج له أنصار النظرية الاقتصادية/ الرأسمالية تحديدا كما هو الشأن في

إمكانية استيعاب الانترنت لموضوع الانتخابات في الدول التقليدية مثلا[1]. فهذه النظرية الاقتصادية السالفة تتنازعها رياح التغيير منذ ما يقارب النصف قرن حتى الان، وبما يدعو الى التأكيد على أن نموذج الديمقراطية الغربية أصبح تقليديا في معنى إمكانية وجود نماذج أخرى للعملية الديمقراطية لا تتخذ النموذج الغربي قدوة او مثالا يُحتذى، وبما يمكن عدادها متميزة عن المنهج الغربي المذكور في معنى وجود فكر وأرضية لها تتمتع بخصائص مستقلة.

اما الفكرة الفردية في ضوء التفسير المعلوماتي فمنبتها العالم الافتراضي الذي خلقته الآلة والذي لا يمكن التواصل معه الا في ضوء المنهج المعلوماتي. فهي فكرة جديدة او ان تفسير مصطلح الفردية يحتاج الى أدوات تفسير جديدة وبشكل يمكّن من القول ان تطوير القائم الآن لا يكفي وحده لسد فهم هذا المصطلح في المجتمع المعلوماتي. فنظام الشبكات **Networks** الحالي والمستقبلي أيضا لا يمكن أن يتفق مع نموذج الديمقراطية التقليدية من الناحية المعلوماتية ولكنه يتفق مع فلسفة الديمقراطية المباشرة، في حين ان الديمقراطية الغربية التقليدية وجدت ذاتها رقميا ملزمة بتحريك الدورة التقنية الى منتهاها كالتزام علمي تقني يقع على عاتقها. وهنا فان صدام سوف يحدث بين المنهج النظري العقائدي في الفلسفة الغربية وبين المنهج العملي لها في معنى جديد لفكرة الصدام الواقع في ذات الهيكلة التي يقوم عليها النظام السياسي في تلك الفلسفة، فهو هنا صدام ذاتي تحديدا لن يكون له وجود في فلسفة الديمقراطية المباشرة على الاطلاق وانما مركزه الفكر التقليدي فقط.

ان خطوة الى الأمام في فهم الفردية في المجتمع المعلوماتي تستدعي من الباحث ضرورة البحث عن نقطة البداية هنا، اذ كيف يمكننا التوصل الى صيغة تمكننا من الحصول على تفسير لمصطلح الفردية؟

نقطة البداية تكمن في حركة الاتصال بالعالم الافتراضي، فهذا العالم يبدأ عندما يتصل فرد بعينه بالآلة لكي تمهد له الوصول الى العالم الافتراضي. وهنا يصبح لدينا فردية افتراضية او فيما يصطلح على تسميته بـ .. "عضو الانترنت" الذي يصبح كذلك بمجرد ولوجه الى العالم الافتراضي مستخدما الحاسوب على أية شاكلة يكون عليها هذا الحاسوب. فـ .. عضو الانترنت هنا ليس له

[1] **Benoît Tabaka - Internet et la diffusion des sondages électoraux : une réforme législative impossible?- http://www.juriscom.net**

جنسية محددة يتعامل بها في ذلك العالم الجديد وانما له بصمته الخاصة به يستخدمها في صيغة عالمية عابرة للحدود التي كانت تعترف بالجنسية والمواطنة.. الخ.

ولما كانت عضوية المجتمع المعلوماتي هنا قد دخلت في طور الفكر الشعبي وأضحت العامة تستخدمها كجزء من تكوينها الاجتماعي والاقتصادي فإن الحركة التطويرية في التاريخ الإنساني سوف تخلق انتقائية إذا تخلف الركب عن التحول الى القيم المعلوماتية. وسوف تلحق الانتقائية الأفراد دون مسؤولية تقع على كاهل الدول، فما دامت الانترنت قد انتقلت الى المرحلة الأهلية او الشعبية فان الفرد مسؤول عن نفسه هنا وبالتالي سوف يتم وصمه بالجهل او الأمية إذا لم يكن أحد أعضاء العالم الافتراضي. لذلك ان النتائج التي انتهى اليها المجتمع الدولي فيما يتعلق بتنمية الحركة التعليمية في العالم وفق اعلان داكار (المنتدى العالمي للتربية في داكار / السنغال **26** – **28** ابريل **2000**) بشعار التعليم للجميع **Education for all** والذي يعد امتدادا لما اعتمده الاعلان العالمي حول التربية للجميع (جومتيين / تايلاند **1990**) من حيث الالتزام الجماعي بالعملية التعليمية يكاد يتخلف عن اطار العمل العربي من أجل تأمين حاجات التعليم الأساسية في الأعوام **2000** – **2010** (المؤتمر العربي الإقليمي حول التعليم للجميع – القاهرة **24** – **27** يناير **2000** – اعلان القاهرة : التعليم للجميع في البلدان العربية : تجديد الالتزام) فقد أكد اعلان القاهرة على عبارة ذات مغزى، بل وذات بعد يعبر عن الظاهرة الثقافية المعاصرة في الوطن العربي وبما يشكل بحثه لأزمة خطيرة ، ففي صدر الفقرة **33** من اعلان القاهرة جاءت عبارة (الوقت يمر ..) .. وهذه عبارة ربما يفهمها البعض وربما لا يفهمها البعض الاخر ولكن في النهاية فان المحصلة من هذه العبارة ان المسؤولية كبيرة فيما يبدو.

وهنا يأتي التفسير الجديد للقيم المعلوماتية والرقمية في الحركة الثقافية الفردية للإنسان، ومثل هذا التفسير يتناقض مع التوجه الفردي في الفكر الغربي القائم، فالمجتمع المعلوماتي له ثقافته الخاصة به، والتي يمكن ان تحدث تعارضا او تلاق بينها وبين ثقافة المجتمع المادي او العالم التقليدي ولكن لا يمكن ان ينتقل المفهوم التقليدي للثقافة الانسانية برمته الى المجتمع المعلوماتي. وسبب ذلك ان المفهوم التقليدي للثقافة الانسانية له مشاكله ومشكلاته في حين ان المجتمع المعلوماتي/ العالم الافتراضي مبني على أساس عداده ليس مناطق خلاف متعددة على الإطلاق وانما هو منطقة واحدة وهي منطقة اتفاق بالضرورة. ومثل هذا الامر يقود في النهاية الى انه لا يمكن أن تشكل ثقافة المجتمع المعلوماتي في العالم الافتراضي جزءا من ثقافة احد مجتمعات العالم المادي، فلا يصح

مثلا القول بان ثقافة المجتمع المعلوماتي هي جزء من تكوين المواطن الأمريكي او الكندي او الياباني او الايطالي او الليبي او المصري او .. الخ، وهو الإيحاء الذي جاء به مدلول نتائج قمة مجموعة الثمانية في **KANANASKIS** في كندا **2002** بشأن أفريقيا والذي يوحي بوجود حركة تصدير ونقل للتكنولوجيا المتخلفة من جديد كتلك التي تم تنفيذها في التسعينات من القرن العشرين. اذ يجب ان يرتبط المفهوم الثقافي للمجتمع المعلوماتي بالفردية هنا، بحيث يمكن القول ان هذا الفرد (دون اعتبار لجنسيته) هو أحد أعضاء المجتمع المعلوماتي/ العالم الافتراضي في حين ان الآخر ليس كذلك.

رابعا: خلق بيئة حرة فكريا (حرية تجول المعلومة والكشف عن مناطق التفكير والرأي والتعبير).

ان المعلومات هي مقياس بشري بالضرورة، وحتى الآن فان تعريف، وبالتالي تحديد، المعلومة يمكن أن يكون مجال علم جديد هو علم المعلومات كمصطلح دخل القاموس العالمي بجدارة فائقة في المرحلة المعاصرة.

ان الأساس الذي تبنى عليه حركة المعلومة في الثقافة والفهم الانساني لا ينطلق في مرحلة العصر الصناعي من نقطة تعريف المعلومة تحديدا وانما ينطلق من فكر وفلسفة البحث في كيفية اكتسابها من ناحية ثم في البحث في منطق توريدها مرة أخرى، فهذا الأساس يعتمد على السيطرة في حركة توريد المعلومة مع افساح المجال الكامل لعملية تصديرها. ومثل هذا الامر لا يمكنه ان يتوافق مع منهج الفكر المعلوماتي في هذا العصر.

ولقد جعل تفسير العصر الصناعي لمصطلح المعلوماتية الجميع في نقطة بداية بعيدة عن المفهوم الذي يطرحه المصطلح في صيغته الجديدة (مبدأ الرقمية منهج) لكون العامل الحضاري الغربي في الفلسفة الانسانية يقتصر على مفهوم تصدير المعلومة من خلال قنوات محددة بدقة كبيرة. وهي قنوات ظاهرها حقيقي الا انها في موقعها المعلوماتي، وعلى الصورة التي يجب أن تكون عليها، توصم بأنها قناة واحدة فقط. ويعد الجهاز الإعلاني او الإعلامي العالمي النسق الذي يسيطر على تنظيم المعلومة في تواصلها مع البشر، فحادثة او واقعة ما لا يمكن تواصل حدوثها مع البشر او الفرد بدون الجهاز الإعلامي العالمي المذكور، على استثناء يتعلق بالرؤيا المباشرة للحدث، وهي رؤيا بالعين المجردة تقتصر على ثلة من البشر ممن حضروا الحدث، ولا يحدث مثل هذا الاستثناء

كثيرا. وفيما عدا ذلك فان المنطق السمعي– المرئي يمكن أن يكون قاصرا في بلوغ الغاية المطلوبة للمعلومة في تواصلها مع البشر.

وهنا تدخل المعلومة في مرحلة جدل لا ينتهي، سواء من حيث صحتها (تكوين المعلومة) او من حيث هيبتها او مصداقيتها (ملكية المعلومة).

لقد ترتب على عدم انتظام مصداقية المعلومة في المجتمع المادي ان استخدم القراصنة البيئة الافتراضية كمجال استطال العدوان على الملكية الفكرية للبيئات ذات المصداقية المعلوماتية الكاملة، مستغلين صعوبات الإثبات – وليس استحالته – في هذا الإطار. فقد استخدم التشفير في العدوان على حقوق المؤلف بذات الضراوة التي استخدم فيها أنصار القوة المجردة أسلحة التدمير الشامل في ارتكاب العدوان على دول وشعوب مختلفة في المرحلة المعاصرة. والغريب رفض القضاء في بعض الدول الاعتراف بقصور الخبرة الوطنية لديه في هذا المجال في الوقت الذي تعدلت فيه التشريعات الوطنية دفاعا عن حقوق المؤلف دون الأخذ في الاعتبار خطورة هذا الاتجاه، وان كان في دول أخرى أفسح المجال للخبرة الدولية لتتخذ دورها في هذا الإطار دون حرج او كلل او ملل[1].

وفي النهاية فإن مجتمعا بشريا قابع في نطاق الأعلام او الأعلان المادي المقيد لا يستطيع بناء جسور ثقة بينه وبين أية معلومة تصل إليه لكون عوامل التحليل مفقودة عنده، من حيث عدم ثقته في وسائل او وسيلة الأعلام العالمية المتصفة بالتوحدية التي تسيطر على مسار وصياغة المعلومة في تواصلها مع البشر. والمثال التطبيقي على ما سلف يبرز لنا حال البحث في قنوات صياغة المعلومة في العالم المادي بقصد تواصلها مع البشر، فمثل هذه القنوات على ضخامتها لا تشكل قيمة مساحية او حيز ما يذكر في المجتمع المعلوماتي، فهي مجرد مواقع او ورش عمل هناك، وبحيث يمكن أن يكون موقعا فرديا خاصا بشخص واحد له تأثير أعلامي أقوى منها هناك.

فاذا تحولنا الى الواقعية فان سدس عالمنا المعاصر – في افتراض نسبي مضمونه عدم وجود عوالم أخرى– يمكن أن يكونوا بعيدين اليوم عن المعلومة المصاغة ماديا لكونهم يتواصلون مع معلومة أكثر جدية هي المعلومة الرقمية، فهؤلاء وصلوا الى مرحلة استحداث الجدل العقلي بالضرورة ويبقى

[1] **See: Licra v. Yahoo Fr.**

عليهم هنا ان تبدأ نقطة انطلاق حقيقية في قياس الجدل العقلي حول المعلومة المصاغة في المجتمع المعلوماتي. ففي هذا الاطار نجد ان المعلومة عند سدس سكان العالم نابعة من المجتمع المعلوماتي/ العالم الافتراضي في صيغة جدلية جديدة يتلقفها عضو المجتمع المعلوماتي بكثير من التفكير والتحليل وبشكل يتفاعل مع الحدث ذاته، فقد أصبحت تقارير البنك الدولي وتصريحات البيت البيض الأمريكي اليومية سهلة المنال في الوقت الذي يتابع فيه سدس سكان العالم أخبار باقي العالم في دقائق بسيطة باستخدام وسيلة الاشتراك في قوائم المراسلات البريدية عبر الانترنت.

ومن الأهمية بمكان الاشارة الى ضعف الموقف الإعلامي ازاء العالم الافتراضي، فلم تعد الدول التي تسيطر على الأعلام الدولي قادرة على التحكم في مسار الفكر المعرفي وقراءة التاريخ، فمن يلج الى المجتمع المعلوماتي/ العالم الافتراضي لا يحتاج الى وسائل الأعلام التقليدية لكي يفي المعرفة حقها، بل انه لا يلج الى مواقع وسائل الأعلام التقليدية المذكورة الا للارتباط وفيما عدا ذلك فانه يصل الى موقع الحدث ذاته، الذي تتناقله وسائل الأعلام، لكي يطلع عليه مباشرة، او مسجلا. وهذا يحتاج الى تواصل في القيمة المعلوماتية بين الحدث وبين العالم الافتراضي، وهو تواصل لا يحتاج الى اذن من أية جهة بقدر ما يحتاج الى مبادرة توصيل المعلومة او الحدث الى العالم الافتراضي. وهذا النوع من المبادرات يلزمه التفاعل مع الأحداث، حيث ان العالم الافتراضي يحتاج الى التواصل الفوري مع الأحداث وبشكل يكون فيه الزمن الافتراضي متفاعلا مع العالم المادي في صورة نقل ما هو حادث الى العالم الافتراضي. ومن ثم يمكن القول بان شخصا ما يمكنه وضع كاميرا رقمية في حجم القداحة في منزله بقصد تسجيل الوقائع اليومية فيه، فلا يعد ذلك منه مجرد عملية تجسسية يقوم بها على أهل منزله، بل هي كتابة تاريخ رقمي لمنزله وعائلته تسمح للاجيال الجديدة فيها من الاطلاع على نظام عمل الاسلاف، بل ومن الممكن أن يكون أهل المنزل ممن يخضعون لعملية التسجيل السمعي مرئي على دراية وعلم بهذه الكاميرا والغرض المعد لها وهم سعداء بذلك.

ويلزم أن يكون هناك مفارقة واضحة بين كل من الرأي **Opinion** وبين التعبير **Expression** وبين المعلومة **Information** . فمثلا المادة **(19)** من الاعلان العالمي لحقوق الانسان تنص على انه "لكل فرد الحق في حرية الرأي والتعبير"، في حين كانت المادة **(9)** من الميثاق الأفريقي

لحقوق الانسان والشعوب تنص على انه ".. لكل فرد الحق في استقبال **Receive** المعلومات.."[1]، ولقد انضم هذا الميثاق الى ميثاق الاتحاد الأفريقي[2] المؤرخ **11** يوليو **2000** في المادة **(3 / H)**.

ومن الملاحظات المهمة في إطار ميثاق الاتحاد الأفريقي هو تناوله لمسألة المشاركة الشعبية **Popular Participation** في المجال السياسي (المادة **g/3**) كمصطلح تطويري يمكن أن يكون له امتداد ايجابي عبر المجتمع المعلوماتي/ العالم الافتراضي. وحتى المرحلة المعاصرة فان مسألة التمييز بين الرأي وبين التعبير وبين المعلومة من الموضوعات ذات الجدلية العقلية التي لم تأخذ حظها بذات المهارة التي يمكن بها اعتبار كل من الرأي والتعبير من مصادر المعلومة[3]. ومثل هذا يؤدي الى الخلط، وهو ما يخلق العديد من المفارقات في الآلية التي تعمل بها المعلومة. فمثلا ان المعلومة أضحت سلعة (ولم تعد خدمة) حين ان كل من الرأي والتعبير ليسا من السلع وانما من الحقوق التي قد يقابلها التزامات وواجبات، سيما من الناحيتين القانونية والأخلاقية.

---

[1] African Charter on Human and Peoples' Rights , EIGHTEENTH ASSEMBLY OF HEADS OF STATE AND GOVERNMENT, JUNE 1981, NAIROBI, KENYA 21 October 1986 . " Article 9:
1. Every individual shall have the right to receive information.
2. "Every individual shall have the right to express and disseminate his opinions within the law". African [Banjul] Charter on Human and Peoples' Rights, adopted June 27, 1981, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), entered into force Oct. 21, 1986: [excerpts] . . .

[2] Constitutive Act of the African Union, Lomé, Togo, this 11th day of July, 2000. Article 3 : Objectives : The objectives of the Union shall be to: h - Promote and protect human and peoples' rights in accordance with the African Charter on Human and Peoples' Rights and other relevant human rights instruments;

[3] Thomas Cochrane , Note, The law of nations in cyberspace: fashioning a cause of action for the suppression of human rights reports on the internet 4 Mich. Telecomm. Tech. L. Rev. 157 (1998) available at http://www.mttlr.org/volfour/cochrane.pdf P. 174

(3)

القانون الوطني الامريكي

The USA Patriot Act

The Uniting & strengthening America by Providing Appropriate Tools Required to Intercept & Obstruct Terrorism
Public law No. 107- 56, Oct. 26, 2001

فهرس:

مقدمة:

أثار صدور القانون الوطني الامريكي (القانون الوطني) العديد من التساؤلات، وكان أهمها مسألة التعارض الذي يمكن أن يقيمه القانون الوطني هذا مع الحق في الخصوصية وفق المفاهيم الانسانية الكبرى والدستورية وكما أرساها– تحديدا– التعديل الرابع للدستور الامريكي والتطورات الحادثة تشريعا وقضاءا في النظام القانوني الامريكي. والحقيقة التي لا ينازعها شك أن موضوع الخصوصية من الموضوعات المرنة في القانون المقارن ككل. لذلك فإن مسألة تقرير قواعد عامة في إطار الدفاع عن الحق في الخصوصية لا يعني أن هناك تقرير عام يشمل كافة الاجراءات التي يمكن أن تتعارض مع الخصوصية بقدر ما يعني أن الخصوصية تقترب من الطرح الاجرائي في مقابل تصور موضوعي يخضع لما يقرره القضاء هنا، فلا يستطيع أحد الجزم بأن هذه او تلك الاجراءات تمس الخصوصية الانسانية إلا بتقرير القضاء لذلك. وهذه النقطة كانت حتى مرحلة ما قبل صدور القانون الوطني الامريكي من الموضوعات المثيرة للجدل في الحقيقة. فلم يكن أحد هناك يستطيع حسم موضوع الخصوصية وفيما إذا كان هذا او ذلك الاجراء المتخذ من قبل السلطات فيه تعريض بالخصوصية سوى القضاء. ولهذا الامر تسبيب لائق، فالأصل في البحث في مجال الخصوصية هو ذلك الارتباط الذي يبدو منطقيا بين موضوع التفتيش والضبط **Search & Seizure** كاجراء قانوني يتخذ في مواجهة واقعة اجرامية معينة وبين إجراء التفتيش والضبط.

وفي هذه الورقة سوف نستعرض هذا القانون في مجال تأثيره على الخصوصية، وتحديدا في إطار التعرض لعلاقة الخصوصية والعالم الافتراضي **Cyberspace** وهو العالم الذي خلقه تشابك الحواسيب في اجتماع رائع نجم عنه التقاء المعلومات وتداولها فنشأ المجتمع المعلوماتي. فالسؤال– في هذه الورقة– يبدأ إذن من نقطة تأثير التفتيش والضبط للأدلة الرقمية على الحق في الخصوصية؟ فنعرض في شكل موجز للتطور التاريخي لمرحلة ما قبل القانون الامريكي ثم تأثير القانون الوطني في هذا الشأن. وبطبيعة الحال يستدعي هذا الامر البحث في تعريف التشريع الوطني الامريكي وبحيث تكون هذه الورقة في النهاية معينا على فهم هذا القانون الذي أثار جدلا كبيرا في محيط فقه القانون المقارن. وكان له كذلك تأثيرا من نوع ما على السياسة الدولية. فقد برز هذا القانون على المجتمع الدولي كما لو كان يد طولة للحكومة الفيدرالية الامريكية تهدد به السياسة الدولية القائمة على فكرة المصالح الانسانية لكي يستعاض عنها بفكرة الهيمنة المطلقة.

لقد كان من أهم أسباب نشاطنا في طرح هذه الورقة هو إن تغييرا سوف يحدث في حركة تفاعل قانون الاجراءات الجنائية عبر الانترنت في النظام القانوني المقارن، وهو تغيير وإن كان النظام القانوني الامريكي قد تفاعل معه، فإن المجتمع الدولي لم يتخذ بعد الخطوات الملائمة للقيام بذلك التفاعل او الاعتداد به حتى وإن كان اتجاه السياسة القانونية والإجرائية في سعي دؤوب للوصول الى هذه النقطة التي وصل اليها المشرع الأمريكي. ويبدو السبب في ذلك منطقيا نوعا ما، فمسألة التقرير بأن أغلب نصوص القانون الوطني هي نصوص مؤقتة سوف تنتهي مع غروب شمس ديسمبر **2005** من الموضوعات التي جعلت تأجيل البحث في هذا القانون لدى فقه الاجراءات المقارن من الأمور الصحيحة، فقد استوعب الفقه الاجرائي وقتية هذا القانون ولم يكن في الحسبان تراجع المشرع الفيدرالي الامريكي عن هذا الوعد التشريعي المقنن.

وبانتهاء العام **2005** فوجيء النظام القانوني المقارن بنوايا المشرع الفيدرالي الامريكي الصريحة بعد أن كانت مجرد نوايا أخذت طابع الحركة البسيطة المتجددة، باستخدام تشريعات قد يتوافر لها الفرصة المتوالية لكي تعرض على القضاء الدستوري، من حيث استحداث نصوص خلال فترة الأربعة أعوام المنصرمة تتفاعل أليا مع القانون الوطني مثل قانون الوطن الأم **The Homeland Security Act 2002** [1] وقانون الحكومة الالكترونية **The Electronic Government Act 2002** [2] ..الخ. فقد بدا من خلال هذه النصوص أنه ليس في نية المشرع الفيدرالي الأمريكي

---

[1] **The Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002).**

[2] **ويتضمن قانون الحكومة الالكترونية الامريكي في محتواه قانونا أخرا هو قانون ادارة أمن المعلومات لعام 2002 (اختصارا FISMA) الذي تعود جذوره الأولى الى قانون أمن الحاسوب لعام 1987 وقانون تقليل التعامل الورقي لعام 1995 وقانون مراجعة تكنولوجيا المعلومات لعام 1996 وأخير قانون مراجعة نظام المعلومات الحكومي لعام 2000 الذي ألغي بمقتضى قانون الحكومة الالكترونية لعام 2002 محل الطرح. ولقد صدر قانون الحكومة الالكترونية هذا بعد صدور قانون الوطن الأم The Homeland Act 2002 الذي تم بموجبه إنشاء وزارة للداخلية في الولايات المتحدة الامريكية. وكان الالتزام بمقتضى العنوان الثالث Title III من قانون الحكومة الالكترونية والذي يتضمن قانون FISMA هنا هو ضرورة قيام نظام أمني متكامل للحكومة الالكترونية بما في ذلك الالتزام بتطوير هذا النظام الأمني. ومن مظاهر الالتزام الأمني هنا: التوسع في النظام الأمني لكي يشمل المعلومات ونظم المعلومات بحيث يجب أن يتوافر لكافة الجهات التي تتعامل بوثائق او معلومات او مرتبطة بنظام معلومات حكومي نظاما امنيا تتوافر له مقومات حماية المعلومات والنظام المعلوماتي على السواء. لأن قانون FISMA لا يتولى بالحماية المعلومات فقط وإنما نظم المعلومات أيضا مثل التأكيد على وجود ادارة تهيئة قوية: حيث يتطلب FISMA ضرورة قيام كل مؤسسة بتطوير نظام تهيئة بحيث يتوافق مع حاجاتها. ومثل هذا الأمر المقرر قانونا يجعل كل**

القيام بإلغاء القانون الوطني وإنما.... تثبيته[1]. وهذا ما حدث فعلا من خلال تصريحات المسئولين في الادارة الامريكية خلال شهر أغسطس **2005**. لقد بدا الأمر هنا كما لو كان ذلك التعايش المؤقت للبشرية مع القانون الوطني الامريكي يتحول لكي يصبح تعايشا دائما هنا! فكأنما التشريع أداة تدريب للبشرية على تقبل مسألة تقييد حركتها.

على أن لهذا الأمر منظور آخر يمكن أن يكون صحيحا. فإذا كانت فكرة مراقبة وحماية سيادة الدولة هي الدافع الرئيسي الى قيام النظام القانوني في العصر الصناعي باتخاذ كافة الاجراءات المناسبة في هذا الإطار مثل القرارات السياسية والحربية والاقتصادية وغيرها...الخ. فإن السيادة الفردية هي مهد العصر الرقمي، وبالتالي كيف يمكن مراقبة السيادة الفردية هنا؟ ذلك هو السؤال الذي يعد القانون الوطني الامريكي وجهة نظر (تكاد تكون وحيدة) في طرح الإجابة على السؤال المذكور. ومن هذا المنطلق يمكن البحث في القانون الوطني الامريكي. وهذا الأمر بدأ واضح المعالم في السياسة التشريعية الامريكية حيث استقر الرأي لدى المشرع الفيدرالي على انتهاج سياسة تشريعية تميز بين مختلف أنواع الاتصالات عوضا عن الاهتمام بمنهج القضاء الأمريكي في تفسير الخصوصية التي تضمنها وتولاها بالحماية التعديل الرابع للدستور الأمريكي[2]. فالصراع إذن بين المشرع والقاضي الفيدراليين حول الخصوصية في منهجية تقرير سياسة تشريعية يمكن على أساسها بناء تفسير مناسب بين الخصوصية وبين الأشكال المختلفة للاتصالات وتكنولوجيا المعلومات.

مؤسسة تلتزم بالتطوير بما يتناسب وتطور تلك الحاجات. وتقنين المتطلبات لتأمين استمرارية تشغيل النظم: بحيث يتوافق هذا مع الاستمرار في تقديم الخدمة بما يعرف في فقه القانون الإداري بالتزام الادارة باستمرار ادارة المرفق العام.

[1] لقد تنبأنا بذلك في مؤلفنا المجتمع المعلوماتي والحكومة الالكترونية/ مقدمة الى العالم الافتراضي وقانونه– انظر الطبعة الأولى (2002) والطبعة الثانية (2003) دار الفكر الجامعي ودار النهضة العربية.

[2] Robert A. Pikowsky- The Need for Revisions to the Law of Wiretapping and Interception of Email, 10 Mich. Telecomm. Tech. L. Rev. 1 (2003), available at http://www.mttlr.org/volten/pikowsky.pdf P. 3 "Congress unduly focused on the different communications technologies rather than the common privacy interests that exist across all media of communication. As a result, different standards govern the issuance of judicial authorization for law enforcement officers to conduct a telephone wiretap, to intercept email, or to covertly access email from storage in a person's mailbox at his Internet Service Provider.".

لذلك فإننا نكرر أنه ليس هناك من بد في أنه يلزم فقه القانون المقارن وخاصة العربي التعرض لهذا القانون بشكل يحقق مصلحة في فهمه لكي يكون هذا الفهم منطقة وعي بهذا القانون تتفاعل مع التطورات المستقبلة، وبحيث يكون مرسى هذا الوعي ليس البحث في ثنايا هذا القانون بقدر ما يكون مستهدفه هو تأمل التطورات التي يمكن أن تحدث في قانون الاجراءات الجنائية المقارن. إذ تحتم طبيعة دراسة القانون أن نبحث في جدواه ومدى الحاجة اليه بحكم أن المصلحة هي المحرك الرئيسي للقانون وإقراره. فما هي المصلحة المرجوة من هذا او ذاك القانون ومدى ملائمة هذه المصلحة للمشروعية...الخ؟ تلك هي الأسئلة الأساسية التي يجب أن تكون محركا لإقرار أي قانون.

سوف نتناول في هذه الورقة– وكما أسلفنا– البحث في تأثير القانون الوطني على الحق في الخصوصية عبر الانترنت. وإذا كنا قد أسلفنا أن موضوع الخصوصية في العالم المادي– رغم دستوريته– لا يزال في إطار محنة الموضوعية التي يفصل فيها القضاء فإن الامر يتسع الى أبعد من هذا المفهوم عبر العالم الافتراضي والانترنت. فالخصوصية عبر الانترنت من الموضوعات ذات الجدل الكبير أصالة في الوقت الذي توسع فيه المشرع الامريكي ليفرض نوعا من التأكيد حول أهمية هذا الجدل في إطار وبحيث يبدو للباحث في أي مكان أنه لا يوجد خصوصية على الإطلاق عبر الانترنت!

إن من الموضوعات الهامة التي يلزم الفقه إثارتها في بحوث المشروعية تتمثل في البحث عن مقياس للمشروعية يتناسب مع القانون الوطني الامريكي. وهذا يعني في الحقيقة أن طرحا يجب أن يتم مسعاه البحث في المشروعية التقليدية التي تطالب بإنهاء هذا القانون وبين مشروعية جديدة تعمل على التغيير في مفهومها وبالتالي لا ترى في المطالبة بإلغاء هذا القانون منطقا ملائما خاصة وإن شرطها لإلغاء هذا القانون– وبالتالي مسايرة الاتجاه التقليدي– هو البحث في بديله الذي يجب أن يكون له وجود.

الفصل الأول

الاجراءات في مرحلة ما قبل القانون الوطني الامريكي[1]

كان الحال قبل **11** سبتمبر **2001** متميزا بنوع من الغرابة، فمحاولة اتخاذ إجراء للتفتيش او أي إجراء يتضمن عدوانا على الحق في الخصوصية يعد من المشكلات، خاصة فيما يتعلق بتفتيش الحواسيب والانترنت. ومع ذلك فإن مشكلة التفتيش والتعقب والتقصي من الموضوعات التي كانت الجهات القضائية وبصفة خاصة مكتب التحقيقات الفيدرالي **FBI** يقوم بإجرائها بكثير من الحذر. واذا كان المشرع الفيدرالي في القانون الوطني قد منح هذه الجهات مبررا قانونيا للقيام بذلك واتخاذ الاجراءات الجنائية التي تنتهك الخصوصية فكيف كان الحال قبل الحادي عشر من سبتمبر **2001**؟

إننا اذا عدنا الى العام **2000** وهو العام الذي ظهرت فيه الخطة الوطنية لأمن المعلومات في الولايات المتحدة الامريكية لوجدنا أن هذه الخطة كانت قد تقررت نتيجة لدراسات حول موضوع أمن الانترنت بدأت في تاريخ سابق عليها. فالمباحث الفيدرالية بدأت فعلا تطبيق إجراءات تقنية في التفتيش والتقصي عن الجريمة، ولقد بدأت مشاكل هذا الطرح في قيام المباحث الفيدرالية في طرح برنامج كارنيفور[2] **Carnivore** [3] الذي تحول تسميته في عهد الرئيس بوش الابن الى **DCS**

---

[1] **انظر في تفصيل ذلك مؤلفنا المجتمع المعلوماتي والحكومة الالكترونية/ مدخل الى العالم الافتراضي وقانونه– الطبعة الثانية– دار النهضة العربية القاهرة 2005. ص. 108 وما بعدها.**

[2] **انظر في هذا البرنامج موقع مكتب المباحث الفيدرالية الامريكي، تمت المراجعة في يونيو 2005 على الموقع التالي:**

http:// www.usdoj.gov/jmd/publications/Carnivore_draft_1

[3] **"إن مصطلح كارنيفور Carnivore في ترجمته الحرفية يعني (آكل لحوم البشر بعكس كلمة Omnivore التي تعني الحيوانات أكلة الأعشاب) وهو هنا يشير الى برنامج يأخذ شكل أداة تشخيصية Diagnostic Tool مهمتها تقصي المواقع الإجرامية وتحركات المجرمين والمشتبه بهم في اطار تكنولوجيا المعلومات. فهو عبارة عن برنامج محلل للشبكات Network Analyzer بقصد التقصي Sniffer ، والهدف من هذا البرنامج هو تمكين مكتب التحقيقات الفيدرالي (المباحث الفيدرالية الامريكية) FBI من تقصي المعلومات حول الجريمة بالسرعة الممكنة التي تحدث بها الجريمة، دون حاجة للرجوع الى مزود خدمات الانترنت ISP على الإطلاق. ومن حيث الطبيعة يعمل كارنيفور كـ .. برنامج تنفيذي Application Program في حاسوب شخصي عادي Normal PC في بيئة**

1000. على أن الطبيعة القانونية لهذا البرنامج لم تتحدد سوف في اعتباره محل تشكيك من قبل النظام القانوني، فقد تم اعتباره من طبيعة موحدة على الرغم من أنه يخضع لمجموعة بدائل سيما في إطار تحديد المهام الموكلة اليه. فقد بدأت مهمة هذا البرنامج فقط في تحديد رؤوس الرسائل **Headers** وأخذ التطور ينال منه الى أن انتهى الى كونه كاشف لمحتوى الرسائل ذاتها. الهدف من هذا البرنامج مراقبة حركة الجريمة بما يتوافق مع تكنولوجيا المعلومات والاتصالات نتيجة للقصور الواضح في التتبع والتقصي المادي.. ويتبع في صيغة عمل هذا البرنامج إيداع نسخة منه في الخوادم والملقمات حول العالم بحيث يؤدي دوره في تتبع وتقصي التحركات المشبوهة للمجرمين والهكرة. ولقد دخل برنامج كارنيفور الخدمة في يونيو **2000** وفي ذلك العام كتب الرئيس الامريكي السابق بيل كلينتون يقول "إن الخطة الوطنية لحماية نظم المعلومات تعد ركنا جوهريا ذات تأثير قوي. هذه الخطة للدفاع عن العالم الافتراضي سوف تتطور ويتم إضافة الجديد اليها بذات القوة التي نتفهم فيها الانتهاك وخطورة التهديد. فهي تبرز مدى رؤيتنا لضرورة تحديد الحماية للقطاعات الأساسية في اقتصادنا، وأمننا القومي، والصحة والسلامة العامة"[1].

او نظام تشغيل النوافذ Widows OS ، ويتم تشبيه كارنيفور بالصندوق الأسود Black Box حيث يتم وضعه في كل شبكة مزود خدمات الانترنت لكي يقوم بنسخ كل ما يقوم به مستخدم الانترنت من أعمال . ولقد كان هذا البرنامج في بداية إعداده في معامل FBI مهيأ لتقصي رؤوس الموضوعات Header فقط مثل عناوين البريد الالكتروني From و To وكذلك نطاقات الأسماء DNS .. الخ ، إلا انه تم تطويره لكي يمكنه كذلك نسخ محتويات المراسلات بأنواعها بما في ذلك مضمون الرسائل الالكترونية ومضمون حركة التصفح عبر الانترنت كاملة" انظر مؤلفنا السابق الاشارة (المجتمع المعلوماتي) ذات الموضع.

[1] "The National Plan for Information Systems Protection is the first major element of a more comprehensive effort. The Plan for cyber defense will evolve and be updated as we deepen our knowledge of our vulnerabilities and the emerging threats. It presents a comprehensive vision creating the necessary safeguards to protect the critical sectors of our economy, national security, public health, and safety. " . Bill Clinton USA President Introduction to (Defending America's Cyberspace) National Plan for Information Systems Protection ,Version 1.0, An Invitation to a Dialogue The White House 2000 http://www.ciao.ncr.gov .

- الأساس القانوني للإجراءات قبل صدور القانون الوطني:

في مرحلة ما قبل صدور القانون الوطني كانت المباحث الفيدرالية تعتمد في هيكلة النظام القانوني لهذا البرنامج على محاولة تفسير وإعادة تفسير متكررة لبعض التشريعات والسوابق المتعلقة بمشروعية مراقبة حركة الاتصالات بشكل عام ونعرض لها فيما يلي:

- The Communications Act of 1934.

يُعد قانون الاتصالات الأمريكي الصادر عام **1934** التشريع الأساسي الذي بدأت حركة مراقبة الاتصالات بمقتضاه. ولقد قامت الجهات القضائية والرسمية في الولايات المتحدة بمحاولة إعادة تفسيره بما يتوافق مع التطورات الحادثة في تكنولوجيا المعلومات والاتصالات وسط انتقادات حادة في هذا الشأن. ولقد كانت أحد المعادلات الصعبة التي لم تنته الى حل في مرحلة ما قبل صدور القانون الوطني الأمريكي هي تلك المعادلة التي كانت الشغل الشاغل لمزودي خدمة الانترنت **ISPs** حيث كان يجب عليهم إقامة توازن بين تعارض التزامهم تجاه الأفراد وتجاه السلطات في شأن الخصوصية. وما إذا كان يجب مراعاة الحق في خصوصية الأفراد او الدفاع عن الأمن العام ومساعدة السلطات في مكافحة الجريمة حتى قبل وقوعها، إذ من غير المعقول أن يكون هناك مشروع إجرامي سوف يتم ومع ذلك يكون هناك التزام ثقيل على عاتق مزود الخدمة بعدم الكشف عنه استنادا الى الحق الخصوصية[1]. لذلك تتابعت التشريعات وتواترت أحكام القضاء على إعداد محاولة تفسير في هذا الشأن وصولا الى حسم للموضوع.

[1] **FEDERAL COMMUNICATIONS COMMISSION FCC Washington, D.C. 20554 Communications Assistance for Law Enforcement Act and Broadband Access and Services ET Docket No. 04-295 RM-10865. "For years, service providers have attempted to balance the conflicting obligations of protecting the privacy interests of their customers while at the same time fulfilling the lawful and ever-increasing demands of law enforcement for subscriber information and call detail records as well as demands for technical assistance for electronic surveillance.**
The origins of these conflicting obligations can be found in Section 605 of The Communications Act of 1934 and the cases interpreting Section 605.2 With respect to the records created by service providers that contain detailed information about a customer's calling patterns, for example, the court held that Section 605 did not apply to the release of telephone toll records because they are business accounting records that subscribers know the telephone company prepares in the regular course of its business. United States v. Costello, 410 F.2d 536 (2nd Cir. 1969). Costello and similar decisions of other courts foreshadowed Smith v. Maryland, 442 U.S. 735 (1979), which

held that there is no Fourth Amendment protection for toll records created by telephone companies in the regular course of their business. Service providers now respond to well over a million subpoenas, court orders, and search warrants annually for the production of subscriber information and toll or call detail records. Except in very limited circumstances, however, service providers bear entirely the burdensome cost of producing these records for law enforcement. Hurtado v. United States, 410 U.S. 578 (1973); see Ameritech v. McCann, 297 F.3d 582 (7th Cir. 2002).3

Title III of The Omnibus Crime Control and Safe Streets Act of 1968, codified, as amended, at 18 U.S.C. §§ 2510 et seq., (hereinafter Title III), resolved a long-standing national debate whether law enforcement could engage in electronic surveillance and whether the results of such surveillances would be admissible in court. Telephone companies, however, resisted voluntarily cooperating with law enforcement in implementing court-authorized interceptions. When it was established that Title III did not authorize a federal court to compel a telephone company to assist law enforcement, Application of the United States For Relief, 427 F.2d 639 (9th Cir. 1970), Congress promptly amended Title III to enable law enforcement to request the court approving the electronic surveillance to direct at the same time that the service provider provide all information, facilities and technical assistance ("technical assistance") necessary to carry out the wiretap the court was authorizing. Since 1970, law enforcement has routinely included a request that the court direct the service provider to provide the essential technical assistance to make their electronic surveillance tools operational. When such an order is issued, it also directs law enforcement to reimburse the service provider for the costs it has incurred.

Nevertheless, service providers continued to resist assisting law enforcement in installing pen registers, which were not covered by Title III, but their efforts were unavailing. In United States v. New York Telephone Co., 434 U.S. 159 (1977), the Court held that a federal court could compel a telephone company to provide technical assistance (which the Court described as "meager," id. 434 U.S. at 175) to law enforcement in connection with the installation of a pen register. Service providers' arguments that they could not be compelled to provide technical assistance for traps and traces were similarly rejected. See, e.g., In the Matter of the Application of the United States for an Order Authorizing Installation of a Pen Register or a Touch-Tone Decoder and a Terminating Trap, 610 F.2d 1148 (3rd Cir. 1979).

These opinions emphasized that service providers have an interest in assisting law enforcement because they have a duty to see that their facilities are not used unlawfully. See New York Tel. Co., 434 U.S. at 174. The Court noted that private citizens, such as service providers, have a "duty to provide assistance to law enforcement officials when it is required." 434 U.S. at 176 n. 24. It has also been established by other courts that this duty to assist law enforcement can even include having the service provider itself execute a search warrant on behalf of law enforcement. See, e.g., In the Matter of the Application of the United States for an Order Authorizing an In-Progress Trace of Wire Communications Over Telephone Facilities, 616 F.2d 1122 (9th Cir. 1980), cited with approval in United States v. Bach, 310 F.3d 1063 (8th Cir. 2002).

When Congress enacted the Foreign Intelligence Surveillance Act of 1978, (codified, as amended, at 50 U.S.C. §§ 1801 et seq.), and Pen Registers and Trap and Trace Devices, (codified as amended at 18 U.S.C. §§ 3121 et seq.)("Pen/Trap Statute"), (which was part of The Electronic Communications Privacy Act of 1986, Pub.L. 99-

508, 100 Stat. 1848 ("ECPA")),4 it ensured that law enforcement could compel a service
provider to provide the technical assistance that is necessary to carry out the electronic surveillance authorized by the court. See 50 U.S.C. § 1805(b)(2)(B) and 18 U.S.C. §§ 3129(a) & (b) respectively. But until 1994 service providers incurred no significant expense or technical burden in complying with these court orders because they could use those facilities and services that were readily available in their networks to serve their customers to provide technical assistance to law enforcement.
With the enactment of CALEA, however, the nature, complexity and expense of the technical assistance that service providers are now compelled to provide changed radically. CALEA mandates that service providers deploy only those services that ensure that electronic surveillance remains a viable investigative tool for law enforcement. With CALEA, service providers could no longer fulfill their obligation to provide technical assistance as they had in the past from service features that had been designed to serve their customers. The service provider's obligation changed from reactive to proactive, thereby making the provision of technical assistance a considerably more complex and expensive undertaking for service providers and forcing service providers to become more involved in the technical issues surrounding electronic surveillance. The expenditures incurred and technical complexities encountered by service providers to meet the obligations of CALEA, however, were considerably underestimated in 1994, and remain so today.
At the same time, service providers also risk criminal sanctions and civil liability if, in the course of providing their technical assistance, things go awry, see, e.g., 18 U.S.C. §§ 2232 (d) and (e) and 18 U.S.C. § 2520, or they do not meet their CALEA obligations. 18 U.S.C. § 2522. Out of concern for these potential sanctions and liabilities, some service providers, particularly the large entities, have established sizable internal staffs to handle these matters. These service providers train and update their internal staffs on a continuing basis on both the technical and legal aspects of providing technical assistance.5 With the variations between the federal and state electronic surveillance statutes, service providers face a complex challenge to ensure they are complying with valid court orders.6 This challenge is even more complex for service providers that operate in multiple states because there are additional variances between state electronic surveillance statutes.
The financial reality for the service provider is that the production of customer records and the provisioning of technical assistance afford only a limited opportunity to recover its associated costs, making the production of records and the provision of technical assistance an increasingly expensive cost center. It is not surprising that many service providers, especially new entrants providing voice communications and traditional Internet service providers, have chosen to fulfill their obligations by looking to third parties for best-cost, efficient solutions associated with these support services rather than incur the burdensome expense. Many service providers have chosen Fiducianet to provide full end-to-end law enforcement support services.".

- Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III) , the Wiretap Act, 18 U.S.C. §§ 2510–2522 (1994).

وهو القانون الذي ينظم استخدام الرقابة الالكترونية **Electronic Surveillance** لتقصي المضمون الكامل للاتصالات الهاتفية فيما يعرف بمصطلح **Wiretapping** [1] (انظر تحديدا القسم **18 U.S.C. § 2516 (1994)**). وهذا القانون يعد التطوير الأول العام للبحث في تشريعات حماية الخصوصية التي يقدسها المجتمع الأمريكي. ومن هذا القانون تم استقاء التشريعات المتتالية اللاحقة عليه. بل ولقد كان هذا القانون المحتوى التشريعي الأول لكافة التشريعات المرتبطة بمراقبة الاتصالات.

فمثلا مراقبة محتوى المكالمات الهاتفية ومحتوى المراسلات الالكترونية **Emails** تم تنظيمها بمقتضى قانون المراقبة هذا **The Wiretap Act, 18USC Sec. 2510-22**. فهذا القانون

---

[1] يميز هنا بين وسيلتين للمراقبة:

- **الوسيلة الأولى: هي مراقبة الاتصالات الهاتفية Wiretapping. ففي حالة Wiretap فإن الوسيلة الى تنفيذها هي وضع أداة مراقبة الكترونية في جهاز هاتف الشخص المستهدف بالمراقبة. وبالتالي استخدام هذه الوسيلة في الاستماع الى المحادثة او المحادثات التي تتم مع الشخص المستهدف.**
- **الوسيلة الثانية: وهي مراقبة المحادثات مباشرة Bugging حيث يقوم المستمع باستخدام وسيلة الكترونية ووضعها بجوار المستهدف بالمراقبة. كأن يتم وضع الجهاز في غرفة نومه او عربته او على مكتبه...الخ ويتم الاستماع الى ما يدور من أحاديث قد تكون للمستهدف او للغير ممن يتواجد بجوار الأداة.**

وكل من مراقبة الهاتف ومراقبة المحادثات مباشرة باستخدام المراقبة الالكترونية ووسيلتيها المشار اليهما يخضعان للعنوان الثالث Title III او ما يعرف بـ... Wiretap Act المشار اليه. ويشترط العنوان الثالث المذكور لكي تتم المراقبة الالكترونية ما يلي:

1. **أن يكون هناك سبب معقول Probable Cause يُعتقد بموجبه أن هناك شخصا محددا قد ارتكب جريمة فأكثر مما هو منصوص عليه في القانون.**
2. **أن يكون هناك سبب معقول مضمونه أن المراقبة سوف ينتج عنها دليل في الجريمة.**
3. **تم اتخاذ إجراءات تحقيق عادية ولم يتم التوصل بمقتضاها الى شيء يساهم في الإدانة او كانت هذه الاجراءات معرضة للفشل او للخطر.**

أن يكون هناك سبب معقول يدعو الى الاعتقاد بأن الأدوات المستخدمة في المراقبة قد سوف يتم استخدامها عند وقوع الجريمة او مرتبطة بشخص المشتبه به دون غيره.

يتطلب قبل القيام بالإجراء الحصول على أذن تفتيش **Super Warrant** مؤسس على سبب معقول **Probable Cause** ما لم يتوافر استثناء يبيح القيام بالاجراء دون حاجة لهذا الأذن.

- The Electronic Communications Privacy Act of 1986 (ECPA) 18 U.S.C. §§ 3121–3127 (1994)[1].

---

[1] في عام 1986 أصدر الكونجرس الأمريكي قانون خصوصية الاتصالات الالكترونية ECPA المشار اليه أعلاه (Pup. L. No. 99-508,100 stat.1848) الذي تضمن في الفصل الأول منه Tit. I تعديل قانون الرقابة السلكية the Wiretap Act وهذا الأخير كان حتى تاريخ التعديل المشار اليه يتولى تنظيم رقابة المحادثات Oral والرقابة السلكية Wire لكي تمتد لتشمل بمقتضى تعديل ECPA رقابة الاتصالات الالكترونية أيضا. أما الباب الثاني من Tit. II ECPA فقد تضمن قانون الاتصالات المخزنة The Stored Communications Act SCA المقنن في الموسوعة الأمريكية في الباب 18 USC. Sec. 2701-2711 الذي يتولى تنظيم الدخول على الملفات والسجلات التي يتم اعدادها بواسطة الاتصالات الالكترونية. انظر هنا أيضا قضية ستيف جاكسون للألعاب:

- Steve Jackson Games v. US Secret Services. US App. 5th Cir. No. 93 – 8661 36 F.3d 457 Oct. 31, 1994 " As stated, the sole issue is a very narrow one: whether the seizure of a computer on which is stored private E-mail that has been sent to an electronic bulletin board, but not yet read (retrieved) by the recipients, constitutes an "intercept" proscribed by 18 U.S.C. Sec. 2511(1)(a). Section 2511 was enacted in 1968 as part of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, often referred to as the Federal Wiretap Act. Prior to the 1986 amendment by Title I of the ECPA, it covered only wire and oral communications. Title I of the ECPA extended that coverage to electronic communications. In relevant part, Sec. 2511(1)(a) proscribes "intentionally intercept[ing] ... any wire, oral, or electronic communication", unless the intercept is authorized by court order or by other exceptions not relevant here. Section 2520 authorizes, inter alia, persons whose electronic communications are intercepted in violation of Sec. 2511 to bring a civil action against the interceptor for actual damages, or for statutory damages of $10,000 per violation or $100 per day of the violation, whichever is greater. 18 U.S.C. Sec. 2520. The Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. Sec. 2510(4).

- An "electronic communication" is defined as:

any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whoole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include--

(A) the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;

(B) any wire or oral communication;

(C) any communication made through a tone-only paging device; or

ومجال هذا القانون هو أدوات التسجيل **Pen Register Devices** التي تسمح لهيئات الرقابة بتسجيل أرقام الهواتف التي يقوم المشتبه بهم بالاتصال بها وكذلك مصدر المكالمات التي يتم استقبالها من قبل هؤلاء المشتبه بهم، مثل أدوات معرفة رقم الطالب **ID caller Devices** (انظر تحديدا القسم **18 U.S.C. § 3127(3) (4) (1994)**). فمثلا تجميع ما هو غير المحتوى مثل أرقام الهواتف او عناوين حسابات البريد الالكتروني فقد تم تنظيمها بمقتضى قانون **Pen Register Statute, 18 USC Sec. 3121-27**. ويمكن القيام بإجراء المراقبة هنا استنادا الى أمر قضائي له علاقة مثل **Subpoena**.

وأساس عبارة **Pen Register** هنا هي أسم كان قد أطلق على تلك الأداة التي ابتكرتها شركة الهاتف في عام **1964** لمراقبة الهواتف، وبحيث يتم تركيبها في خطوط الهاتف. وكانت المهمة الأساسية لهذه الأداة هي إعداد سجل للأرقام التي يتم الاتصال بها من قبل مشترك ما في الهاتف، لذلك اعتبر هذا الأمر من الموضوعات التي تتناول العدوان على الخصوصية ومع ذلك فلم يصدر المشرع الامريكي قانون لهذه الأداة إلا في عام **1986** هو **Pen Register Act** الذي كان جزءا

(D) any communication from a tracking device (as defined in section 3117 of this title)....
18 U.S.C. Sec. 2510(12).
- Title I of the ECPA increased the statutory damages for unlawful interception from $1,000 to $10,000. See Bess v. Bess, 929 F.2d 1332, 1334 (8th Cir.1991). On the other hand, as noted, Title II authorizes an award of "the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case ... less than the sum of $1000". 18 U.S.C. Sec. 2707(c). As discussed, the individual appellants each received Title II statutory damages of $1,000.
- Wire and electronic communications are subject to different treatment under the Wiretap Act. The Act's exclusionary rule, 18 U.S.C. Sec. 2515, applies to the interception of wire communications, including such communications in electronic storage, see 18 U.S.C. Sec. 2510(1), but not to the interception of electronic communications. See 18 U.S.C. Sec. 2518(10)(a);
- Stored wire communications are subject to different treatment than stored electronic communications. Generally, a search warrant, rather than a court order, is required to obtain access to the contents of a stored electronic communication. See 18 U.S.C. Sec. 2703(a). But, compliance with the more stringent requirements of Sec. 2518, including obtaining a court order, is necessary to obtain access to a stored wire communication, because Sec. 2703 expressly applies only to stored electronic communications, not to stored wire communications. See James G. Carr, The Law of Electronic Surveillance, Sec. 4.10, at 4-126--4-127 (1994) (citing H.R.Rep. No. 99-647, 99th Cong., 2d Sess. 67-68 (1986)). “.

من قانون خصوصية الاتصالات الالكترونية هذا **ECPA** موضوعا في القسم **(a) 301** منه. ويسمح هذا القانون للسلطات بتجميع المعلومات بعد عرض الأمر على القضاء واستصدار أذن تفتيش من المحكمة وذلك في إطار معلومات الإرسال **To** والاستقبال **From** خلال مدة ستين يوما فقط. فمن حيث **To** يكون النظام المتبع هو نظام **Pen Register** أما من حيث نظام الاستقبال فيكون النظام المتبع هو نظام **Trap & Trace** وهذا الأخير يكون باستخدام أداة مختلفة عن أداة **Pen Register** يطلق عليها **Terminating Trap** كما قررت ذلك الدائرة الثالثة الفيدرالية في عام **1979**.[1]

---

[1] In re: IN THE MATTER OF THE APPLICATION OF THE UNITED STATES, FOR AN ORDER AUTHORIZING THE ROVING INTERCEPTION OF ORAL No. 02-15635 COMMUNICATIONS, D.C. No. CV-01-01495-LDG THE COMPANY, v. UNITED STATES OF AMERICA,.App.Filed November 18, 2003: "Section 2518 was first enacted as part of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351(1968). Title III of the Act, Wiretapping and Electronic Surveillance, has the dual goals of: "(1) protecting the privacy of wire and oral communications, and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized." S. Rep. No. 90-1097, at 66 (1968), reprinted in 1968 U.S.C.C.A.N. 2112, 2153. Title III therefore attempts to balance protecting the privacy interests of individuals with facilitating the investigation of crime, especially organized crime. Pub. L. No. 90-351, § 801 (1968); S. Rep. No. 90- 1097, at 66-73, reprinted in 1968 U.S.C.C.A.N. at 2153-63; see also Bartnicki v. Vopper, 532 U.S. 514, 523-24 (2001); Dalia v. United States, 441 U.S. 238, 252-53 & n.13 (1979) (citing S. Rep. No. 90-1097, at 70); United States v. Kalus- tian, 529 F.2d 585, 588 (9th Cir. 1975); Clifford S. Fishman & Anne T. McKenna, Wiretapping and Eavesdropping § 1.6 (2d ed. 1995).

"To assure the privacy of oral and wire communications, title III prohibits all wiretapping and electronic surveillance by persons other than duly authorized law enforcement officers." S. Rep. No. 90-1097, at 66, reprinted in 1968 U.S.C.C.A.N. at 2153. Law enforcement officers may only intercept communications after receiving "the authorization of a court order obtained after a showing and finding of probable cause." Id. Any person who illegally intercepts oral, wire, or electronic communications is subject to civil and criminal penalties. §§ 2511 & 2520. The statute prohibits the admission of most evidence obtained in violation of title III. § 2518(10)(a).

[2] The statute also has provided, since 1970, that certain enumerated entities and individuals must assist law enforcement in wiretapping or eavesdropping when directed by a court order to do so. See Pub. L. No. 91-358, § 211(b) (1970); § 2518(4). …….. Tracing allows law enforcement to determine the telephone numbers from which incoming calls originated. See In re Application of the United States for Order Authorizing Installation of Pen Register, Touch-tone Decoder, Terminating Trap, 610 F.2d 1148, 1152-53 (3d Cir. 1979).

"A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is

ويجب أن يكون تقديم الطلب من قبل عضو الادعاء (النيابة العامة) وأن يتم التصديق عليه من قبل قاض فيدرالي على أن يتضمن ما يشير الى أن المعلومات المستهدفة ذات علاقة بتحقيق جنائي مفتوح. ولا يترتب على انتهاك هذا القانون بطلان في الدليل وإن كان يحتمل وجود إدانة جنائية في هيئة جنحة مع الإدانة الأخلاقية استنادا الى أن ما تم تقديمه الى المحكمة من معلومات تعد معلومات غير صحيحة. والسؤال الذي كان مثارا حول هذا القانون هو مدى إمكانية إقامة علاقة بينه وبين الانترنت؟ ولقد كانت الإجابة المقتضبة آنذاك هي أن أغلب تكنولوجيا الانترنت هي تكنولوجيا اتصالات لذلك يمكن أن ينطبق هذا القانون على الانترنت. على انه لم يكن الأمر مطلقا هنا فقد قررت محكمة شمال كاليفورنيا/ سانت خوزيه في **17** نوفمبر **2000** في حكم غير معلن أن قانون **Pen Register** لا ينطبق على الانترنت نظرا لأنه يشير في نصوصه الى خطوط الهاتف التي لا يمكن أن تكون مجالا للتطبيق على الانترنت. فقد أشار الحكم الى أن ما يتطلبه قانون **Pen Register** هو ضرورة اشتمال أذن التفتيش على رقم الهاتف وكذلك موقع خط الهاتف، إذا كان معلوما، أي الخط محل طلب وضع أداة المراقبة فيه. ولما كان أذن مراقبة الانترنت لا يتضمن عبارة خط الهاتف فإن هذا أدعى الى القول بعدم إمكانية تطبيق هذا القانون على الانترنت. ولقد تم إهمال هذا الحكم من قبل الجهات الرسمية في الولايات المتحدة الامريكية[1] رغم أن هذا التشريع يعد سندا غير مباشر لإصدار القانون الوطني الأمريكي إزاء معادلة لزوم وجود برامج مراقبة وتعقب وتقصي تخص الانترنت بأقسامها مباشرة.

- The Communication Assistance for Law Enforcement Act of 1994 (CALEA)[2] 47 USC 1006 (b).

وفي هذا القانون الصادر عام **1994** تمت احاطة الاتصالات الهاتفية التقليدية وتلك التي تتم عبر الحواسيب بحماية معلوماتية بحيث يحظر هذا القانون الوصول الى معلومات عن المشترك

---

released. It does not overhear oral communications . . . .” United States v. N.Y. Tel. Co., 434 U.S. 159, 161 n.1 (1977).“.

[1] Orin S. Kerr- Internet Surveillance Law after The USA Patriot Act: The big brother that isn’t- GWU- Public Law & legal theory Working paper No. 043- Northwester Uni. School of Law, Northwestern Law Review Vol. 97 No. 2. (2003) p. 635, Founded at http://www.ssrn.com .

[2] Pub. L. No. 103-414, 108 Stat. 4279 (1994).

من خلال استخدام برامج تقصي ما دامت هذه المعلومات تخرج عن الغاية من التقصي والتفتيش[1].
ومن ثم فقد تم تقليص مسألة ضبط الجريمة العرضية في هذا القانون.

---

[1] **Testimony of Robert Corn-Revere, Hogan & Hartson L.L.P. before the Subcommittee on the Constitution of the Committee on the Judiciary United States House of Representatives The Fourth Amendment and the Internet April 6, 2000 http://www.house.gov/judiciary/corn0406.htm**
Also See: FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 In the Matter of: Communications Assistance for Law Enforcement Act Petition for Rulemaking under Sections 107 and 109 of the Communications Assistance for Law Enforcement Act, filed by Center for Democracy and Technology Joint Petition for Expedited Rulemaking, filed by Federal Bureau of Investigation and U.S. Department of Justice Petition for Rulemaking, filed by Telecommunications Industry Association CC Docket No. 97-213 May 20, 1998 "Congress enacted the Communications Assistance for Law Enforcement Act in 1994 in order to "preserve the government's ability . . . to intercept communications involving advanced technologies . . . while protecting the privacy of communications and without impeding the introduction of new technologies, features, and services.8 CALEA did not replace the basic statutory framework for authorization of wiretaps – which is contained in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"), as amended by the Electronic Communications Privacy Act of 1986 ("ECPA"). Rather, the purpose of CALEA was "to further define the industry duty to cooperate with wiretaps and to establish procedures based on public accountability and industry standards-setting.
Congress made it very clear in enacting CALEA that the statute was not driven by just one purpose, but involved a balancing of competing interests. In defining telecommunications industry duties under CALEA, Congress weighed the asserted needs of law enforcement against the interests of privacy, innovation and efficiency. Accordingly, Congress sought to balance three key policies: (1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies.
In interpreting CALEA, the Commission must be careful to balance the competing policies considered by Congress, rather than to focus only on satisfaction of the needs of law enforcement, as DOJ and FBI urge. The "hallmark" of CALEA, as FBI Director Freeh has testified, "is reasonableness." Another important, and unusual, aspect of CALEA is that there is no agency responsible for overall implementation of the statute. While the Commission plays certain important roles in implementation of CALEA, it is the telecommunications industry, in the first instance, that is responsible for adopting standards for design of networks that comply with the statute. Under CALEA, with regard to network design, "industry, not a government official, runs the show.
CALEA explicitly restricts the role of law enforcement in design of CALEA compliant networks. Law enforcement agencies are not authorized "to require the adoption of any specific design of equipment, facilities, services, features, or system configurations" or "to prohibit the adoption of any equipment, facility, service, or feature" by any telecommunications carrier or equipment manufacturer.16 Recently,

Senator Leahy, one of the original sponsors of CALEA, stated: "This law did not give a license to the FBI to redesign our telecommunications networks to suit its purposes." Indeed, FBI Director Freeh himself has stated that "law enforcement has no intention of becoming a technology czar or of regulating the development of new and beneficial telecommunications systems, services or features." provisions of CALEA at issue in this rulemaking proceeding – Sections 103 and 107 of the statute – make clear the general limitations on CALEA obligations imposed by Congress and the primary role of the telecommunications industry in implementation of CALEA. These provisions also carefully define the nature of the Commission's review, in a proceeding like the present one, of industry standards like JSTD- 025 that are adopted for CALEA compliance.

The affirmative obligations of CALEA at issue in this proceeding are the "assistance capability requirements" of Section 103 of CALEA.19 Under Section 103(a), telecommunications carriers must, to the extent "reasonably achievable," have the capability (1) to deliver the content of communications to law enforcement, (2) to deliver "reasonably available" call-identifying information to law enforcement, (3) to make such information available to law enforcement at remote locations, and (4) to protect the privacy of intercepted communications and the security of information regarding the interceptions. It is these requirements that J-STD-025 implements, and it is these requirements that are the basis of the DOJ/FBI Petition and the CDT Congress explicitly cautioned against "overbroad interpretation" of the assistance capability requirements of Section 103.22 "Carriers are required to comply [with assistance capability requirements] only with respect to services or facilities that provide a customer or subscriber with the ability to originate, terminate or direct communications." Furthermore, a carrier need only assist interception of communications which are in its control, a question which "will depend on the design of the service or feature at issue . . . ." In addition, if call-identifying information "is not reasonably available, the carrier does not have to modify its system to make it available."

Section 107 of CALEA26 provides the Commission's authority to consider the DOJ/FBI Petition and the CDT Petition. Section 107(a) contains a "safe harbor," providing that telecommunications carriers and equipment manufacturers are considered to be in compliance with the assistance capability requirements of Section 103 if they comply with "publicly available technical requirements or standards adopted by an industry association or standard-setting organization . . . to meet the requirements of section 103." Section 107(a) thus provides that telecommunications industry organizations, in the first instance, are responsible for setting standards that satisfy the requirements of Section 103 of CALEA.

Section 107(b) of CALEA gives the Commission authority to resolve disputes that arise where a government agency or other person believes that industry-adopted standards are "deficient." In considering such disputes, the Commission is required to evaluate factors relating to (1) cost-effectiveness, (2) protecting privacy and security of communications, (3) minimization of costs to ratepayers, and (4) encouraging provision of new technologies and services to the public. Thus, Section 107(b) explicitly indicates that the Commission's review of J-STD-025 must be based upon consideration of the various competing interests that Congress considered in adopting CALEA.

ومن الأهمية بمكان استدراك أنه كانت هناك عملية مزج تقوم بها **FBI** بين كل من قانون **ECPA** و قانون **CALEA** لكي تبرر نشاط كارنيفور بـ .. القانون[1].

- The Foreign Intelligence investigations act of 1978 (FISA) 50 U.S.C. sec. 1842.

المعادلة في سبب صدور هذا القانون كانت ممثلة في مدى إمكانية الاستفادة من التعديل الرابع للدستور الامريكي الذي يصون الحياة الخاصة ويحميها لكي يمكن استصدار أوامر تفتيش ومراقبة غير مرتبطة بالتحقيقات الجنائية وإنما بالإجراءات الأمنية والمخابراتية.

فقانون **FISA** هذا هو قانون التحقيقات الأمنية الخارجي الذي قام القانون الوطني الأمريكي بتنشيطه من حيث استحداث ارتباط تجديدي بعض الشيء في علاقات الآمن الخارجي والتحقيق الجنائي[2]، وذلك بالتوسع في صلاحيات رصد المعلومات حول الإرهاب والتجسس[3]، ومن ذلك ما هو

In sum, CALEA is a carefully-conceived statute that seeks to preserve a reasonably-focused ability of law enforcement to intercept the content of wire and electronic communications, as well as reasonably available associated call-identifying information, while not impairing the important interests of the public in privacy, reasonable telecommunications rates, and innovation. In considering the DOJ/FBI Petition and the CDT Petition, the Commission should carefully consider these statutory policies, as well as the defined standards of review imposed on the Commission by Sections 103 and 107 of CALEA.

[1] Anthony E. Orr – Marking carnivore's territory: rethinking pen registers on the internet (Note) – 8 Mich. Telecomm. Tech. L. Rev. 219 (2002), P. 221 available at http://www.mttlr.org/voleight/orr.pdf

[2] Charles Doyle - Terrorism: Section by Section Analysis of the USA PATRIOT Act, P. 17, Updated December 10, 2001, Order Code RL31200, American Law Division, also see to the author : The USA PATRIOT Act: A Legal Analysis, CRS Report for Congress , Received through the CRS Web, Order Code RL31377, April 15, 2002, Congressional Research Service,The Library of Congress P.12

[3] SEC. 218. FOREIGN INTELLIGENCE INFORMATION.
Sections 104(a)(7)(B) and section 303(a)(7)(B) (50 U.S.C. 1804(a)(7)(B) and 1823(a)(7)(B)) of the Foreign Intelligence Surveillance Act of 1978 are each amended by striking `the purpose' and inserting `a significant purpose'.

مقرر في القسم (3) (a) 214[1] من القانون الوطني الأمريكي الذي سمح للقائمين على تنفيذ قانون FISA بتجاوز ما هو مقرر في قانون ECPA من متطلبات حول تطبيق برامج Pen Registers .

[1] SEC. 214. PEN REGISTER AND TRAP AND TRACE AUTHORITY UNDER FISA.
(a) APPLICATIONS AND ORDERS- Section 402 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1842) is amended--
(1) in subsection (a)(1), by striking `for any investigation to gather foreign intelligence information or information concerning international terrorism' and inserting `for any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution';
(2) by amending subsection (c)(2) to read as follows:
`(2) a certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.';
(3) by striking subsection (c)(3); and
(4) by amending subsection (d)(2)(A) to read as follows:
`(A) shall specify--
`(i) the identity, if known, of the person who is the subject of the investigation;
`(ii) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;
`(iii) the attributes of the communications to which the order applies, such as the number or other identifier, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied and, in the case of a trap and trace device, the geographic limits of the trap and trace order.'.
(b) AUTHORIZATION DURING EMERGENCIES- Section 403 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1843) is amended--
(1) in subsection (a), by striking `foreign intelligence information or information concerning international terrorism' and inserting `foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution'; and
(2) in subsection (b)(1), by striking `foreign intelligence information or information concerning international terrorism' and inserting `foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such

ويتم الاستناد الى قانون **FISA** هذا حين مباشرة ثلاثة أشكال من الاجراءات[1]:

1- عند مباشرة إجراء التفتيش المادي، وهنا فإن هذا التفتيش وفق قانون **FISA** غير محكوم بما هو مقرر في القواعد الفيدرالية للإجراءات الجنائية وانما بما هو مقرر في القسم **18 USC Sec. 1821-29**.

2- عند القيام بإلزام الطرف الثالث بالكشف عن سجلات وأدلة مادية، فهنا لا يخضع هذا الاجراء لما هو مقرر في القواعد الفيدرالية للإجراءات الجنائية **(Subpoena)** وانما بما هو مقرر في القسم **18 USC Sec. 1861-62** والقسم **18 USC Sec. 2709**. ويلاحظ أن هذا الاجراء الثاني كان عرضة للجدل فيما يتعلق بالتمييز في تطلب أذن التفتيش والضبط **Subpoena** بين حالتي التحقيق الأمني والجنائي قبل حتى صدور القانون الوطني الامريكي.

3- عند القيام بإجراء مراقبة اتصالات تتم في الزمن الفعلي **Real-time** على شبكات الاتصالات. فالقسم **18 USC Sec. 1801-22** يتولى تنظيم الحصول على محتوى الاتصالات عوضا عما هو مقرر في قانون المراقبة **Wiretap Act** المتعلق بالجرائم، وكذلك القسم **18 USC Sec. 1841-45** يتولى تنظيم الحصول على البيانات التي لا تكون في ذاتها محتوى مثل رؤوس المراسلات **Headers** وذلك عوضا عن تطبيق قانون **Pen Register Statute** المتعلق بالجرائم.

---

investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution'.

[1] Testimony of Orin S. Kerr, Associate Professor, George Washington University Law School, United States Senate, Select Committee on Intelligence, Hearing on The USA Patriot Act February 19, 2005 "FISA covers the three basic authorities as follows: First, 18 U.S.C. §§ 1821-29 covers the authority to conduct physical searches, a parallel to the provision of the Federal Rules of Criminal Procedure that allows investigators to obtain a search warrant in criminal cases. Second, 18 U.S.C. §§ 1861-62 and 18 U.S.C. § 2709 covers authority to compel third-parties to disclose records and physical evidence, a parallel to the provision of the Federal Rules of Criminal Procedure that allows the issuance of subpoenas in criminal investigations. Third, 18 U.S.C. §§ 1801-22 and 18 U.S.C. §§ 1841-45 cover the authority to conduct real-time monitoring over communications networks. Specifically, sections 1801-22 cover the authority to obtain the contents of communications, a parallel to the Wiretap Act used in criminal cases, and sections 1841-45 cover the authority to obtain non-content information, a parallel to the Pen Register Statute used in crime investigations.".

- الأساس الدستوري للإجراءات قبل صدور القانون الوطني:

أما عن الأساس الدستوري الذي كان يتم الاستناد إليه- قبل صدور القانون الوطني- في عمل كارنيفور كبرنامج تقصي وتسجيل **Pen Register and trap and trace Device**[1]، فان **FBI** وجدت في قضية **Smith**[2] مقصدها، حيث انتهت المحكمة العليا الفيدرالية الامريكية في هذه القضية الى التقرير بان المشترك في خدمة الهاتف لا يحظى بحصانة التعديل الرابع للدستور الأمريكي[3] فيما يتعلق بخصوصية اتصالاته ولا يجب أن يتوقع مثل هذه الحصانة[4]، فلا يكون هناك خصوصية فيما يتعلق بالنبض الالكتروني **Electronic Impulses** عند الاتصال **Dialed** والإرسال **Transmission** عبر خطوط الهاتف لكي يتمكن للمشترك القيام بمكالمة هاتفية، وبناء على ما هو مقرر في القانون الجنائي فان **FBI** تؤكد أنها تحصل على أمر قضائي **Court order** حال قيامها بإنزال **Install** برنامج كارنيفور في شبكة ما.

---

[1] **وفقا للقانون الوطني الأمريكي فان التعريف الجديد لهذه الأدوات هو على النحو التالي:**

- a pen register is "device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication".

- A trap and trace device is defined as "a device or process which captures the incoming electronic or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication"

[2] **Smith v. Maryland, 442 U.S. 735 Supp. (1979)**

[3] **The Forth Amendment: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. ".**

[4] **"Telephone customers have no reasonable expectation of privacy in the electronic impulses dialed and transmitted over telephone lines to initiate a telephone call" See Anthony E. Orr – Marking carnivore's territory op cit**

بيد إن الأساس القانوني المذكور لم يكن كافيا لكي يحظى برنامج كارنيفور بأساس له لاختلاف طبيعة الاتصالات الهاتفية عن تلك التي تتم عبر الانترنت، لذلك استطال النقد استخدام **FBI** لهذا البرنامج[1]، استنادا الى أن المسألة فيما يبدو تتخذ بعدا جديدا في استحداث تقسيم بين مصطلحات **Surveillance** [2] و مصطلح **Interception** ، فالأول مصطلح جديد يمكن ان يحقق خطوات في مجال ردع أنشطة اجرامية بعينها وذلك باتخاذ تدابير وقائية سابقة على وقوعها (وهو ما يتولى تبريره القانون الوطني الأمريكي)، ومثل هذا الأمر يرفضه بشكل مطلق أنصار مدرسة الدفاع

---

[1] **انظر في بعض مظاهر هذا النقد**

Orin S. Kerr - DIGITAL EVIDENCE AND THE NEW CRIMINAL PROCEDURE - Columbia Law Review (Jan. 2005), This paper can be downloaded free of charge from the Social Science Research Network at: http://ssrn.com/abstract=594101

[2] **Nikos Bogolikos - Zeus E.E.I.G -The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception , EVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE OF ECONOMIC INFORMATION- Report by Working document for the STOA Panel, SCIENTIFIC AND TECHNOLOGICAL OPTIONS ASSESSMENT STOA - Luxembourg, October 1999 PE 168.184/Vol 5/5. Workplan Ref.: EP/IV/B/STOA/98/1401 Publisher: European Parliament Directorate General for Research Directorate A The STOA Programme. P.11. DEFINITIONS Surveillance is the systematic investigation or monitoring of the actions or communications of one or more persons. The basic born physical surveillance comprises watching (visual surveillance) and listening (aural surveillance). In addition to physical surveillance, several kinds of communications surveillance are practiced, including mail covers and telephone interception. The popular term electronic surveillance refers to both augmentations to physical surveillance (such as directional microphones and audio bugs) and to communication surveillance, particularly telephone taps. Data surveillance or Dataveillance is the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons. Dataveillance is of two kinds: "personal Dataveillance", where a particular person has been previously identified as being of interest, "mass Dataveillance", where a group or large population is monitored, in order to detect individuals of interest, and / or to deter people from stepping out of line. Surveillance technology systems are mechanisms, which can identify, monitor and track movements and data. Privacy is the interest that individuals have in sustaining a "personal space" free from interference by other people and organizations. Information privacy or data privacy is the interest an individual has in controlling, or at least significantly influencing the handling of data about themselves. 'Confidentiality is the legal duty of individuals who come into the procession of information about others, especially in the course of particular kinds of relationships with them'… Communication Intelligence (Comint).. defines Comint,,, as.. Comint is a large-scale industrial activity providing consumers with intelligence on diplomatic, economic and scientific developments.**

الاجتماعي الجديد. في حين يوجد لمصطلح **Interception** تقاليد قانونية عريقة في هذا الإطار منذ قانون المراقبة السلكية **The Wiretap Act** الذي تطبقه المحاكم بجدارة بعد تعديله بمقتضى قانون خصوصية الاتصالات الالكترونية **ECPA** في عام **1986**. وبين المصطلحين صراع خفي تدور رحاه في إطار النظام القانوني الأمريكي.

الفصل الثاني

الاجراءات في مرحلة ما بعد صدور القانون الوطني الامريكي

الى أن كانت أحداث **11** سبتمبر **2001** في الولايات المتحدة الامريكية حيث أصدر الكونجرس الأمريكي في دورته **107** القانون الوطني الأمريكي **The Patriot Act** في **26** أكتوبر **2001**.

- التعريف بالقانون الوطني الامريكي:

القانون الوطني الامريكي **The Patriot Act** هو القانون الصادر بعد أحداث **11** سبتمبر **2001**– حيث تم قصف مدن رئيسية في الولايات المتحدة الامريكية بالطائرات التجارية والمدنية– وهو القصف الذي نسب الى جهات اسلامية ذات طابع عسكري كان لها– في فترة زمنية سابقة– علاقات أساسية استخباراتية مع الولايات المتحدة ذاتها خاصة في مرحلة مكافحة الشيوعية واحتلال أفغانستان على يد القوى الشيوعية المنتهية ممثلة في الاتحاد السوفيتي.

يطلق على القانون الوطني الامريكي في المصطلح **Patriot Act** وهو اختصار تم انتقاؤه بعناية رسما للحروف الأولى للقانون المسمى باللغة الإنجليزية

The Uniting & strengthening America by Providing Appropriate Tools Required to Intercept & Obstruct Terrorism
Public law No. 107- 56, 115 Stat. 272

والاسم المختار لهذا القانون هو مزج لأسمي مشروعين وموضوعهما كان تقدم بهما أعضاء في كل من مجلس النواب ومجلس الشيوخ في الكونجرس:

- المشروع الأول لمجلس الشيوخ هو:

The Uniting & Strengthening America Act (The USA Act), Senate Bill No. 1510.

ولقد تم تقديم هذا المشروع في **4** أكتوبر واستغرقت المناقشات حوله سبعة أيام متوالية وتم التصويت عليه وحصل على **96** صوتا مقابل صوت واحد **(Senator Russ Feingold)**[1] في **11** اكتوبر **2001**.

- المشروع الثاني لمجلس النواب هو:

The " Provide Appropriate Tools Required To Intercept & Obstruct Terrorism Act". (The Patriot Act). H.R. Bill No. 2975.

تقديم هذا القانون الى المجلس في **2** أكتوبر واستغرقت المناقشات حوله عشرة أيام، وتم التصويت عليه وحصل على **337** صوتا في مقابل **79** صوتا في **12** اكتوبر **2001**.

وأما المشروع النهائي فقد بدأ في إعداده من خلال مشروع مجلس الشيوخ وتمت إضافة نصوص قررها مشروع مجلس النواب اليه بهدف استظهار قوة تضامن الاتحاد الفيدرالي الامريكي في مواجهة العدوان. ولقد تم عرض المشروع النهائي على مجلس النواب في **24** اكتوبر **2001** والموافقة عليه بـ... **356** صوتا في مقابل **66** صوتا. وتمت إحالته الى مجلس الشيوخ الذي وافق عليه بـ... **98** صوتا في مقابل صوت واحد في **25** اكتوبر **2001**. وقام الرئيس الامريكي جورج بوش الابن بالتصديق على هذا القانون في **26** اكتوبر **2001** ليصبح نافذا منذ ذاك التاريخ. وكانت عدد صفحات القانون **130** صفحة.

[1] **والحقيقة أن اعتراض السيد Russ Feingold كان سببه الرئيسي هو خوفه الكبير على المهاجرين ونحن نورد في الملاحق في نهاية هذا البحث شهادة السيد Feingold كاملة.**

- المصلحة في إقرار القانون الوطني:

إن المصلحة والقصد الأساسي من القانون الوطني الامريكي تتمثل في السير على نهجين أثنين:

1- السير على نهج مكافحة الارهاب الذي يمس الدول.

2- تقوية برنامج الولايات المتحدة لمكافحة الارهاب بتوسيع قاعدة المكافحة.

وإذا كان المجتمع الدولي يعترف بضرورة مكافحة الارهاب بصورة او اخرى، وهذا الامر محل اتفاق المجتمع الدولي ككل. فإن مسألة تقوية برنامج الولايات المتحدة الامريكية لمكافحة الارهاب له منطقه الخاص الذي نعرض له في هذه الورقة. فالسؤال هنا ما المقصود بتقوية برنامج الولايات المتحدة الامريكية لمكافحة الارهاب؟ وما تأثير ذلك على الارهاب الالكتروني او الرقمي الذي يتم عبر الانترنت ويقصد بالهدم والتدمير المجتمع المعلوماتي والعالم الافتراضي؟

يغطي القانون الوطني الامريكي طائفة كبيرة الموضوعات المتعلقة بمصطلح الارهاب دون أن يورد تعريفا محددا لهذا المصطلح كقاعدة عامة وإن كان قد أفرد لموضوعات اجرامية اعترف بعلاقتها بالإرهاب، مثل الدعم المالي للإرهاب **Terrorism Funds** وغسل الأموال **Money Laundering** والهجرة **Immigration** وحتى العقوبات الجنائية **Criminal Penalties**. ومن بين الموضوعات التي أثارها القانون الوطني هي إزالة الفصل بين السلطات المحلية كما هو الشأن في سلطات التحقيق الجنائي وبين السلطات الأمنية الخارجية[1].

وأما الباب الثاني من هذا القانون الذي يغطي موضوع المجتمع المعلوماتي فهو بعنوان **Enhanced Surveillance Procedures** الذي تم تقسيمه الى اثنين وعشرين قسما[2]

---

[1] **Seth F. Kreimer- Watching the Watchers: Surveillance, Transparency, and Political Freedom in the war on Terror- 7 U. Pa. J. Const. L. 133 (2004). (Vol. 7-1) P. 134.**

[2] **Uniting and Strengthening America Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Public Law 107-56. "An Act to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes"**

وهذه الأقسام هي:

TITLE II--ENHANCED SURVEILLANCE PROCEDURES

وضعت بقصد تقوية وضعية برنامج الولايات المتحدة لمكافحة الارهاب الالكتروني. حيث سمح هذا القانون بان يكون أساسا متينا لبرامج المراقبة والتقصي/ ومنها برامج **Pen Register** و **Trap & Trace Devices**، التي تبثها مؤسسات مختلفة ومنها مكتب التحقيقات الفيدرالي الأمريكي **FBI**. وبمقتضى القسم **216**[1] من هذا القانون تمت إزالة كافة القيود على إنزال مثل برامج التقصي

Sec. 201. Authority to intercept wire, oral, and electronic communications relating to terrorism.
Sec. 202. Authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offenses.
Sec. 203. Authority to share criminal investigative information.
Sec. 204. Clarification of intelligence exceptions from limitations on interception and disclosure of wire, oral, and electronic communications.
Sec. 205. Employment of translators by the Federal Bureau of Investigation.
Sec. 206. Roving surveillance authority under the Foreign Intelligence Surveillance Act of 1978.
Sec. 207. Duration of FISA surveillance of non-United States persons who are agents of a foreign power.
Sec. 208. Designation of judges.
Sec. 209. Seizure of voice-mail messages pursuant to warrants.
Sec. 210. Scope of subpoenas for records of electronic communications.
Sec. 211. Clarification of scope.
Sec. 212. Emergency disclosure of electronic communications to protect life and limb.
Sec. 213. Authority for delaying notice of the execution of a warrant.
Sec. 214. Pen register and trap and trace authority under FISA.
Sec. 215. Access to records and other items under the Foreign Intelligence Surveillance Act.
Sec. 216. Modification of authorities relating to use of pen registers and trap and trace devices.
Sec. 217. Interception of computer trespasser communications.
Sec. 218. Foreign intelligence information.
Sec. 219. Single-jurisdiction search warrants for terrorism.
Sec. 220. Nationwide service of search warrants for electronic evidence.
Sec. 221. Trade sanctions.
Sec. 222. Assistance to law enforcement agencies.
Sec. 223. Civil liability for certain unauthorized disclosures.
Sec. 224. Sunset.
Sec. 225. Immunity for compliance with FISA wiretap.

[1] **SEC. 216. MODIFICATION OF AUTHORITIES RELATING TO USE OF PEN REGISTERS AND TRAP AND TRACE DEVICES.**
(a) GENERAL LIMITATIONS- Section 3121(c) of title 18, United States Code, is amended--
(1) by inserting `or trap and trace device' after `pen register';
(2) by inserting `, routing, addressing,' after `dialing'; and

(3) by striking `call processing' and inserting `the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications'.
(b) ISSUANCE OF ORDERS-
(1) IN GENERAL- Section 3123(a) of title 18, United States Code, is amended to read as follows:
`(a) IN GENERAL-`
(1) ATTORNEY FOR THE GOVERNMENT- Upon an application made under section 3122(a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. The order, upon service of that order, shall apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order. Whenever such an order is served on any person or entity not specifically named in the order, upon request of such person or entity, the attorney for the Government or law enforcement or investigative officer that is serving the order shall provide written or electronic certification that the order applies to the person or entity being served.
`(2) STATE INVESTIGATIVE OR LAW ENFORCEMENT OFFICER- Upon an application made under section 3122(a)(2), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court, if the court finds that the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.
`(3)(A) Where the law enforcement agency implementing an ex parte order under this subsection seeks to do so by installing and using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public, the agency shall ensure that a record will be maintained which will identify--
`(i) any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network;
`(ii) the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information;
`(iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and
`(iv) any information which has been collected by the device.
To the extent that the pen register or trap and trace device can be set automatically to record this information electronically, the record shall be maintained electronically throughout the installation and use of such device.
`(B) The record maintained under subparagraph (A) shall be provided ex parte and under seal to the court which entered the ex parte order authorizing the installation and use of the device within 30 days after termination of the order (including any extensions thereof).'.

(2) CONTENTS OF ORDER- Section 3123(b)(1) of title 18, United States Code, is amended--
(A) in subparagraph (A)--
(i) by inserting `or other facility' after `telephone line'; and
(ii) by inserting before the semicolon at the end `or applied'; and
(B) by striking subparagraph (C) and inserting the following:
`(C) the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap and trace device under subsection (a)(2), the geographic limits of the order; and'.
(3) NONDISCLOSURE REQUIREMENTS- Section 3123(d)(2) of title 18, United States Code, is amended--
(A) by inserting `or other facility' after `the line'; and
(B) by striking `, or who has been ordered by the court' and inserting `or applied, or who is obligated by the order'.
(c) DEFINITIONS-
(1) COURT OF COMPETENT JURISDICTION- Section 3127(2) of title 18, United States Code, is amended by striking subparagraph (A) and inserting the following:
`(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals having jurisdiction over the offense being investigated; or'.
(2) PEN REGISTER- Section 3127(3) of title 18, United States Code, is amended--
(A) by striking `electronic or other impulses' and all that follows through `is attached' and inserting `dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication'; and
(B) by inserting `or process' after `device' each place it appears.
(3) TRAP AND TRACE DEVICE- Section 3127(4) of title 18, United States Code, is amended-
(A) by striking `of an instrument' and all that follows through the semicolon and inserting `or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication;'; and
(B) by inserting `or process' after `a device'.
(4) CONFORMING AMENDMENT- Section 3127(1) of title 18, United States Code, is amended-
(A) by striking `and'; and
(B) by inserting `, and `contents' after `electronic communication service'.
(5) TECHNICAL AMENDMENT- Section 3124(d) of title 18, United States Code, is amended by striking `the terms of'.
(6) CONFORMING AMENDMENT- Section 3124(b) of title 18, United States Code, is amended by inserting `or other facility' after `the appropriate line'.

والاتصالات عامة. ومن ذلك برنامج كارنيفور المشار اليه، فهذا البرنامج كما أشرنا الى ذلك أنفا يخضع لمعدلات البدائل هنا، فزعم المباحث الفيدرالية إن هناك إمكانيات هائلة في هذا البرنامج لم يتم الكشف عنها بعد[1] يعني في الحقيقة قابلية هذا البرنامج للتطوير وان عمله لن يكون في إطار ما هو موكل اليه فقط، وإنما سوف تقوم المباحث الفيدرالية الأمريكية والجهات الأمنية الاخرى في الولايات المتحدة بالتعاون فيما بينها بتطوير حركة الرقابة باستخدام ملكات التطوير التي تمنحها صناعة البرمجيات. فبدا الامر كما لو كان كل ما تحتاج اليه المباحث الفيدرالية والجهات الأمنية الاخرى هو تحديد نسق قانوني عام يتصف بالفاعلية ولا يقتصر على وقائع معينة حين الاستعانة بهذا البرنامج. فالحاجة هنا بدت واضحة في تقليص الدور البشري المتبع في هذا الشأن والذي وصل الى حد تجنيد الأطفال في هذا الإطار[2]، ليأخذ بعدا أخرا إلكترونيا ممثلا في تجنيد تكنولوجيا المعلومات للقيام بدور في مكافحة الاجرام.

ولقد كانت احد الوقائع التي حدت بالولايات المتحدة الامريكية وخاصة مكتب المباحث الفيدرالية الامريكية الى نهج هذا الاتجاه ذات سبب مقنع نوعا ما ممثلا في عدم الحصول على الدعم الكاف من الدول الأجنبية لردع الجريمة عبر الانترنت، ففي خريف عام **2000** نما الى علم المباحث الفيدرالية الامريكية حدوث اختراقات لشبكات مصرفية في الولايات المتحدة، وعند تعقب **Trace Back** المخترقين تبين ان نقطة الانطلاق **Back Source** هي شبكات في روسيا، وفشلت المباحث الفيدرالية في الحصول على مساعدة الشرطة الروسية لاستطلاع **Monitoring** هذه الشبكات وتعقب الأنشطة الإجرامية خلالها، وبعد الحصول على أمر تفتيش **Search Warrant** من الولايات المتحدة قامت المباحث الفيدرالية باستخدام **Sniffer** وهو نظام برمجي لمراقبة الشبكات **Network monitoring tool**[3] يسمح بالتوصل الى أسماء المستخدمين **Usernames**

---

[1] Catherine M. Barrett, FBI Internet Surveillance: The Need for a Natural Rights Application of the Fourth Amendment to Insure Internet Privacy, 8 RICH. J.L. & TECH. 16 (Spring 2002) at http://www.law.richmond.edu/jolt/v8i3/article16.html

[2] Darci G. Osther - JUVENILE INFORMANTS — A NECESSARY EVIL? , Washburn Law Journal [Vol. 39 – 1999] P. 108

[3] Honors Report, Active Network Security Theuns Verwoerd. 5 November, 1999, Supervisor: Ray Hunt P. 39

للشبكات وكلمات العبور **Passwords** ، بغرض التعرف على الهكرة ولقد أطلق على هذه العملية البوليسية تسمية تعبيرية ذات علاقة بمدلول إحداث السوابق هي **Remote cross-border searches and seizures** .[1]

ولم يقف الامر عند هذا الحد، فعملية المراقبة الالكترونية مستخدمة بكثافة في تتبع وتقصي الجريمة في الولايات المتحدة الامريكية. واذا كان موضوع المراقبة **Interception** تعني في منطقها المادي الاستمرار في الرؤيا والقدرة على تسجيل الاحداث بصمت، فان القدرات التي تمنحها تكنولوجيا المعلومات في هذا المجال تسمح بمفارقة كبرى تتغلب على تلك التي يقوم بها البشر، حيث يبدو التفوق هنا في عملية التسجيل الدقيقة لكافة الوقائع المراد تقصي موضوعها. لذلك سمحت تكنولوجيا المعلومات بظهور مصطلح جديد في نظرية القانون الجنائي/ التدابير الوقائية، هذا المصطلح هو **Electronic Surveillance** في معنى المراقبة الالكترونية الذي تطور الى مصطلح **Digital Surveillance** او المراقبة الرقمية التي تفيد تدخل الحوسبة والرقمية في التتبع والتقصي واقامة الشراك بقصد الكشف عن الجرائم وغيرها.

ولكن عملية التسجيل التي تقوم بها المؤسسات المفوضة بذلك او أي كان باستخدام ما هو متوافر في اطار تكنولوجيا المعلومات يصل بنا الى مسألة على درجة من الخطورة، ذلك انه من الممكن أن يقوم أي برنامج للتقصي **Sniffer** بدور البحث والتقصي والتسجيل بكل سهولة هنا، ولكن المفارقة التي تظل قائمة هنا هي مدى إمكانية برامج التقصي هذه في تمييز المراد تقصي تحركاته، فحتى الان فشلت هذه البرامج في إحداث ذلك التمييز. ويكمن السبب الرئيسي هنا في أن مسألة التتبع والتقصي الالكتروني او الرقمي يجب أن تكون معدة في مفهوم ضيق جدا لا يسمح بتوسع ما، ويتمثل هذا التضييق في ضرورة أن تنتهي حركة التقصي هذه الى الحاسوب او الشبكة الأساس التي أنطلق منها تنفيذ الجريمة فيما يعرف بمصطلح **Trace Back**. هذا في الوقت الذي لا يمكن حصر ارتكاب الجريمة في شخص معين لكون الجريمة بدأت من الحاسوب تحديدا وبما يعني أن مرتكب الجريمة يظل في إطار الاحتمالات التي تحتاج الى دعم مادي لتأييد نسبة الجريمة اليه. ولقد جعل مثل هذا الامر فكرة نسبة مصطلح المستخدم **User** الى الحاسوب (وليس للبشري العامل عليه) تتغلب حيث أفصح القضاء الأمريكي صراحة عن هذا الاتجاه معتبرا إن مصطلح المستخدم

[1] **Jack L. Goldsmith - The Internet and the Legitimacy of Remote Cross-Border Searches , University of Chicago Law School 2002**

تنسب الى الحاسوب دون غيره[1]. وهذا كله فضلا عن أن قوة الهكرة سمحت بفهم الآلية التي تعمل بها هذه البرامج بما يعني في النهاية إن صناعة تكنولوجيا المعلومات لا تزال في حاجة الى إثبات هوية التفوق البشري الممزوج بفكرة المتعة والسعادة، وهو التفوق الذي لا يمكن حصره في نطاق او حيز جغرافي معين، وبحيث بدا الامر ان علاقة الشيطان بالدكتور فاوست، في رواية أديب ألمانيا جوته، لن يكون لها وجودا على الإطلاق في المجتمع المعلوماتي، ذلك أن تكنولوجيا المعلومات لن تهب الانسان المتع كافة ، كذلك إن الانسان لن يصبح عبدا لأي نوع من المتع في المجتمع المعلوماتي/ العالم الافتراضي.

- تطور رؤية القانون الوطني:

كانت الوعود التشريعية بإقرار النص في القانون الوطني الامريكي قد قررت أن معظم النصوص الواردة في هذا القانون هي عرضة للإلغاء مع غروب شمس **2005**. ومثل هذا الامر حمل وعدا للشعب الامريكي والمجتمع الدولي قاطبة بأن الأزمة الطارئة التي تمر بها الولايات المتحدة الامريكية هي أزمة مؤقتة بالضرورة بسبب الإقرار التشريعي المذكور. ولم يتنبأ إلا قلة من فقه القانون المقارن بعدم مصداقية مثل هذا الالتزام التشريعي خاصة في ضوء تصريحات العديد من المسئولين في إدارة الرئيس بوش الابن بأهمية القانون الوطني الامريكي بالنسبة للفيدرالية وللولايات. وبدأت الأمور تتضح شيئا فشيئا مع تسريب نسخ من مشروع قانون وطني ثان **Patriot II** الى الصحافة مع وعود بأن يحل محل القانون الأصلي او الأول.

على أن الامر تطور فيما يبدو الى أبعد من ذلك فقد وجدت تصريحات يتم تداولها في نهاية العام **2005** توحي بعدم التزام الكونجرس بوعوده التشريعية. فالمسألة فيما يبدو أخذت منحى البحث في مدى أهمية القانون الوطني في حماية الولايات المتحدة بشكل يوحي بأن عدم وجوده كان قد يؤدي الى أكثر من كارثة قد تتفوق جسامتها على أحداث **11** سبتمبر **2001**.

---

1 **In re DOUBLECLICK INC. PRIVACY LITIGATION, Master File No. 00 Civ. 0641 (nrb) opinion and order by NAOMI REICE BUCHWALD US District judge, US District court southern district of New York March 28, 2001 P. 8 "It is important to note that the term "user" actually refers to a particular computer, not a particular person".**

تبدو رؤية استمرار القانون الوطني الأمريكي من خلال بحث القسم **203** منه، وهو القسم الذي يتضمن نقطة التعاون الملزم بين الجهات الأمنية سواء تلك التي تتولى الشئون الداخلية مثل مكتب التحقيقات الفيدرالي **FBI** والجهات الأمنية التي تتولى الأمن الخارجي مثل مركز المخابرات الخارجية **CIA**...الخ. إذ يسمح هذا القسم للجهات الأمنية المختلفة بالتعاون فيما بينها والدخول على نظم المعلومات الأمنية لكل منها. ومثل هذا التعاون الأمني يساهم بصورة كبيرة في مكافحة الاجرام ككل. وهو يبدو نظريا من الأمور الطبيعية حقيقة حيث يجب أن يكون هناك تعاون أمني في مكافحة الاجرام.

ولكن المشكلة التي تقابل وجود هذا النص أنه ليس هناك معايير قياسية يمكنها تحقيق معدلات المحافظة على الحقوق والحريات في إطار بحث نقطة التدابير الوقائية السابقة واللاحقة على وقوع الجريمة. فمثلا أن تعريف عبارة المعلومات الأمنية الخارجية **foreign intelligence information** الواردة في النص تأخذ الطابع الموسع شكلا وموضوعا[1]. كذلك يعطي هذا القسم صلاحيات للنائب العام الامريكي في تحديد المعلومات المتعلقة بنشاط المواطن الامريكي في الخارج التي يسمح بالكشف عنها وإخفاء تلك التي يرى عدم ضرورة الكشف عنها.

ولكن لا يعني منطق التطور هذا أن نصوص القانون الوطني هذه هي نصوص سيادية (رغم هيبتها الكبيرة). فالقانون المذكور ليس له قيمة سيادية فقد كان عرضة لمناقشات القضاء الامريكي من الناحية الدستورية. ففي **27** يناير **2004** قضت أحد المحاكم الفيدرالية في لوس انجلوس/ كاليفورنيا بعدم دستورية القسم **Sec. 805 (a) (2(B** الواردة القانون الوطني والتي تتضمن منع الحصول

---

[1] John Podesta- USA Patriot Act, The Good, the Bad, and the Sunset - American Bar Association- available at http://www.abanet.org/irr/hr/winter02/podesta.html Last Visited October 2005. "The definition of "foreign intelligence information" contained in the Patriot Act is quite broad. Foreign intelligence is defined to mean "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons or international terrorist activities." The definition goes on to specifically include information about a U.S. person that concerns a foreign power or foreign territory and "relates to the national defense or the security of the United States" or "the conduct of the foreign affairs of the United States." The sharing of such a broad range of information raises the specter of intelligence agencies, once again, collecting, profiling, and potentially harassing U.S. persons engaged in lawful, First Amendment-protected activities. ".

على رأي ومساعدة الخبراء في تحديد المنظمات الدولية للإرهاب وأن مثل هذا النص ينتهك التعديل الأول للدستور الامريكي[1]. حيث ردد القاضي **Audrey Collins** بأن هذا النص على درجة كبيرة من التوسع وبما يجعله غامضا في فحواه وقد يضر بالأبرياء هنا. وهذه الرؤية القضائية قد تكون دافعا كبيرا الى مزيد من البحث والتطوير في ثنايا القانون الوطني الأمريكي. فالصراع بين القضاء وبين المشرع في الولايات المتحدة الأمريكية قد بدأ باتجاه رصد القيمة الدستورية لتحركات السياسة التشريعية الامريكية.

كانت أحد نقاط تأييد استمرار وجود القانون الوطني هي تلك التي أشار اليها الفقه في عام **2005** من ان هذا القانون مفيد للتنظيم القانوني للانترنت من حيث أنه لم يتول فقط توسيع سلطات الأجهزة الحكومية في التعامل مع الارهاب وإنما أيضا ساهم بشكل كبير بالاعتراف بقانون الانترنت وتعديل العديد من التشريعات لكي تتواءم مع الانترنت. حيث تضمن هذا القانون ما يفيد إمكانية تعامل المشرع مع تكنولوجيا المعلومات والاتصالات والانترنت بشكل كبير وبصورة جعلت العديد من مناطق الاستفهام تتقلص لدى الفقه والقضاء. واذا كان هذا الرأي صحيح في الحقيقة من حيث تحقق مصلحة التقرير بالاعتراف بالتنظيم القانوني للانترنت اعترافا كاملا من قبل المشرع الأمريكي إلا أن هذا الاعتراف كان يمكن أن يتوافر في تشريع عادي، فلم تكن هناك حاجة لأن يكون هناك اعتراف بقانون الانترنت من خلال تشريع طوارىء هنا. إذ لدى هذا الاتجاه فإن منطق المساومة واضح المعالم في معنى أنه لكي يمكن للمشرع (الشعب) الاعتراف بقانون الانترنت او التنظيم القانوني للانترنت فإننا يجب أن نتنازل على مزيد من الصلاحيات لمصلحة الأجهزة الحكومية! فكأن الامر فيه مساومة بين الشعب والحكومة هنا!!.

---

[1] **Judge Strikes Down Part of USA PATRIOT Act. A federal judge has ruled that a provision of the USA PATRIOT Act that prohibits providing "expert advice or assistance" to designated international terrorist organizations violates the First and Fifth Amendments because it is overly vague. This is the first court decision striking down a provision of the controversial law. (Jan. 27, 2004) See: http://www.epic.org/privacy/terrorism/usapatriot/**
- See: In her ruling in Humanitarian Law Project v. Ashcroft, 2004 U.S. Dist. LEXIS 926 (C.D. Cal. 2004).
وكذلك قضى هذا الحكم بعدم دستورية الأقسام (302) و (303) من قانون The Antiterrorism & Effective Death Penalty Act AEDPA والتي تتعلق بزاوية الخبرة هذه.

الفصل الثالث

تطبيقات القانون الوطني الامريكي

المجال الحقيقي للقانون الوطني الامريكي يكمن في تقليص مجال الحق في الخصوصية تحديدا، وهو الحق المضمون دستورا في التعديل الرابع للدستور الأمريكي. فقد كان موضوع الخصوصية الى مرحلة ما قبل صدور القانون الوطني الأمريكي موضوعا نسبيا يقتصر الجدل فيه فيما قررته السوابق القضائية وما سوف ينتهي اليه قضاء الموضوع أيضا. وبالتالي كان الجدل مستمرا حول الخصوصية. ولما صدر القانون الوطني الأمريكي تم توسيع سلطات المراقبة والتقصي على حساب الخصوصية. هذا التوسع في الحقيقة أثار جدلا كبيرا ليس لكون هذا التشريع مخالف لحقوق الانسان فتلك مسألة يتنازعها صراع الديمقراطية والأمن على السواء وهي في مرحلة القانون الامريكي اعتبر هذا النزاع منهيا لمصلحة الأمن على حساب الديمقراطية تبعا لمبدأ المصلحة. وكما يطلق على هذا الامر في تقارير العدالة الجنائية مصطلح إزالة الجدار **The Wall** القائم بين السلطات المختلفة الأمنية والجنائية[1] في إشارة الى الحواجز التي كانت قائمة بين تلك السلطات في مرحلة ما قبل صدور القانون الوطني، على أن السؤال المثار هنا يسعى الى بحث موضوع مدى إمكانية وجود اختلاف بين الصلاحيات الأمنية والجنائية في إطار مأمورية الضبط القضائي وما إذا كانت السلطات الأمنية معزولة عن صفة الضبط القضائي في إطار البحث عن المعلومات وتقدير تبادل هذه المعلومات مع الجهات الجنائية والأمنية الاخرى.

والحقيقة أن الجدل المثار حول القانون الوطني الأمريكي كان أساسه مثار الفقه لموضوع سببية اعتراف المشرع الفيدرالي بإمكانية تطبيق معايير قديمة على الانترنت. إذ جل ما فعله المشرع الفيدرالي هنا هو التقرير بصحة انطباق التشريعات والنصوص التي تتناول مراقبة الهاتف على الانترنت! وفي هذا تراجع حقيقي للقيمة الحقيقية لتكنولوجيا المعلومات والاتصالات وتشبيه لها بالهاتف[2] على الرغم من أنه تقنيا هناك اختلاف كبير بين الهاتف والانترنت. يضاف الى ذلك أن مثل هذا الأمر كان فيه تراجع فقهي كبير في إطار الصراع المعاصر ما بين الاتجاه المجازي

---

[1] See: U.S. Department of Justice- REPORT FROM THE FIELD: THE USA PATRIOT ACT AT WORK- JULY 2004 p. 2

[2] Orin Kerr- Internet Surveillance Law after The USA Patriot Act: The big brother that isn't- Op Cit at 642.

والوظيفي في مدرسة التنظيم القانوني للانترنت. ففي الوقت الذي يجتهد فيه رجال القانون المقارن باتجاه إرساء معالم مطورة في إطار هذه المدرسة نجد مشرع أكبر دولة تقنية يتجه الى الدفاع عن اتجاه قديم أنصاره من قليلي الحيلة. ولهذا الأمر سلبيته الخطيرة على حركة حقوق الانسان. ويكفي الاشارة هنا الى التقرير بالمفارقة الكبيرة بين محتوى الهاتف (المحادثة الهاتفية او التراسل الصوتي) ومحتوى الانترنت (أنواع متعددة من المعلوماتية ومن بينها المحادثة المباشرة او التراسل المعلوماتي). فالقيمة الحقيقية للانترنت أنها جعلت من التراسل المعلوماتي تفوقا واضح المعالم عن التراسل الصوتي.

لقد أتى القانون الوطني الامريكي على تعديلات كبيرة في النظام القانوني الامريكي[1]. وفيما يلي نستعرض بعض التطبيقات التي تناولها الفقه في شأن ما ورد في القانون الوطني الامريكي من نصوص تتناول الأمن المعلوماتي:

- القسم **203** وتعديل قانون الاجراءات الجنائية الفيدرالي **Federal Rules of Criminal Procedure** : بمقتضى هذا القسم من القانون الوطني تم تعديل المادة **Rule 6(e)(3)(c)** من قانون الاجراءات الجنائية الفيدرالي إذا كان هناك معلومات (بالطبع سرية) قد تم الإفصاح عنها أثناء التحقيق الذي تقوم به هيئة المحلفين العليا **Grand Jury**. فمثل هكذا معلومات لم يكن القضاء يرضى بقبولها مطلقا إذا قدمت اليه دون أمر او إحالة منه. فنص المادة **203** الذي قام بتعديل

---

[1] **وهذه التشريعات هي:**

- **Wiretap Statute (Title III):**
- **Electronic Communications Privacy Act**
- **Computer Fraud and Abuse Act**
- **Foreign Intelligence Surveillance Act**
- **Family Education Rights and Privacy Act**
- **Pen Register and Trap and Trace Statute**
- **Money Laundering Act**
- **Immigration and Nationality Act**
- **Money Laundering Control Act**
- **Bank Secrecy Act**
- **Right to Financial Privacy Act**
- **Fair Credit Reporting Act**

See: http://www.epic.org/privacy/terrorism/usapatriot/

القسم **18 U.S.C. 2517** سمح بقبول هذه المعلومات وإحالتها الى الهيئات الأمنية للاختصاص اذا كانت هذه المعلومات ذات علاقة بالإرهاب او العمل المخابراتي[1].

[1] **See: U.S. Department of Justice- REPORT FROM THE FIELD: THE USA PATRIOT ACT AT WORK- JULY 2004. p. 8 "Section 203: Other provisions of the USA PATRIOT Act besides sections 218 and 504 have also facilitated the sharing of information between law enforcement and intelligence personnel. Before the USA PATRIOT Act, for example, federal law was interpreted generally to prohibit federal prosecutors from disclosing federal grand jury and wiretap information (including "wire, oral, or electronic communications") to intelligence and national defense officials even if that information indicated that terrorists were planning a future attack, unless such officials were assisting with the criminal investigation itself. Sections 203(a) and 203(b) of the USA PATRIOT Act, however, now allow for the dissemination of that information to assist federal law enforcement, intelligence, protective, immigration, national defense, and national security officials in the performance of their official duties, such as protecting the nation's security, even if their duties are unrelated to the criminal investigation. Section 203(d) further specifies that any foreign intelligence information obtained by investigators and prosecutors as part of a criminal investigation may be disclosed to such officials. The Department has made disclosures of vital information to the intelligence community and other federal officials under section 203 on many occasions. For instance, such disclosures have been used to support the revocation of visas of suspected terrorists and prevent their reentry into the United States, track terrorists' funding sources, and identify terrorist operatives overseas.**
The Attorney General issued guidelines in 2002 that establish procedures for carrying out these sharing provisions including, under section 203(c), for sharing grand jury and wiretap information that identifies a United States person with the Intelligence Community. These guidelines provide important safeguards to United States citizens identified in information disclosed to the Intelligence Community under the USA PATRIOT Act. These procedures require that precautions are taken to ensure the information is used appropriately. All such information must be labeled by law enforcement agencies before disclosure to intelligence agencies and must be handled by intelligence agencies pursuant to specific protocols.

Section 905
Additionally, section 905 of the USA PATRIOT Act requires all federal law enforcement agencies to disclose expeditiously to the Director of Central Intelligence any foreign intelligence acquired in the course of a criminal investigation. Section 905 makes such information sharing mandatory unless the Attorney General, after consultation with the Director of Central Intelligence, determines that disclosure of certain foreign intelligence would jeopardize an ongoing law enforcement investigation or impair other significant law enforcement interests. On September 23, 2002, the Attorney General released guidelines that formalized the sharing procedures and mechanisms for the Department of Justice and other federal law enforcement agencies that acquire foreign intelligence in the course of a criminal investigation.

– القسم **204** ومراقبة المراسلات الالكترونية (البريد الالكتروني): يتولى القسم **204** تعديل العنوان الثالث **Title III** وكذلك قانون الدخول على الاتصالات المخزنة **The Stored Communications Access Act** وبحيث يمكن للسلطات الوصول الى الاتصالات التراسل الصوتي والايميل من خلال أذن التفتيش عوضا عن الأوامر والأذون الاكثر صرامة. فالقسم **204** يتولى وضع التراسل الصوتي في اطار القسم **209** الذي يسمح بوجود أذن تفتيش ذي طبيعة فيدرالية وليس مقيدا بحدود معينة. على أنه تظل المراسلات المخزنة على شرائط أجهزة **Answering Machine Tap** خارج إطار تطبيق هذا القسم.

– القسم **206** من قانون **Foreign Intelligence Surveillance Act FISA**: يتولى قانون **FISA** تسهيل مهمة سلطات الأمن الداخلي عند تجميع المعلومات. ويتولى القسم **206** من القانون الوطني الامريكي تحديث الصلاحيات المقررة في قانون **FISA** هذا. ولما كان الكونجرس قد سمح– منذ العام **1986**– بمراقبة خصيصة التجوال **Roving Wiretap** في التحقيقات الجنائية شريطة الحصول على أذن المحكمة. ولم يكن قانون **FISA** في السابق يستلزم، لكي تتم مراقبة اتصالات كل شخص يعد هدفا لتحقيق جنائي، الحصول على أمر من المحكمة. فقد تم تعديل القسم **206** المشار اليه لكي تسري عليه القواعد المقررة هنا. فمن الناحية العملية فإن الفارق بين ما هو مقرر في التشريع الجنائي وبين ما جلبه القانون الوطني من تعديل: أنه في الاجراءات الجنائية كان القانون يستلزم وجود تأكيد بأن الشخص المستهدف من المراقبة يستخدم الالة الاتصالية (الهاتف النقال او المحمول) المستهدفة بالمراقبة، وفي هذا ما يضمن عدم الدخول على الهواتف الاخرى. ولقد تم تقرير هذا النص في قانون **FISA** الذي لم يكن له وجود فيه. فقد كان القانون في نصه القديم يستلزم تحديد الطرف الثالث مثلا لكي يمكن القيام بالمراقبة وبعد التعديل لم يعد تحديد الطرف الثالث أمرا لازما بل أضحى إمكانية القيام بالمراقبة من خلال أي طرف ثالث (كالمكتبات ومقاهي الانترنت ومزودي الخدمات بشكل عام) بل يمكن المراقبة من أطراف ثالثة متعددة في ذات الوقت.

ومن الأهمية بمكان هنا الاشارة الى أن البعض من الفقه الامريكي يرى في مسألة إلزام الطرف الثالث بالكشف عن المعلومات والبيانات ليس له علاقة بما هو مقرر في التعديل الرابع للدستور الامريكي المتعلق الخصوصية وإنما يمكن تبريره على المستوى الأمني بما هو مقرر في قضية **Miller** عام **1976** وبعض القضايا اللاحقة. وفي هذا ما يدعو الى التأكيد بأن هناك أساس دستوري يبرر القيام بإلزام الطرف الثالث كالمكتبات وبعض الجهات الاخرى بالكشف عن البيانات

المخزنة لديها للجهات الأمنية دون أن يكون في ذلك علاقة بما هو مقرر في التعديل الرابع المشار اليه[1].

– القسم **210** والتوسع في محتوى أذن تفتيش وضبط السجلات والاتصالات الالكترونية: كان القانون في السابق يسمح في أذن التفتيش **Subpoena** بالحصول على اسم المستخدم وعنوانه وسجل الاتصالات الهاتفية المحلية والدولية ورقم الهاتف من مزود خدمات الانترنت. وبعد صدور القانون الوطني قام المشرع الفيدرالي بمد نطاق موضوع أذن التفتيش بمقتضى القسم **210** لكي يشمل أيضا امكانية الحصول على معلومات سجلات الدخول على الانترنت وعدد مرات الدخول وكذلك أي عنوان مؤقت لشبكة ما وكذلك كافة طرق التي تم استخدامها لأداء مدفوعات مالية..الخ دون ان يكون الارهاب سببا للحصول على مثل هذه المعلومات.

---

[1] Testimony of Orin S. Kerr, Associate Professor, George Washington University Law School, United States Senate, Select Committee on Intelligence, Hearing on The USA Patriot Act February 19, 2005 Op cit "The constitutionality of orders to compel evidence without probable cause can be justified on two alternative grounds. The first is that the disclosure of information to third parties has been held to eliminate Fourth Amendment protection in that information. As the Supreme Court stated in United States v. Miller, 425 U.S. 435, 443 (1976): This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed. Under the disclosure rationale of Miller, third parties normally can be ordered to disclose records held by them without implicating the Fourth Amendment on the theory that the information was disclosed to them in the course of their coming into possession of the information."……

The rationale also applies to library records. For example, in Brown v. Johnston, 328 N.W.2d 510 (Iowa 1983), a library challenged a subpoena obtained by a state investigator who wanted to gather library circulation records to see if anyone had checked out books relating to cattle mutilation. The Iowa Supreme Court rejected the argument that an ordinary subpoena could not be used to collect library records: "It is true the State's investigation was only preliminary; and as Brown and the library board argue, no suspects were identified nor was the search for information limited to any named library patrons. This does not diminish the need for the information, however, as we assume the whole purpose in examining the record was to gain enough information so that the investigation could be narrowed. The State's interest in well-founded criminal charges and the fair administration of criminal justice must be held to override the claim of privilege here. Brown and the library board have cited no cases to us which have reached a contrary conclusion under similar facts, and we have found none. Id. at 513.".

– القسم **211** والتزام مزودو خدمات الانترنت بالإجراءات الأمنية: تولى القسم **211** من القانون الوطني الامريكي تعديل العنوان الثالث **Title III** قانون مراقبة الاتصالات لكي يقرر بضرورة التزام شركة مزود خدمات اتصالات او انترنت بالخضوع للقوانين التي تنظم المراقبة والكشف عن محتوى الاتصالات والتي قد يكون مصدرها شركات او مزودي خدمات الانترنت آخرين. وذلك وفقا لما هو مقرر في الباب **18 USC Ch. 119 (Title III) 121 & 206** وهي النصوص التي تنظم المراقبة والكشف عن محتوى الاتصالات السلكية او الشفوية او الالكترونية ومراقبة الهاتف وتعقب المكالمات والمعلومات في الزمن الفعلي ويشمل ذلك مراقبة الاتصالات المخزنة.

– القسم **213**: صلاحية القيام بتفتيش سري **Sneak & Peak**: سمح قانون خصوصية الاتصالات الالكترونية **ECPA** لعام **1986** للحكومة بسلطة تأخير أذن التفتيش في بعض أشكال الاتصالات الالكترونية التي هي في رعاية طرف ثالث. ولقد سمح القسم **213** من القانون الوطني بامتداد السلطة في تأخير الأذن الى كافة أشكال التفتيش المادية والرقمية شريطة أن يكون ذلك استنادا الى أن استصدار الأذن قد يؤدي الى نتائج عكسية **adverse result** [1] . والقسم **213** هذا لا يدخل في عداد النصوص التي التزام المشرع الفيدرالي بالغائها في نهاية عام **2005**.

– القسم **215**: هذا القسم يسمح لمكتب المباحث الفيدرالي **FBI** بالإلزام بإنتاج أية مواد مادية ذات علاقة بالعديد من التحقيقات المضادة للتجسس[2] والإرهاب. ومثله مثل العديد من نصوص القانون الوطني فإن هذا النص سوف ينتهي العمل به مع غروب شمس ديسمبر **2005** ما لم يتم التمسك به بمقتضى قانون آخر[3].

---

[1] The "adverse result" standard (defined in 18 U.S.C. § 2705.

[2] ذلك أن مكافحة التجسس من اختصاص الـ... FBI كما هو مقرر في قانون FISA. انظر في ذلك:
The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (Oct. 31, 2003) redacted version available at http://www.usdoj.gov/olp/nsiguidelines.pdf.

[3] Michael J. Woods- Counterintelligence and Access to Transactional Records: A Practical History of USA- PATRIOT Act Section 215- JOURNAL OF NATIONAL SECURITY LAW & POLICY [Vol. 1:37] P. 53 (The USA PATRIOT Act revisions to authorities governing counterintelligence access to transactional information are spread across three sections: §214 ("Pen register and trap and trace authority under

- القسم **217** ومراقبة اتصالات الهكرة:

Interception of "Computer Trespasser" Communications

كان المشرع قد حظر على أي شخص تعمد القيام بمراقبة او الكشف عن محتوى الاتصالات التي تخص أي كان بدون توافر الشروط التي يتطلبها قانون مراقبة الاتصالات **Wiretap Act** ، مع الأخذ في الاعتبار ما هو مقرر من استثناءات على النص المطلق المذكور. وبعد صدور القانون الوطني الأمريكي تقرر في القسم **217** منه استحداث استثناء جديد يُسمح بمقتضاه للسلطات بمراقبة اتصالات مخترقي ومنتهكي الحواسيب اذا كان مالك او حائز او مشغل الحاسوب المرتبط بالانترنت قد سمح بداية بالمراقبة. ولهذا الاستثناء الجديد المقرر في القسم **217** من القانون الوطني تطبيقات واسعة بحيث تقرر فيه أن الحاسوب المرتبط بالانترنت يشمل الحاسوب المستخدم فيما بين الولايات او في التجارة او الاتصالات الخارجية بما في ذلك الانترنت والتي تشمل أيضا الحاسوب وذلك بدون أذن قضائي على عكس ما هو مقرر في القوانين الفيدرالية الاخرى التي تتطلب تحديد المستهدف من المراقبة. فالاستثناء الجديد هنا يجعل تقدير وجود الهدف من المراقبة للسلطات ولمالك او لمشغل النظام.

كذلك يقنن القسم **217** من القانون الوطني الأمريكي حالة رضا الشخص بقيام السلطات بالدخول على جهاز الحاسوب دون حاجة الى أن يكون بيد السلطات أذن تفتيش. فيكتفي المشرع هنا برضا مالك او حائز الحاسوب. فهذا النص يسمح للسلطات بمراقبة جهاز الحاسوب الخاص بشخص ما بعد الحصول على موافقته. ويلاحظ أن نص القسم **217** يأخذ بالمفهوم الواسع لمنتهك الحاسوب **Computer Trespasser**. لكي تشمل كافة مظاهر العدوان بما في ذلك مراقبة من ينتهك

FISA"), §215 ("Access to records and other items under the Foreign Intelligence Surveillance Act"), and §505 ("Miscellaneous national security authorities"). The cumulative effect of these three sections is to make an across-the-board adjustment of the legal standard for access from "relevance" plus "specific and articulable facts giving reason to believe" the target was a foreign power or an agent of one, to simple "relevance" to an investigation to protect against international terrorism or clandestine intelligence activities (provided such an investigation of a U.S. person is not based solely on protected First Amendment activity).110 Section 505 also lowers the signature authority for the three types of FBI national security letters from Deputy Assistant Director to Special Agent in Charge.).

الاتفاقات التي تتم عبر الانترنت مع مزود خدمات الانترنت كما هو الشأن في امكانية مراقبة منتهك الاتفاق الذي يتم مع مزود خدمة ملفات موسيقى مثل **MP3**. ومما يشار اليه هنا ان هذا النص بسمح للسلطات بالمراقبة بناء على رضا صاحب او مالك او حائز الحاسوب ولكنه لم يحدد المدة التي تستمر فيها المراقبة وما اذا كانت السلطات تحتاج الى رضا واحد لكافة الحالات ام أنه يجب الحصول على موافقة ورضا حائز الحاسوب في كل حالة على حدة.

– القسم **218** : قبل صدور قانون **FISA** في عام **1978** لم تكن هناك سلطات واضحة ومحددة للجهات الأمنية والاستخباراتية تستطيع بموجبها القيام بمراقبة المواطنين والمنظمات في الولايات المتحدة الامريكية. ولقد ابتكر المشرع في هذا القانون محكمة خاصة تتولى التأكد من أن عمل الجهات الأمنية والاستخباراتية كان بغرض مراقبة الوصول الى معلومات أمنية خارجية. فهذه المحكمة الخاصة ذات الغرض الوحيد تعد محاولة لإقامة التوازن بين الحاجة لجمع المعلومات الخارجية بدون انتهاك الحقوق المقررة في التعديل الرابع للدستور الامريكي (انتهاك الحرمات) وكذلك المحافظة على ممارسة الأمريكيين لحرية التعبير المقررة في التعديل الأول للدستور. وبعد **11** سبتمبر **2001** أضحى الامر أكثر تعقيدا حيث سمح القانون الوطني لسلطات الولايات المتحدة الامريكية بتفتيش منازل المواطنين دون أن تكون هناك حاجة او سند الى سبب معقول يستدعي التفتيش. لذلك ينتقد الفقه هذا القسم كثيرا باعتباره يسيء الى سمعة النظام القانوني الامريكي.

– القسم **220** وامتداد نفاذ أوامر المراقبة وأذون التفتيش الى كافة أراضي الولايات المتحدة الامريكية: قبل صدور القانون الوطني كانت أذون التفتيش والمراقبة التي تصدر بناء على أمر قضائي يتم تنفيذها في إطار الاختصاص المكاني للمحكمة التي أصدرت الامر. ولقد تضمن القانون الوطني في القسمين **216** و**220** امتداد سلطان الاختصاص في تنفيذ تلك الأذون والأوامر بحيث سمح للمحاكم أن تأمر بتحميل أدوات المراقبة في كافة الأراضي الخاضعة للولايات المتحدة الامريكية. فقد تولى القسم **220** من القانون الوطني تعديل القواعد الفيدرالية للإجراءات الجنائية وبحيث يجوز للمحاكم بمقتضى هذا التعديل مد أذون التفتيش لتشمل أماكن خارج نطاقها المكاني أثناء التحقيق في جريمة إرهاب محلي او دولي.

– خاتمة: عندما نتناول بالحديث القانون الوطني الأمريكي فنحن في الحقيقة نتعرض لمدى التلامس الحادث بين الحق في الخصوصية التي يقدسها الانسان في الولايات المتحدة الأمريكية وبين توسيع

صلاحيات السلطات وتعددها التي يمكنها تجاوز هذا الحق لكي يتحقق لها تنفيذ برنامج مكافحة الارهاب كما تضع خطته الدولة الفيدرالية. وما بين المحافظة على الحق في الخصوصية وتبرير قيام السلطات بتجاوزه منطقة تفكير ما عدمت أنصارها على الإطلاق. فمسألة الحقوق والحريات والالتزامات الرقمية مسألة هامة في تاريخ التطور البشري، ويعد الحق في الخصوصية من أبرز الموضوعات فيها لأن المساس بحياة البشر الخاصة مسألة نسبية يعتريها غموض كبير، ولأجل هذا الغموض نجد البعض يسعى في تبرير وجود القانون الوطني الأمريكي من حيث أنه القانون الذي يربطنا بالعالم الافتراضي ويصحح مسار التشريعات التي كانت نافذة قبله، بل يذهب هذا الرأي الى القول إن الفضل في ربط النظام القانوني بالانترنت للقانون الوطني، فلولاه لما كان من الممكن التوسع في هذا الربط. والحقيقة أن بين الرأيين منطقة لن يتم فيها لقاء على الإطلاق فكأنما عملية تطوير النظام القانوني واتصاله بالرقمية لن يتأتى إلا بوجود ظروف طارئة وأنظمة تحكمها. ففي اتجاه تأييد القانون الوطني الأمريكي مبالغة كبيرة هنا لا يمكن قبولها بأي شكل من الأشكال. وذات الأمر يسري على مؤيدي رفض القانون الوطني الذين يرون فيه عدوان على حقوق الانسان، فهؤلاء يقررون أن القانون الوطني يشكل عدوانا كبيرا على الحق في الخصوصية الذي ضمن وجوده كمقيد للسلطات التعديل الرابع للدستور الفيدرالي. ولكن أي شكل من أشكال الخصوصية التي يتم العدوان عليها، فالخصوصية مصطلح مرن لا يمكن التنبوء بوجود معيار يميزه عن غيره، بل أن القضاء يتعامل مع ما هو مقرر في التعديل الرابع للدستور (الحق في الخصوصية) بكثير من الحذر وبشكل يقرر فيه في كل حالة على حده حتى تكون لديه مجموعة سوابق أخذها المواطن والفرد في الولايات المتحدة بعين الاعتبار ورتب عليها أموره الحياتية، وجاء القانون الوطني لكي يجعل الجميع هنا يعيد النظر في تلك السوابق.

..... انتهى

إعداد/ فرج بشير برنوص
ماجستير قانون جنائي (فرع قانون الانترنت)
خبير محلف فى الجرائم الافتراضية
2017م

وجيز
النظرية العامة
لقانون الانترنت

المحتويـات

الفصل الأول - نشأة الإنترنت

مقدمة

من أهم مميزات المجتمع المعلوماتي أنه قابل للتطور ومجال رحب لكل ما هو جديد دون قيود أو حدود للطموحات العلمية والتي عادة ما تبدأ بأفكار بسيطة. وهذا يؤكد القاعدة الأصولية في الشريعة الإسلامية وهي إحدى مفردات المنهج العلمي ونقصد بها مبدأ الحق في المعرفة، ولو بحثنا بشكل أعمق لوجدنا أن كل التطورات العلمية بدأت بأفكار لاقت التشجيع والدعم ولم تقابلها البيروقراطية الإدارية.

نشأة الانترنت :-

1 كانت إحدى نتائج الصراع على التفوق العالمي بعد الحروب العالمية في القرن العشرين، قيام الاتحاد السوفيتي القديم بإرسال القمر الصناعي SPUTNIK Space في عام 1957م مما وضع تلك الدولة المنتصرة في الحرب العالمية الثانية في موقع متقدم وهو الأمر الذي جعل الدولة المنافسة (الولايات المتحدة الأمريكية) في موقف محرج، والمهمة الأساسية لهذا القمر الصناعي كانت تمثل صيغة التفوق العالمي ذاتها، حيث تتمثل في قيام هذا القمر الصناعي بتحديد الأهداف بدقة جغرافية كبيرة، مما جعل كافة الأهداف العسكرية الأمريكية سهلة المنال، وعلى إثر ذلك اجتمعت القيادات العسكرية الأمريكية لتحديد المشكلة وتبين لها أن الضربة الأولى first strike هي صيغة التفوق الأولى للإتحاد السوفيتي ومن ثم على الولايات المتحدة الأمريكية أن تستقبل الضربة الأولى واستلزم الحال هنا تبعاً لذلك تحديد سؤال للرد على الضربة الأولى المذكورة.

وقررت القيادات العسكرية الأمريكية السؤال وهو. كيف يمكن استمرار التواصل بين مؤسسات الولايات المتحدة الأمريكية بعد الضربة الأولى ؟.

2 تمت إحالة السؤال المذكور إلى البنتاغون (وزارة الدفاع الأمريكية) وتحديداً إلى مكتب الدراسات المتطورة بالوزارة ARBA وكان هذا المكتب متعاقداً مع جمعية أهلية علمية هي راند RAND وكانت مهمتها إعداد الدراسات المستقبلية أثناء الحرب الباردة لإبراز تفوق الولايات المتحدة الأمريكية، وبالفعل قام مكتب ARBA بإحالة هذا السؤال إلى مؤسسة راند في تلك الأثناء كان هناك شاب يعمل مهندس كهرباء متدرب في شركة البوينغ للطائرات قدم استقالته والتحق بالعمل في مؤسسة RAND، المذكورة هذا الشاب المتدرب هو Paul Baran - حيث تم تكليفه بالإجابة على هذا التساؤل.. واستغرقت الإجابة منه الفترة من9591م وحتى1964م.

وفي عام 1964م – وضع Paul Baran تقرير بعنوان الاتصالات الموزعةon Distributed communicationsقام بإيداعه وتسجيله باسمه في مكتبة الكونجرس حفاظاً على حقوق الملكية الفكرية، ويتضمن هذا التقرير إمكانية استمرار التواصل بين مؤسسات الولايات المتحدة الأمريكية على الرغم من الضربة الأولى.

وذلك باستخدام نظام الشبكات الإلكترونية والرقمية، وكان أهم ما لوحظ في هذا التقرير استشراف Paul Baran للمستقبل حيث «قرر أنه في يوم ما سوف يكون مطلب الإنسان كفاءة أكثر للتواصل ألمعلوماتي من تلك الكفاءة المتطلبة في التراسل الصوتي».. ولقد صدق فعلاً .

3 وفي سنة 1967م وضع الدكتور (john Postel) نظام نطاق الأسماء Domain Nama System و التي تعرف اختصاراً DNS عبر الانترنت من اجل تنظيم حركة المواقع والوصول إليها , وقام بوضع الهيكلية النظرية لمنظمة تحديد الأسماء والأرقام عبر الانترنت.

4 أو ما يعرف اختصاراً باسم الإيكان Internet Corporation for Assigned Names and Numbers ICANN, ولذلك قصة أخرى سوف نعرض لها في عدد قادم. ولكن مما تجدر الإشارة إليه أن موضوع نطاق الأسماء من الموضوعات الكبيرة التي تداخلت فيها السياسة الدولية والصراعات الاقتصادية بين الدول ووصلت إلى حد وجود انقسام في تحديد شركاء المجتمع المعلوماتي حيث انقسم أصحاب الشراكة إلى أربعة أقسام:-

- القطاع الخاص.
- القطاع الدولي (المنظمات الدولية).
- قطاع المجتمع المدني.
- القطاع الحكومي.

وذلك على إثر القمة الثانية للمجتمع المعلوماتي – تونس 2005م World Summit on information society و التي تعرف اختصارا WSIS. وكان مبنى الخلاف يدور حول اقتصاديات نطاق الأسماء كعلامة مسجلة من حيث مدى إمكانية تطبيق تشريعات العلامة التجارية عليها.

5 سنة 1969م وضع Kenneth Thompson وكان عمره 25 سنة نظام التشغيل الحر UNIX والذي يمكنه استيعاب حركة المعاملات المعلوماتية الضخمة.

6 سنة 1970م وضع Kenneth Thompson لغةB و اضطر صديقه Dennis Ritchie إلي تطوير نظام التشغيل UNIX ليتماشى مع اللغة الجديدة B.

7 سنة 1971 م اخترع Ray Tomlinson مصادفة البريد الالكتروني Electronic Mail عندما مزج بروتوكولات مع بعضها ضمن برنامج يسمى SND-MSG و وضع له علامته الشهيرة @ التي أصبحت إشارة تقليدية لاستخدامات البريد الالكتروني و كانت اول رسالة يتم تجربتها عشوائية حسب حروف لوحة مفاتيح الحاسوب الاولي QWERTYUIOP و أصبح يعرف اختصارا E-mail.

8 خلال سنة 1972 م وضع Dennis Ritchie لغة البرمجة الشهيرة C.

9 خلال سنة 1972م انعقد مؤتمر التكنولوجيا في الولايات المتحدة الأمريكية حيث طرح فيه كلٌ من Vinton Cerf وRobert Kahn النظام الحزمي و لأول مرة TCP/IP الذي يمثل النظام التراسلي الذي اعترف به النظام القانوني المقارن كأساس في قانون الانترنت. حيث أن القاعدة تقرر ان القواعد

القانونية تطبق على النظام التراسلي ولا تطبق على نظام التخزين إلا إذا وجد نص صريح يخالف ذلك.

10 خلال سنة 1980م فكر مهندس الاتصالات الانجليزي Tim Burners Lee خريج جامعة اكسفورد عندما يأس من كثرة مفكراته وتعددها في وضع برنامج يساعده على تنظيمها في الحاسوب مستخدما أفكار Ted Nilson مبتكر الخطوط النشطة الدالة وتصادف أن وجد Lee نفسه أمام شبكة المعلومات الدولية World Wide Web والتي تعرف اختصاراً WWW او W3 فأطلقها كمشاع للإنسانية من معهد سيرن Cern بسويسرا كان ذلك سنة 1991م.

11 وخلال سنة 1990م وضع المهندس James Gosling الكندي لغة Java جافا والتي بدأت إرهاصتها بمسمى Oak كجزء من المشروع الأخضر Green Project في شركة Sun Microsystems وانتهت سنة 1994م بلغة عالية المستوى.

12. وخلال سنة 1991م تمكن Linus Torvalds كان طالباً بجامعة هلسنكي / فلندا - من وضع نظام تشغيل Linux تطبيقاً لمبدأ البرمجة الحرة Free software كما يطلق عليه فقه حقوق الملكية الفكرية.

13 وخلال سنة 1994م فكر الشابان Jerry yang – David filo وهما طالبان بقصد إحداث تفاعل واعي مع شبكة المعلومات الدولية W.W.W وهي فكرة الرئيس بوش في برنامج الانتخابات ولتسهيل الوصول إلي المعلومة توصلا إلي عرض فكرة قواعد البيانات وهي تقترب من المنهج الموسوعي وهو منطقة جديدة على الفكر الغربي من عناوين كبرى إلي تفريعات تربط بموضوعات وهو الأسلوب الذي وضعه الموسوعي العربي الليبي الأستاذ المرحوم / محمد أبوبكر بن يونس رحمه الله في عام 1962م في إطار موسوعة التشريعات العربية. و اختار الشابان أسم الموقع (Yet Another Hierarchical Office Oracle) وتم اختصاره إلي (Yahoo) الذي يعتبر من أشهر مواقع البحث الاجتماعية الان.

ونتيجة لهذه الخطوات العلمية والسريعة لتطور الإنترنت جاء في تقرير الأمين العام للأمم المتحدة سنة 2000م السيد كوفي عنان أهمه (أن المذياع أستغرق وصوله إلي 50 مليون شخص 38 سنة وأستغرق التلفاز 13 سنة أما الإنترنت فقد أستغرق وصولها إلي 50 مليون شخص أربعة سنوات فقط وخلال سنة 1993م كانت عدد الصفحات 50 صفحة على الشبكة أما خلال سنة 2000م (تاريخ كتابة التقرير) فهو 50 مليون صفحة، وكان عدد المرتبطين بالشبكة خلال 1998م 143 مليون شخص وسيرتفع العدد خلال سنة 2001م إلي 700 مليون شخص وأما مستوى الإنترنت في مجال التجارة الإلكترونية فقد كانت خلال سنة 1996م 2,6 مليون دولار وخلال سنة 2002م 300 مليون دولا(. (انتهى التقرير)

ويتوقع بنهاية سنة 2010م حسب الإحصاءات المتوقعة أن يتجاوز عدد مستخدمي الإنترنت إلي 2

مليار شخص وهو ما يعادل تقريباً ثلث سكان العالم تقريباً.

ولكن هل هناك قرار سياسي ليبي اتجاه ظاهرة الانترنت؟هذا ما سنعرضه في الفصل الثاني.

الفصل الثاني

القرار السياسي الليبي اتجاه الانترنت

ولقد برزت مصداقية هذا التقرير في تبني القرار السياسي لعديد من دول العالم. منها ذلك قرار الرئاسي في دولة التشيلي وأغلب دول العالم والأمم المتحدة، أما فى ليبيا فقد برزت مظاهر هذا القرار فى عدة أحداث ومناسبات نذكر منها :-

1 مؤتمرا وزراء الأعلام الأفارقة بمدينة طرابلس– يوم 1999/11/4م. حيث أكدت ليبيا على أهمية ثورة الاتصالات والمواصلات ويجب إلا نبقى في حالة دفاع بل سنتحول إلى حالة تقدمويجب أن نحرص على أدجال كل البيانات إلى الانترنت «

2 الجلسة الافتتاحية لمؤتمر الشعب العام سرت-يوم2000/1/28م, وما دار فيها من نقاش كان أهمها أن هناك عصر جديد والزمن قد تغير».

3 الجلسة الافتتاحية لفعاليات الندوة الدولية حول أفاق الاستثمار والتجارة والتي عقدت بمدينة طرابلس بتاريخ 1999/9/2-»حيث دار النقاش على ان الانترنت هذه فرضت نفسها مهما حاولت الدول والحكومات من وضع قيود واشتراطات والتضييق عليها لكن في النهاية القبضة الحديدية ستتحطم مهما كانت قوية أمام هذه الظاهرة « وان لا يجب الوقوف ضد كل هذه المعطيات الحديثة من الأقمار الصناعية إلى الانترنت إلى التقنية إلى حرية التجارة كذلك أهمية البحث العلمي فى عصر الانترنت» .

4 الجلسة الافتتاحية لمؤتمر وزراء الأعلام الأفارقة أكدت ليبيا على حقوق الإنسان وحرية التعبير وكافة الحريات الإنسانية الاخري ولا يمكن لأي شخص أن يملي عليك ما تكتب أو تقرأ. «

5 المحاضرة السياسية بكلية الاقتصاد والعلوم السياسية بالجامعة الليبية بطرابلس بتاريخ 1999/12/27م , وما دار فيها من نقاش حول عدم استطاعتنا تجاهل العالم الآن وهو يتحول بشكل خطير ويمسنا وسيؤثر على حياتنا ولا تستطيع أن تغض النظر وندعي أن هذه التقنية لا تهمك وهي أشياء مؤثره جداً تبدأ من الإذاعة المرئية من الانترنت إلى الهواتف وغيرها».

6 ومجال الاقتصاد أن ابرز معالم القرار السياسي الليبي اهتماماته بالسياسات الاقتصادية وربطها بالاقتصاد الرقمي وكان ذلك في الجلسة الافتتاحية لفعاليات الندوة الدولية حول أفاق الاستثمار والتجارة المنعقدة بمدينة طرابلس –بتاريخ 1999/9/2م وكان أهم ملامح هذا القرار « العقل الآلي والتقنية الفائقة ستبدأ بوجود نشاط اقتصادي بدون بشر وبدون عمال».

7 فتح سوق العمل عبر الانترنت واتخاذ القرار الأحداث الذي تظهر به ليبيا بمظهر الدولة التي تجعل من الانترنت جزء من نسيجها الاجتماعي والاقتصادي بقيام الخبرات الليبية بتطوير تقنية المعلومات وصولاً إلى الظاهرة لإبراز الانترنت فائق السرعة Wi Max كخدمة للمجتمع الليبي.

8.الجلسة لافتتاحية لمؤتمر الشعب العام سرت بتاريخ 2000/1/28م. وفي مجال الإدارة الإلكترونية أكد القرار السياسي الليبي على أن» الآلات تخدم نيابة عن البشر ولم يعد هناك موظفون في العالم. بل هو عدد قليل من المبرمجين ويكونون خبراء وعلماء وفنيين , « .

9.وكان للقرار السياسي الليبي فى مجال الانترنت والإدارة الالكترونية أثر فعال حيث صدرت حزمة من التشريعات ذات العلاقة بقانون الانترنت وأقسامه المختلفة أي إنها بعبارة أدق تطبيق مباشر لقانون الانترنت حيث اعترف المشرع الليبي بمبدأ الرقمية كمنهج ويعني مبدأ الرقمية منهج هو تداخل الرقمية أو قدرة المجتمع على تقبل الرقمية في النسيج الاجتماعي والاقتصادي وهذا ما كان واضحاً من خلال إصدار مجموعة من التشريعات الليبية سنتعرض لها في الفصل الثالث من هذا البحث.

بعد أن تناولنا القرار السياسي الليبي اتجاه الانترنت نظرياً. هل هناك تطبيقات في نظام القانون الليبي من الناحية العملية. هذا ما سنعرفه في الفصل الثالث.

الفصل الثالث

تطبيقات الانترنت في النظام القانون الليبي

تطرقنا إلى اعتراف المشرع الليبي بالحوسبة والرقمية كمنهج وانه صدرت حزمة من التشريعات وهي كالآتي:-

أولاً/ القانون رقم (1) 2005م، بشأن المصارف حيث تنص المادة (97) منه على الأتي:-

-تسري على المصارف أحكام القانونيين المدني والتجاري , وذلك بالقدر الذي لا يتعارض مع أحكام هذا

القانون.

-يُعتد بالمستندات والتوقيعات الالكترونية، التي تتم في المعاملات المصرفية وما يتصل بها من معاملات أخرى، وتكون لها الحجية في إثبات ما تتضمنه من بيانات.

-تعتبر مخرجات الحاسوب، المتعلقة بالمعاملات المصرفية، وفقاً للمنصوص عليه في الفقرة السابقة،

بمثابة الدفاتر القانونية المنصوص عليها في القانون التجاري والقوانين المكملة له وللمصارف أن تحتفظ للمدة المقررة في القانون بنسخ مصغرة على أقراص صلبة أو مرنة أو مضغوطة أو على غير ذلك من الأدوات التقنية الحديثة في مجال حفظ البيانات أو المعلومات، بدلا من أصول الدفاتر والسجلات والكشوفات والوثائق والمراسلات والبرقيات والإشعارات، وغيرها من الأوراق المتصلة بأعمالها , وتكون لهذه النسخ المصغرة حجية الأصل في الإثبات).

ثانياً/القانون رقم 11 لسنة 2010م. بشأن سوق المال حيث تنص المادة (74) علي الأتي : -

(يتم التداول بالسوق الكترونيا وذلك من خلال الربط بين المقر الرئيسي والفروع ويحدد مجلس

إدارة السوق الاشتراطات اللازمة بشان الشركات التي تطرح أسهمها للاكتتاب من خلال سوق الإصدار، و تنص المادة (95) علي الأتي: -

يكون للتوقيع الالكتروني قيمة التوقيع العادي إذا توافرت فيه الضوابط التالية:

أ-ارتباط التوقيع الالكتروني بالموقع دون غيره.

ب-سيطرة الموقع وحده على الوسيط الالكتروني.

ت-إمكانية كشف أي تعديل أو تبديل في بيانات الوثيقة الالكترونية أو التوقيع الالكتروني.

ث-مراعاة الضوابط الفنية والتقنية اللازمة التي تحدد بلائحة تصدرها اللجنة الشعبية العامة بناء على عرض من الهيئة.

وتنص المادة (96) علي الاتي :-

1 تعتبر المستندات الالكترونية التي تتم في إطار معاملات الهيئة وشركة سوق المال الليبي وغيرها من الجهات المصدرة والعاملة بالسوق المالي وما يتصل بها من معاملات حجة في إثبات ما تتضمنه من بيانات.

2 تعتبر مخرجات الحاسوب المتعلقة بمعاملات الهيئة والسوق وغيرها من الجهات العاملة في السوق المالي وفقا لما هو منصوص عليه في الفقرة السابقة بمثابة الدفاتر القانونية المنصوص عليها في قانون النشاط التجاري.

1 على الهيئة والسوق أن تحتفظ للمدة المقررة في القانون بنسخ مصغرة على أقراص صلبة أو مرنة أو مضغوطة أو على غير ذلك من الأدوات التقنية الحديثة في مجال حفظ البيانات والمعلومات بدلا من أصول الدفاتر والسجلات والكشوفات والوثائق والمراسلات والبرقيات والإشعارات وغيرها من الأوراق المتصلة بأعمالها وتكون لهذه النسخ المصغرة حجية الأصل في الإثبات. وتحدد القرارات الصادرة من الهيئة الضوابط الفنية والتقنية اللازمة لذلك).

ثالثاً/قانون علاقات العمل رقم 12 لسنة 2010م. حيث تنص المادة (179) علي الأتي:-

(تكون الاختراعات التي يبتكرها الموظف أثناء تأدية وظيفته أو بسببها ملكا للدولة في الأحوال التالية:

1. إذا كان الاختراع نتيجة تجارب في موقع عمل الموظف.
2. إذا كان الاختراع داخل نطاق واجبات الوظيفة.
3. إذا كان للاختراع صلة بالشؤون الأمنية للدولة.

وفي جميع الأحوال يكون للموظف الحق في مكافأة يراعي في تقديرها تشجيع البحث والاختراع).

رابعاً/قانون الجمارك رقم (10) لسنة 2010م. حيث تنص المادة (50) علي الأتي:-

(لموظفي الجمارك حق الاطلاع على جميع الدفاتر والوثائق والمستندات المتعلقة بالعمليات الجمركية التي تخص مجال عمل كل من:

1. شركات الملاحة البحرية والوكلاء البحريين وممولي السفن والوسطاء البحريين.
2. شركات الملاحة الجوية.

3. شركات النقل البري.
4. الوكالات بما فيها وكالات النقل السريع التي تتكفل بقبول الطرود وجمعها وإرسالها.
5. المخلصين الجمركيين ومتعهدي العبور.
6. المستودعات والمخازن البحرية والمخازن العامة.
7. المخازن والحظائر الجمركية المعدة للتصدير والاستيراد.
8. محطات السكك الحديدية.
9. أي أشخاص طبيعيين أو اعتباريين يصدر بتحديدهم قرار من الأمين.

وعلى المعنيين الاحتفاظ بالوثائق المذكورة في الفقرة الأولى مدة لا تقل عن خمس سنوات، وفي حالة انجاز هذه الوثائق بالوسائل الالكترونية والتطبيقات والمنظومات الإعلامية وكذلك المنظومات والمعلومات اللازمة لتشغيلها، على موظفي الجمارك تسليم قائمة بما تم حجزه لهؤلاء الأشخاص والشركات).

خامساً/ قانون التسجيل العقاري وأملاك الدولة رقم (17) لسنة 2010 حيث تنص المادة (71) علي الأتي:-

(تتمتع الكتابة الالكترونية بنفس قوة الكتابة العادية الموضوعة على دعامة ورقية متى استوفت الشروط التالية:

1. ارتباط التوقيع الالكتروني بالموقع دون غيره.
2. سيطرة الموقع وحده على الوسيط الالكتروني.
3. إمكانية كشف الضوابط الفنية اللازمة التي تحدد بلائحة من الجهة المختصة.

وتكون لصورة المحرر الالكتروني الرسمي نفس حجية الأصل ما دامت مطابقة لأصله وكان هذا المحرر والتوقيع الالكتروني محفوظين على الدعامة الالكترونية على نحو يضمن الرجوع إليهما بشكل مباشر).

سادساً/القانون رقم (20) لسنة 2010م. بشأن نظام التأمين الصحي، حيث تنص المادة (12) علي الأتي:-

(تلتزم المصحة الايوائيه باعتماد نظام الملف الطبي لكل مريض، وعلى كل مؤسسة طبية تقدم خدماتها وفقا لأحكام هذا القانون أن تتبادل الملفات الخاصة بالمرضي لديها، كما لها ان تتبادل المعلومات فيما بينها بالوسائل الالكترونية).

سابعاً /القانون رقم (22) لسنة 2010م. بشأن الاتصالات، حيث تنص المادة (35) علي الأتي:-

(يعاقب بالحبس مدة لا تقل عن ستة اشهر وبغرامة لا تقل عن ثلاثة ألاف دينار ولا تزيد على خمسة ألاف دينار وسحب الترخيص ومصادرة الآلات والأجهزة المستخدمة وذلك كل من أساء استخدام شبكة المعلومات الدولية في نشر معلومات أو بيانات تمس الأمن السياسي أو الاقتصادي أو الاجتماعي أو الموروث الثقافي للمجتمع العربي الليبي أو استخدم الفيروسات أو أي طرق أخرى لإيذاء الغير).

ثامناً/مشروع قانون الجرائم الافتراضية والدليل الرقمي في ليبيا (مقترح موسوعة التشريعات العربية) ويتكون من (94) مادة وتم تقسيمه إلى أبواباً ثلاث:-

الأول :- أحكام عامة

الثاني :- القاعدة الموضوعية.

الثالث:- القاعدة الإجرائية.

ومن الوقائع التي تعرض لها القضاء الليبي اجتهاداً حكم محكمة سرت الجزئية في واقعة التشهير عبر الانترنت باستخدام البريد الالكتروني (حكم رقم 71 -2004م. في القضية رقم 23-2004م)،حيث أصدرت حكمها (إدانة المتهم وبمعاقبته بالحبس لمدة سنة وبمعاقبة الآخرين بالحبس لمدة ستة أشهر) وذلك تطبيقاً لنص المادة 439-3 عقوبات ليبي، وإن المحكمة اعتبرت (إن إدخال صورة المجني عليها عبر الانترنت والكتابة عليها مسيئة لسمعتها تشهيرا لأن ذلك حصل عن طريق العلانية باعتبار أن الانترنت هي وسيلة اتصال وإعلان) بعد أن تعرضنا تاريخياً لنشأة الانترنت و القرار السياسي الليبي و تطبيقاته في النظام القانوني عمليا سوف نتعرض للنظرية العامة لقانون الانترنت لأنها تشكل التنظيم القانوني للعلم الافتراضي في الفصل الرابع من هذا البحث.

تاسعا: القانون رقم (3) لسنة 2014 بشأن مكافحة الإرهاب – الليبي حيث تنص المادة (1) على الآتي:-

(د الأموال :- العملة الوطنية والعملات الأجنبية المتداولة والأوراق المالية والأوراق التجارية وكل ذي قيمة من عقار أو منقول مادي أو معنوي وجميع الحقوق المتعلقة بأي منها والصكوك والمحررات لكل ما تقدم بما في ذلك الإلكترونية والرقمية).

و تنص المادة (2) على الآتي :-

(وكذلك كل سلوك من شأنه الإضرار بالاتصالات أو بالنظم المعلوماتية).

و تنص المادة (14) فقرة (9) على الآتي:- (السيطرة على الموارد الاقتصادية للدولة أو الإضرار بالبيئة أو الموارد الطبيعية أو بالاتصالات أو بالنظم المعلوماتية).

و تنص المادة (15) على الآتي:- يُعاقب بالسجن مدة لا تقل عن خمس سنوات ولا تزيد عن عشر سنوات كل من قام بالدعاية أو الترويج أو التضليل للقيام بالعمل الإرهابي سواء بالقول أو بالكتابة أو بأي وسيلة من وسائل البث أو النشر أو بواسطة الرسائل أو المواقع الالكترونية).

و تنص المادة (17) على الآتي :- (يعاقب بالسجن المؤبد كل من ساهم بطريقة مباشرة أو غير مباشرة في صنع أو تدريب على صنع أو استعمال الأسلحة التقليدية وغير التقليدية والأدوات والمعدات والوسائل السلكية واللاسلكية والوسائل الالكترونية).

المبحث الأول
مدلول الإنترنت

تمهيد

قانون الانترنت Cyber Law هو ذلك الفرع من فروع القانون، و يتضمن مجموعة القواعد القانونية التي تنظم العالم الفعلي للانترنت. و نعني بالعالم الفعلي للانترنت هو العالم الافتراضي cyber Space و هو ذلك العالم الذي خلقه تواصل الحواسيب و الشبكات دون اعتبار للحدود الدولية فالانترنت في حد ذاتها ليست ذلك العالم و ان تصادف اطلاق عبارة الانترنت علي ذلك العالم.

إلا أن العالم الافتراضي و بشكل دقيق هو العالم المقصود بالتنظيم القانوني، لذلك حين نقول قانون الانترنت فان المقصود الدقيق لهذه العبارة هو التنظيم القانوني للعالم الافتراضي.

و لقد برز مصطلح العالم الافتراضي لأول مرة في الأدب ألمعلوماتي أو أدب الخيال العلمي كما كان يسمى قديما و تحديدا في العالم 1984م، عندما وضع الروائي الكندي William Gibson روايته الشهيرة الحالم الجديد NEU Romancer و قد استخدم الفقه و القضاء المصطلحات التي ابتكرها هذا الأديب في روايته و من ذلك مصطلح العالم الافتراضي.

و في هذا الفصل سوف نتطرق إلي التنظيم القانوني للعالم الافتراضي وفق التقسيم التالي:-

المبحث الأول – مدلول الانترنت.

المبحث الثاني – خصائص الانترنت.

المبحث الثالث – قانون الانترنت.

المبحث الرابع – أقسام قانون الانترنت.

المبحث الخامس – اتجاهات مدارس قانون الانترنت.

المبحث السادس – مدارس قانون الانترنت.

المبحث السابع – اتجاهات التفسير في قانون الانترنت.

أن الإنترنت هي ظاهرة تحمل في مكوناتها طبيعة تقنية إنسانية ومند ظهورها برزت تعريفات كثيرة لها لذلك فإن الحصول على تعريف محدد للإنترنت يحقق التوازن بينه وبين واقع الإنترنت الحالي أمر انقسم فيه الفقه القانوني بسبب ظهور عدة تعريفات للإنترنت خلال فترة قصيرة جداً وإذا كان لابد لإحداث تنظيم لهذه التعريفات والتي منها محاولات التمييز بين نشأة الإنترنت وشبكة المعلومات الدولية وهذه الأخيرة عرفها مخترعها Tim Burners Lee بأنها «مبادرة لنقل المعلومات عبر وسائل إلكترونية على نطاق واسع بهدف إتاحة الدخول على وثائق ومستندات عالمية في جميع أنحاء العالم» أما الإنترنت فهي اكتشاف مؤسسة RAND وهي ((وسيلة تواصلية بين الشبكات دون اعتبار للحدود الدولية)) إلا أنه يصعب أحياناً الفصل بين الإنترنت وشبكة المعلومات الدولية (w.w.w World Wide Web) لأن الإنترنت في مفهومها المتطور دائماً لم تعد وسيلة اتصال بل أضحت مكتبة على مستوى عالمي تحتوي على ملايين البيانات المختلفة، وهي وسيلة سريعة وضخمة تنقلنا إلى كل موقع يمكن أن تدركه عقولنا البشرية وبهذا تكون الإنترنت أعم من شبكة المعلومات الدولية بل أن الأخيرة هذه هي أحد أقسام الإنترنت بالإضافة إلى البريد الإلكتروني والاتصال المباشر حسب التقسيم الراجح للإنترنت والمعبر عن حركتها ولعل أهم الاتجاهات التي تناولت تحديد مدلول الإنترنت هما :-الاتجاه التقني والاتجاه التقني الإنساني.

أولاً/ مدلول الإنترنت وفقاً للاتجاه التقني

يرى هذا الاتجاه أن الإنترنت هي ظاهرة تقنية وجديدة وأن الفضل يعود إلى علماء التقنية في ظهور مصطلح الإنترنت وهما عالمين أمريكيين BOB KHAN-VINT SERF مبتكري القاعدة الانفتاحية للإنترنت IP/TCP فيما يعرف بالنظام ألحزمي أو التراسلي Transmission Control Protocol internet Protocol ويعرف هذا الاتجاه الإنترنت بأنها شبكة تسمح بانضمام شبكات معلوماتية ذات أنساق مختلفة في إطار بفضل استخدام البروتوكول الوحيد IP/TCP والبريد الإلكتروني EMAIL والتصفح والمعلومات والآراء وكذلك بنوك المعلومات ويرى أيضاً هذا الرأي إلى أن الإنترنت لها طابعها المميز من حيث كونها مفتوحة وليست ملكاً لأحد. ومن أهم التعريفات في هذا الاتجاه تعريف الأستاذ جورج يوبوفيزي من جامعة بيركلي الأمريكية حيث عرفها «بأنها شبكة الشبكات Network of networks» كما أقرت هذا التعريف المحاكم الأمريكية في أحكامها، وقد أستخدمه نائب الرئيس الأمريكي السابق Algore في خطاباته.

ثانياً/ الاتجاه التقني الإنساني

ويؤيد هذا الاتجاه أغلب الفقه وأحكام المحاكم في القانون المقارن والزعماء السياسيين وكبار القادة ويذهب إلى رصد القيمة الإنسانية للإنترنت ووفقاً لهذا الاتجاه فإن الإنترنت هي ((شبكة دولية

المبحث الثاني

خصائص الإنترنت

فسيحة تسمح لكافة الحواسيب بالمشاركة في الخدمات والاتصالات بشكل مباشر كما لو كانت كلها جهاز حاسوب واحد)) كذلك ذهبت المحكمة الفيدرالية العليا للولايات المتحدة الأمريكية إلى تعريفها ((بأنها شبكة دولية مكونة من حواسيب متصلة تسمح لملايين الأشخاص بالاتصال ببعضهم البعض والدخول إلى مجال فسيح من المعلومات حول العالم)).

كما عرفتها بعض المحاكم الأمريكية ((بأنها شبكة الشبكات The network of Networks أو بأنها شبكة عالمية لمجموعة من الحواسيب المتصل ببعضها بما يسمح للأفراد أو المؤسسات حول العالم بالتواصل بتبادلها المعلومات فيما بينها)).

والحقيقة أن الاتجاه التقني – الإنساني هو الاتجاه السائد على المستوى القانوني والدراسات الاجتماعية في تعريف الإنترنت وكذلك في أحكام القضاء ولقد عرفها إستادنا الفاضل الدكتور / عمر محمد بن يونس- مستشار موسوعة التشريعات العربية ورئيس الجمعية العربية لقانون الإنترنت بأنها» تلك الوسيلة أو الأداة التواصلية بين شبكات المعلوماتية دون اعتبار للحدود الدولية « ولعل هذا التعريف يؤكد حقيقة الإنترنت لا طبيعتها لأن الإنترنت من طبيعة تقنية – إنسانية فهي نتيجة توافق التقنية(التكنولوجية) مع المعلومات والبيانات وحقيقتها إنها وسيلة تواصل بين الشبكات وباستخدام النظام الحزمي أو التراسلي المتمثل في بروتوكول IP/TCP نكون أعضاء فيها بحيث يمكننا أن نتصل بأي شبكة ونطلع على محتوى المضيفات والملقمات مع إمكانية الحركة بكل سهولة من هذه التعريفات لمدلول الانترنت اتصفت بعدة خصائص سنعرضها في المبحث الثاني من هذا الفصل.

أولاً / علاقة الإنترنت بالحاسوب

الإنترنت ترتبط بشكل وثيق بالحوسبة لأنها تعد أهم تقنيات هذه الحوسبة المتطورة، وحتى مع إمكانية الاتصال بالإنترنت عن طريق الهاتف النقال أو الساعات الرقمية أو أجهزة الإذاعة المرئية والمسموعة فلابد أن تكون أحدى مكوناتها أو جزء منها تقنيات متطورة من الحاسوب لأن مسألة ارتباط الإنترنت بالحاسوب يعد أمراً واقعاً لأن الإنترنت هي برنامج عمل متطور منخلال الحاسوب يجعل التواصل والحصول على المعلومات المختلفة ممكناً وسهلاً ذلك أن وضع الأسس الأولى للإنترنت تم من خلال البرمجة عبر الحاسوب وهي حتى الآن معتمدة على تقنيته ومرتبطة به ارتباطا وثيقاً ومع وجود لغة خاصة للإنترنت فإنها تتم برمجتها عبر الحاسوب وإذا أمكنا توقع الاستفادة من الإنترنت على المستوى العالمي فالمقابل لا يمكننا أن نتوقع ذلك بالنسبة لفوائد الحاسوب، لأنه في الحقيقة ثورة تقنية واقتصادية واجتماعية ومتطورة باستمرار لا يستطيع أحد أن ينكر خدماتها على المستوى الإنساني.

ولارتباط الإنترنت بالحاسوب يجعلنا أمام مسألة الارتباط الحاصل بين جرائم الإنترنت وجرائم الحاسوب والنوعية الأخيرة من الجرائم أرجعها الفقه المقارن إلى عام 1960م أما جرائم الإنترنت فقد بدأت عام 1988م بجريمة العدوان الفيروسي فيما معروف في التاريخ القانوني بجريمة((دودة موريس التي جرت أحداثها 1988/11/2م)) ولقد وجد فقهاء القانون الجنائي صعوبة بالغة في التفريق بين جرائم الحاسوب وجرائم الإنترنت وهذا ما يؤكد أننا أمام مفارقة بين الحاسوب وبين أحدى تقنياته، بالرغم من سهولة التمييز بينهما إذ بدون إحداث اتصال بين الحاسوب وبين الإنترنت عن طريق وسيط (مزود الاتصال) لا يمكن وحتى الآن أن نقول أننا موجودين على الإنترنت وهذا يقودنا إلى القول أن ارتكاب جريمة حاسوب لا يعني بالضرورة وجودنا على الإنترنت، وإنما يكفي أن يكون الحاسوب في حالة عمل في حين أنه لا يمكن القول بارتكاب جريمة من جرائم الإنترنت دون أن نكون على الإنترنت وهذا المعني نجده في القانون الأمريكي الذي ميز بين مصطلحي الحاسوب المنفرد Standalone Computer وبين الحاسوب المشمول بالحماية Protected Computer وهو الحاسوب المتصل بغيره عن طريق الإنترنت، أما مصطلح الحاسوب فقط فإنه يعني الحاسوب المنفرد غير المتصل بأي شبكة ولو داخلية وهو هنا يعتبر أداة تخزين فقط ولعل أهمية التعريف في المصطلحين مهمة عندما نتناول تفتيش وضبط الحواسيب المنفردة والمشمولة بالحماية وبظهور التقدم العلمي أنتشر الحاسوب في بلدان العالم المختلفة.

ثانياً/ عدم وجود قيود تقنية على الإنترنت

عندما تم اكتشاف شبكة المعلومات الدولية WWW على يد مهندس الاتصالات الإنجليزي LEE سنة 1991م لم تكن شائعة الاستخدام بل كانت مقتصرة على الممارسين للحاسوب ومحاطة بقيود أمنية إلا أنه وخلال سنة 1994م انطلقت الإنترنت إلى سطح الأرض وتزايد مستخدموها ولم تعد القيود الأمنية ذات أهمية ونتج عن ذلك سهولة استخدامها، وسهولة تطورها، فالإنترنت هي أداة سهلة الاستخدام والاستعمال عند توفير إمكانيات لدى الفرد على استخدام تقنية الحاسوب، وإزاء تطور تقنيات الحاسوب المختلفة آثر بشكل إيجابي على سهولة استخدام الإنترنت وإذا بحثنا في الحقيقة نجد أن غالبية مستخدمي الإنترنت ليست لهم دراية كافية باستخدامات الحاسوب. إذ إن هناك فرق بين التعامل بالإنترنت وبين الحصول على خدماتها ولعل هذا التمييز بشكل كبير في مجال التجريم والعقاب حيث يمكن من خلاله استحداث تمييز جنائي في تجريم الفعل من حيث تعامل المختصين غير المشروع بالإنترنت وبين تجريم الباحث عن خدماتها وهو في العادة شخص غير متخصص له نية استعمال الإنترنت ومن ناحية آخري فإن مسألة تطور الإنترنت لوحظ عليها أنها أصبحت مفتوحة للجميع، ولم تعد محصورة أو حكر في مجموعة العلماء.، ولقد ساعد على إنجاح هذا نظام اللامركزية الذي تتصف به الإنترنت، بل يمكننا أن نؤكد أن الإنترنت هي مجال رحب لكل الأفكار الإبداعية العلمية الجديدة سواء في التعامل معها أو في خدماتها. ومع ذلك أن سهولة وسرعة

تطورها قد يحدث إشكاليات قانونية والتي من ضمنها الجانب السلبي لاستخدامات الإنترنت والذي قد يصل إلى حد التجريم وظهور الدراسات والأبحاث القانونية المتعلقة بتاريخ التطور السريع والمذهل لإمكانيات الإنترنت وأثرها على القانون جعل معظم الدول تعيد النظر في تشريعاتها وتستعد للقادم الجديد بعد انتشارها السريع .

وفي التشريع المقارن هناك حكم للدائرة الثالثة الفيدرالية الأمريكية لسنة 2000م يقضى على (أن المواد التي يتم وضعها على شبكة المعلومات الدولية World Wide Web يمكن الدخول عليها من جميع مستخدمي الإنترنت والتكنولوجيا المعاصرة لا يتيح للناشر على الويب إمكانية تقييد الدخول على المواقع المعدة في الإطار المحلي لكل منها).

ثالثاً / تأثير الإنترنت الاجتماعي الاقتصادي

لقد كان لظهور الإنترنت تأثير اجتماعي اقتصادي ذو طابع عالمي لما أحدثته هذه التقنية العالية من تحولات في الأفكار السائدة، على كافة المستويات، فالتأثير الاجتماعي للإنترنت يمكننا أن نلمسه من خلال الحركة على الإنترنت فهي مجال استقطابي نشط ووسيلة علمية ثقافية فعالة لفتح مجالات البحث والدراسة والإطلاع والاستفادة من كل العلوم بل وحتى علاقات إنسانية جديدة مع أشخاص لا يعرفهم من أقصى بقعة على الأرض، وكذلك اللغة التي يتم فيها التعامل بها ومع وجود حقيقة عدم المفاضلة بين اللغات الإنسانية عبر الشبكات، إلا أن أمر وجود لغة مثل الإنجليزية وهي الأكثر شيوعاً ,يعني أنها ستبقى إلى الأبد إذا أنه من الممكن أحياء بعض اللغات الأخرى، وفي المجال الاقتصادي أصبحت الإنترنت المؤثر الأول في الاقتصاد العالمي وانتشرت مفاهيم التجارة الإلكترونية من بيع وشراء ولعرض بضائع وغيرها، وتقديم خدمات الاقتصاد من متابعة البورصات العالمية وتبادل الأسهم، وسمحت بظهور أفكار اقتصادية جديدة مثل المحل الإلكتروني والعقد الإلكتروني والتوقيع الإلكتروني، كذلك ما تقدمه الإنترنت من وسائل دعاية للمنتجات الاقتصادية. المختلفة وغيرها وعلى الرغم من التحولات الإيجابية للإنترنت على المستوى الاجتماعي والاقتصادي فقد قابلتها تحولات سلبية شرعت المحاكم في النظم المقارنة في التصدي للدعاوي المتعلقة بالإنترنت وبدأت الدراسات والأبحاث في إيجاد مواءمة بين النظام القانوني الوضعي وبين الإنترنت. والحاجة إلى وجود تنظيم قانوني للإنترنت وظهور مصطلح جديد وهو قانون الإنترنت بمدارسه وأقسامه واتجاهات التفسير فيه وهو ما سنتناوله في المبحث الثالث.

المبحث الثالث

قانون الإنترنت

أقسامه ومدارسه واتجاهات التفسير

أن القانون يضع حلولاً لظواهر نشأت بالفعل، فهو لا يأتي مجرداً عن الواقع، وأن هذه الظواهر في حقيقة الأمر لها طابعها الخاص في التنظيم ولها نظامها القانوني الذي يجعلها بمنأى من تدخل القوانين الوضعية السائدة وعندما يتدخل القانون يهدف إلى إحداث مواءمة بين المجتمع وبين التنظيم الطبيعي للظواهر الناشئة في الحقيقة وعلى أرض الواقع، أن ظاهرة الإنترنت وتأثيرها في النظام الاجتماعي والاقتصادي القائم ومدى صدى هذا التأثير على مستوى الأفراد أو الدول وما تحدثه الإنترنت من توافق في الثقافات المختلفة، وقد أستقر علماء القانون في نهاية القرن العشرين على تأثير الإنترنت على النظم الاجتماعية الاقتصادية فكان الاهتمام كبيراً بهذه الظاهرة على كل المستويات ورغم الخلافات الفقهية على ضرورة وجود تنظيم قانوني للإنترنت ((المذهب الحر-المذهب القانوني))ومع الاهتمام الدولي من الناحية التشريعية بإصدار قوانين جديدة أو تعديل الحالية برزت اتجاهات جديدة للتعامل القانوني مع الإنترنت.

أولاً/ قانون الإنترنت

إن عبارة قانون الإنترنت Cyber law يعني بها ((ذلك الفرع من فروع القانون الذي يتناول تنظيم العالم الافتراضي الذي خلقته الانترنت كوسيلة أو أداة تواصلية بين الشبكات دون اعتبار للحدود الدولية)) وبالتالي فهو يشير إلى النطاق القانوني للإنترنت، باعتباره مصطلح مبتكر ويقصد به ذلك الفرع من فروع القانون الذي يهتم بالموضوعات القانونية المرتبطة بالإنترنت وخدمات الاتصالات. وكان ذلك عندما برزت على المستوى الفقهي مسألة نطاق الإنترنت وحدودها أو نظرية الحيز الافتراضي Cyberspatial أو ما يعرف بالحيز الافتراضي في مصطلح جديد وفريد وهو العالم الافتراضي Cyberspace والذي يرجع الفضل في ربطه بالإنترنت إلى البروفيسور الفقيه اللاهوتي Hon Purry Barlow مستنداً إلى الدعم المجازي لإحداث وأفكار الأدب المعلوماتي من خلال رواية الأديب الكندي الأمريكي Gibson الحالم الجديد NEU Romancer، ولقد بحث الفقه تحديد ودراسة هذا المصطلح، ولقد توصل الفقه المقارن إلى فكرة العالم الافتراضي كحقيقة باعتباره العالم الذي خلقه التواصل الذي تحدثه الإنترنت بين الشبكات والحواسيب، ليكون أرضاً جديدة يخترقها الإنسان دون أن يكون له عليها سلطان. والعالم الافتراضي هو العالم المرئي أو المجال الحيوي للبيانات وحركة

البيانات، وهو العالم المختفي في الآلة التقنية والذي يطلق عليه بعض الفقه العربي تسمية الفضاء الإلكتروني وإذا كانت الإنترنت لم يتم تعريفها بعد في النظم القانونية المقارنة بشكل مستقل، ومع ذلك فإن هذه الأنظمة وبإيعاز من الفقه لجأت إلى حيلة قانونية يمكن بها الحصول على تعريف قانوني وذلك باستخدام مصطلح منبثق عن عالمها الافتراضي وهو (Cyber law) أي النظام القانوني للعالم الافتراضي أو قانون الإنترنت، والذي يتكون من مجموعة القواعد القانونية التي تنظم العالم الفعلي للإنترنت وهذه القواعد ماتزال في المراحل الأولى نتيجة عدم ملائمتها مع المنظومة التقليدية للقانون لأن البعض وصفها بالغموض ، ذلك أن مفاهيم قانون العالم الافتراضي (الانترنت) وتركيبته ذات طبيعة مختلفة عما عرفه القانون التقليدي , فهو في الحقيقة يتركب من طبيعة افتراضية ذات أبعاد دولية تتمشى شكلياً مع مفاهيم العولمة , وبرزت عدة اتجاهات فقهية لإقامة علاقة بين القانون وبين الانترنت تتمثل في أحداث ملائمة بين الاثنين بما يكفل معه تطويع القانون للانترنت لمصلحة الإنسان في تعامله معه التقنية ، و ينقسم قانون الانترنت إلي عدة أقسام سوف نتعرض لها في المبحث الرابع من هذا الفصل.

إن قانون الانترنت والذي يتناول مسألة التنظيم القانوني للانترنت ينقسم إلى خمسة أقسام نعرض لها في الفروع التالية :-

الفرع الأول/ التنظيم القانوني للتخزين الرقمي /(Digital Storage)

يتناول هذا القسم التنظيم القانوني لتخزين البيانات وطرق القيام بها ووسائل حمايتها وقد أوردت الدائرة التاسعة الفيدرالية الأمريكية تعريفاً في حكم لها للتخزين الإلكتروني (تعني عبارة التخزين الإلكتروني Electronic Storage القيام بالتخزين للبيانات سواء المؤقت أو الوسيط أو الفجائي أو العرضي أو التخزين التراسلي أو التخزين بهدف الحماية) وقد تناول مشروع قانون الجرائم الافتراضية والدليل الرقمي في الجماهيرية نصوصاً تتعلق منها بجرائم العدوان على التخزين الرقمي منها على سبيل المثال التداول غير المشروع للبيانات الاسمية مادة (24) والتي تنص علي الأتي:-

(كل من قام بنشر أو بث لبيانات أسمية تخص الغير أو استخدمها فيأعماله أو تجارته بمقابل أو بدون مقابل بغير موافقة صريحة ومكتوبة من صاحبها يعاقب بالغرامة حدها الأقصى عشرة ألاف دينار.

كل من استولى على بيانات اسمية بطرق رقمية أو مادية واستخدمها في ارتكاب جريمة من الجرائم المنصوص عليها في الفقرة الأولى السابقة يعاقب بالحبس مدة شهر وغرامة عشرة الآف دينار , وتكون العقوبة الحبس مدة لا تقل عن سنتين والغرامة إذا كان مرتكب الجريمة موظفاً عمومياً أو مستخدماً لدى أحدى الجهات الرسميةويعد من قبل البيانات الاسمية الصور والوثائق التي تخص الغير ما لم تكن متخذة طبيعية الوثائق العامة أو جزءاً منها , وتعد الموافقة الرقمية والشفوية الصريحة

المبحث الرابع

أقسام قانون الانترنت

أو الضمنية من قبل صاحب البيانات في مرتبة الموافقة الكتابية). والدخول غير المصرح به على قواعد البيانات الاسمية مادة (25) حيث نصت المادة على أنه (يعاقب بالسجن والغرامة كل من استخدم مهاراته في الحوسبة والرقمية دون تصريح أو مشروعية مستهدفاً الدخول والإطلاع على قواعد بيانات أسمية يقرر القانون حصانتها وخصوصيتها مثل:-

-الأحوال المدنية.

-التسجيل العقاري.

-قواعد بيانات المستشفيات وبنوك الدم والهيئات الصحية والعلمية والبيولوجية.

-المؤسسات العامة والعسكرية.

-المؤسسات الأمنية والسياسية.

-مصرف ليبيا المركزي.

-المؤسسات الأخرى التي يقرر لها القانون هذه الحصانة.

وتكون العقوبة السجن المؤبد إذا كان مرتكب الجريمة موظفاً أو مستخدماً في تلك المؤسسات وتجاوز صلاحياته في الدخول على البيانات المذكورة , وتكون العقوبة الإعدام إذا كان ارتكاب الجريمة بغرض التجسس لمصلحة دولة أجنبية أو نجم عن الدخول وفق هذه المادة وفاة أو قتل جماعي أو تخريب مواد مؤدي إلى ذلك أو إيذاء خطير أو كارثة) والإطلاع على البيانات السرية مادة (26) حيث نصت:-

(كل من اطلع بيانات رقمية معدة سريه وفق النظم الأمنية المعمول به في ليبيا دون أن يكون له الحق في ذلك يعاقب بالحبس مدة لا تزيد عن شهر وبعقوبة منع استخدام التقنية المدة التي يقررها قاضي الموضوع , ويجوز اتخاذ الإجراءات وفق ما هو مقرر في المادة (187) وما بعدها من قانون الإجراءات الجنائية , ولا تقوم الجريمة أصالة إذا تداخلت الصدفة أو ثبت أن بث تلك البيانات رقميا سببه جريمة سابقة على وقوع فعل الإطلاع , ولا يشترط في هذه المادة أن تكون البيانات الرقمية مرتبطة بالنظام التراسلي).

الفرع الثاني/ التنظيم القانوني لقواعد البيانات (Data Base)

يتناول هذا القسم دراسة الأنماط المختلفة للتخزين في الوقت الذي يجب أن تتجاوب في هيكلتها التخزينية مع القيمة الاسترادادية لها والممثلة في المعلومة المحددة التي يقوم الباحث باستعراضها ومسألة قواعد البيانات من المشكلات التي تواجه الفكر الفلسفي الغربي دون العربي الذي يستند في جذوره إلى أبو الفرج بين النديم في العراق الذي وضع الفهرست في القرن الرابع الهجري / العشر الميلادي ليكون بذلك أول موسوعي في التاريخ العالمي يضع منهجية أولية وأسس بينية لفكر قواعد

البيانات, ولقد تضمن مشروع قانون الجرائم الافتراضية والدليل الرقمي الليبي في نص المادة (56) الأتي (كل من قام ببث رقمي لقواعد بيانات مشمولة بالحماية ودون أن يكون له حق في ذلك أو بشكل غير مشروع يعاقب بالحبس مدة لا تقل عن سنتين وتكون العقوبة الحبس إذا قام مرتكب الجريمة بالاتجار فيها , بمقابل أو بدون مقابل , في أقراص أو وسائط تخزين أيا كانت, وفي كل الأحوال تزداد العقوبة إلى الثلث إذا كان مرتكب الجريمة هو من قام بإجراء التخزين أو النسخ الضوئي لها وقام باستخدام برامج وأدوات الترتيب بقصد التحايل اعتماد على محتوى قواعد البيانات).

و من أجل حماية العدوان على قواعد البيانات تنص المادة (57) من مشروع قانون الجرائم الافتراضية الليبي علي انه (كل من قام ببث لبرامج أو أدوات رقمية تسهل انتهاك حقوق الملكية الفكرية يعاقب بالحبس والغرامة التي لا تقل عن عشرين ألف دينار , وتزداد العقوبة إلى الثلث إذا كان مرتكب الجريمة هو مبتكر هذه البرامج أو الأدوات الرقمية).

وتنص المادة (55) علي انه (كل من قام بنشر رقمي لبرنامج تخزين أو تراسل أو لمصنفات غير مملوكة له أو دون وجه حق أو بثها بمقابل أو بدون مقابل في وسائط تخزين أو عبر المواقع ولو لم يكن أي منها موقعه الخاص أو كانت مواقع خاصة يعاقب بالحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن عشرين ألف دينار , وتزاد العقوبة بمقدار الثلث إذا كان مرتكب الجريمة هو الذي قام بأعمال التخزين).

وفي حكم للدائرة الثالثة الفيدرالية الأمريكية أنه « لكي يمكن إقامة الدعوى حال العدوان على حقوق النسخ فإن المدعي يلزم أن يؤسسها اولاً على ملكيته الفكرية للمصنف الأصلي محل العدوان ثانياً وجود نسخ للمصنف الأصلي المذكور.

الفرع الثالث/ التنظيم القانوني للمعاملات الرقمية / (Digital Transaction)

يتناول هذا القسم من القانون حركة المعاملات المدنية المختلفة عبر الانترنت مثل موضوع الحقوق والحريات والتزامات الرقمية والملكية الفكرية والعقود الرقمية وغيرها من الموضوعات ذات العلاقة وفي مجال العدوان على الملكية الفكرية فقط قضت الدائرة السابعة الفيدرالية الأمريكية بأنه (لا يكفي في العدوان على حقوق النسخ مجرد القيام بتقليد مصنف (برنامج حاسوب)أو أجزاء منه وإنما يجب أن يكون التقليد مؤدياً إلى عدم إمكانية التمييز بين المصنف أو أحد عناصره وبين المصنفات الأخرى المقلدة)، وللحماية من العدوان على المعاملات الرقمية فقد وردت نصوص في مشروع قانون الجرائم الافتراضية والدليل الرقمي في ليبيا ومثالها المادة (55) (كل من قام بنشر رقمي لبرنامج تخزين أو تراسل أو لمصنفات غير مملوكة له أو دون وجه حق أو بثها بمقابل أو بدون مقابل في وسائط تخزين أو عبر المواقع ولو لم يكن أي منها موقعه الخاص أو كانت مواقع خاصة يعاقب بالحبس مدة لا تقل عن سنة والغرامة التي لاتقل عن عشرين ألف دينار ,وتزاد العقوبة بمقدار الثلث إذا كان مرتكب الجريمة هو الذي قام بأعمال التخزين)والمادة (45) والتي تنص (كل من استخدم مضيفات أو خوادم محلية لاختراق حواسيب مشتركة فيها يعاقب بمنع استخدام التقنية لمدة ثلاثة سنوات , ويضاف إلى هذه العقوبة عقوبة

الحبس إذا كان مرتكب الجريمة من العاملين في إطار إدارة الخادم أو المضيف المحلي الذي تم من خلاله الاختراق، ولم يكن لديه مبرر لذلك , ولا تنطبق هذه المادة إذا كانت الشبكة المحلية داخلية وكان ذلك بقصد مراقبة أعمال الوظيفة في مؤسسة أوجهة معترف بها قانونياً أو كانت الجريمة محلها منازعات العائلية). والمادة (51)(كل من قام بتسجيل نطاق اسم Domain Name بسوء نية أو بقصد الحصول على كسب غير مشروع أياً كان وبأي قيمة كانت وسواء كانت مادية أو معنوية، يعاقب بالحبس والغرامة قدرها عشرين ألف دينار, ولا تقام الدعوى إلا بناء على شكوى الطرف المتضرر' ويجوز إيقاف الإجراءات إذا وجد في أوراق الدعوة دلالة على تسوية بين الجاني والغير أو رفع دعوى تحكيم رقمي). كذالك المادة (7) والتي تنص (لا تنطبق أحكام هذا القانون حين قيام الغير بانتهاك علاقة عقدية ليس طرفاً فيها أو تجاوز إجراءات ترخيص إداري مطلوب ما لم يكن هذا الانتهاك مبنياً على أحد الأسس التالية / كحد أدنى للتطبيق :-

- اختراق سنده المهارة الخاصة.
- توفير مناخ إرهابي أو تهديد خطير للعالم الافتراضي.
- جريمة من جرائم الكتاب الثاني من قانون العقوبات والتشريعات ذات العلاقة المباشرة بسيادة الدولة.
- انتهاك الحق في الخصوصية المبني على التوقيع المعقول لها.
-إغراق الخوادم.
-جرائم التزوير والتزييف المنصوص عليها في قانون العقوبات.
-التسبب في انتهاك اتفاقيات دولية أو إقليمية أو ثنائية تكون الدولة طرفاً فيها أو لها مصلحة في وجودها
-إعاقة تحقيق دولي مفتوح له علاقة من أية نوع بالجريمة المرتكبة ولو لم يتم اكتشاف تلك العلاقة أو الجريمة ككل بعد).

-, والمادة (26) والتي تنص (كل من أطلع على بيانات رقمية معدة سرية وفق النظم الأمنية المعمول بها في ليبيا، دون أن يكون له الحق في ذلك، يعاقب بالحبس مدة لا تزيد عن شهر وبعقوبة منع استخدام التقنية المدة التي يقررها قاضي الموضوع ويجوز اتخاذ الإجراءات وفق ما هو مقرر في المادة(187 مكرر) وما بعدها من قانون الإجراءات الجنائية, ولا تقوم الجريمة أصالة إذا تداخلت الصدفة أو ثبت أن بث تلك البيانات رقمياً سببه جريمة سابقة على وقوع فعل الإطلاع , ولا يشترط في هذه المادة أن تكون البيانات الرقمية مرتبطة بالنظام التراسلي).

الفرع الرابع/ التنظيم القانوني للتجارة الالكترونية Electronic Commerce

وهذا القسم يتجاوب مع فكرة التجارة عبر الانترنت بما في ذلك التطورات الحادثة فيها والتي صاحبها العديد من التفسيرات، ويشمل ذلك استخدام الانترنت في التجارة أو التجارة الرقمية كما هو الحال في الاتجار بمواد رقمية ليس لها وجود سوى في بيئة تقنية المعلومات مثل البرمجيات والبرامج...

وغيرها, وفي القضاء المقارن نجد الدائرة الرابعة الفيدرالية الأمريكية في حكم لها بشأن التنظيم القانوني للتجارة الإلكترونية حيث قضى الحكم على (أن الانترنت هي منطقة تجارة ويجب أن يتم معاملتها كاحتياطي وطني لكي يمكن حماية المستخدم من التنظيم غير الدقيق لها والذي يمكن أن يصل بها إلى الشلل التام الذي يسبب تخلف تطويرها، إن إي تنظيم قانوني لطريقة الاستخدام المشروع للانترنت ينتهك شرط التجارة الدستوري).

وقد أورد مشروع قانون الجرائم الافتراضية والدليل الرقمي في ليبيا نصوصاً لحماية التجارة الالكترونية ومثالها استخدام نظم التجارة الالكترونية في الاتجار غير المشروع مادة (32) والتي تنص (كل من استخدام نظم التجارة الالكترونية بقصد الاتجار غير المشروع بالمخدرات والمؤثرات العقلية يعاقب بالإعدام , ويعاقب بالسجن المؤبد, وغرامة تعادل ضعف قيمة المعاملة , كل من استخدام نظم الحوسبة والرقمية بقصد الاتصال بمنظمات الاتجار غير المشروع بالمخدرات والمؤثرات العقلية وكان غرضه التعامل في المخدرات والمؤثرات العقلية مع أفراد هذه المنظمات. وتطبق المواد (4-5-6) من قانون العقوبات لسنة 1953م والمادة الأولى مكرر من قانون المخدرات والمؤتمرات العقلية على المتعامل بنظام التجارة الالكترونية لهذا الغرض من خارج الأراضي الليبية إذا ثبت قيامه بمعاملات توريد مع مؤسسات في داخل البلاد بقصد التعامل بالمخدرات والمؤتمرات العقلية, وإذا كان الضحية ناقص الأهلية فلا تسقط الإجراءات الجنائية بالتقادم)، والمادة (54) حيث تنص (كل من تلاعب رقمياً ببيانات مهيأة كعملة رقمية أو لحركة تداولها على أية شاكلة تكون عليها هذه الحركة , سواء الكترونية أو رقمية أو ذكية , بقصد الاستيلاء عليها يعاقب بالسجن مدة لا يقل عن عشرة سنوات والغرامة تعادل ضعف المبالغ المتضررة من التلاعب , ويعاقب بذات العقوبة كل من ثبت استخدامه لبرامج أو برمجيات أو أدوات خاصة بقصد ارتكاب أو تسهيل ارتكاب عمليات تزييف العملة المادية , ويعد شريكاً في هذه الفقرة من قان بإعداد وتصميم البرنامج أو الأداة أو أي جزئية فيها تساعد في ارتكاب الجريمة إذا ارتكبت فعلاً ' وتشمل العملة المادية وفق هذه الفقرة كروت الاعتماد وغيرها مما يمكن أن يحل محل العملة في التعامل ما دام يمكن ترجمته بشكل فوري إلى نقود متداولة حول العالم)

الفرع الخامس/التنظيم القانوني للجريمة الافتراضية (Cyber Crime)

ويشمل هذا القسم القاعدة الموضوعية والإجرائية , حيث يتبادل رؤية الفقه والقضاء والمشروع لمسألة الحماية الجنائية التي تتم لكافة ما يتعلق بالانترنت, ويتناول كذلك البحث في التطور الذي تتعرض له القاعدة الإجرائية اليوم مع ما يصاحب هذا الأمر من ظهور الدليل الرقمي (Digital Evidence) الذي يعد الشغل الأهم في المرحلة الحالية لعلماء العدالة الجنائية ، وقد أورد مشروع قانون الجرائم الافتراضية والدليل الرقمي في ليبيا، المسئولية الرقمية في نص المادة (58) والتي تنص (المسئولية الرقمية مبرر للدعوى المدنية التابعة). والأهلية الرقمية في نص المادة (59) (لا يعتد في تطبيق أحكام هذا القانون بقواعد الأهلية المقررة في قانون العقوبات ما لم تكن الجريمة الافتراضية تستهدف جريمة تقليدية). والباعث في المادة (60) حيث تنص (مع مراعاة المادة(95) من قانون العقوبات يعتد بالباعث إذا كان لذلك سبب تقني , ويعد من قبيل السبب التقني التحدي بين الهكرة والابتكار إذا تجاوز الحدود المعقولة للإباحة). وأشخاص القانون في نص المادة (62) حيث تنص (مع مراعاة أحكام الاشتراك

المقررة في قانون العقوبات يعد مسئولا عن الجريمة وفق هذا القانون من ارتكبها بنفسه أو مع غيره ولا يعد تنظيماً عصابياً رقمياً وفق القانون سوى التنظيم الذي تتحدد أغراضه في كونه يتمتع بصفة الاستمرار مع تحديد الأهداف التي قام من أجلها أو كانت له جذور في الواقع كعصابة منظمة أو من إتباع الجريمة المنظمة)، وفي المادة (63) مسئولية الطرف الثالث حيث تنص المادة: (لا يسأل الطرف الثالث عن كافة الأنشطة التي يقوم بها الغير ما لم ينص صراحة علي غير ذلك , ومع ذلك يجوز مسألة الطرف الثالث كشريك سلبي إذا لم يتخذ الحيطة والحذر التقني في مجال الجرائم الأخلاقية وجرائم الملكية الفكرية والجرائم المرتكبة ضد شخصية الدولة وأمنها وفق التشريعات النافذة, وتكون مسئوليته كفاعل أو شريك إذا كان على دراية وإدراك بالجريمة وتعد مساهماته التقنية مساهمة فاعل في الجريمة, وفي الحالات الاستثنائية المذكورة بإغلاق الطرف الثالث وجوبياً). وإزالة وإتلاف الأدلة الرقمية في نص المادة (27) حيث تنص (تطبق الأحكام المتعلقة بإتلاف الدليل الواردة في قانون العقوبات والتشريعات الأخرى على جرائم إزالة وإتلاف الدليل الرقمي , ومع ذلك تسأل الجهة الملزمة بالتحفظ واستخلاص الدليل الرقمي إذا لم تتخذ الإجراءات التقنية الكفيلة بالمحافظة على الدليل المدة اللازمة لذلك إذا ترتب على ذلك ضياع حقوق للغير بما في ذلك المؤسسات والجهات العامة والمجتمع , ويكون على هذه الجهة إثبات أنها اتخذت هذه الإجراءات المشار إليها للحفاظ على الدليل), ومع مراعاة المادة (79) من هذا القانون (تحدد مدد التحفظ واستخلاص الدليل الرقمي بقرار اللجنة الشعبية العامة للعدل بناء على توصية اللجنة المحددة في قانون الإصدار). وإتلاف الجاني للأدلة الرقمية ونص المادة (37) (كل من قدم استشارات فنية أو تقنية لمرتكب جريمة غسل الأموال الرقمي أو قام بمساعدة مرتكبيها وقدم لهم التسهيلات المادية والدعم الفني والتقني بأي شكل من الاشكال يعد شريكاً في الجريمة اذا ارتكبت الجريمة فعلاً وكان دوره الاستشاري واضحا فيها , وتطبق أحكام الاشتراك الواردة في قانون العقوبات لسنة 1953م , وإذا كان الاستشاري مؤسسة أو مكتب يحكم بالغلق, ويعد شريكاً في الجريمة من يتواجد لديه ملفات مخزنة لعمليات غسل الأموال ولم يبلغ عنها الجهات المختصة , ولا تسري هذه الفقرة على المرؤوس الذي ينفذ تعليمات التخزين ولو كان ذلك بأساليب التشفير ما لم يكن على دراية بمحتوى تلك الملفات). ونص المادة (80) التفتيش الرقمي حيث نصت (لا يجوز التفويض في إصدار إذن التفتيش تنفيذاً لهذا القانون، ولا يجوز إصدار إذن تفتيش عام ما لم يكن التفتيش مقررا بشكل رقمي , وفي هذه الحالة يجب النص في إذن التفتيش على الغاية منه بشكل واضح وصريح ومباشر وبحيث يشتمل أيضاً على تحديد المسار الذي يتم من خلاله التفتيش الرقمي , ويعد التفتيش رقمياً إذا تم باستخدام النظام التراسلي فقط وبما يستدعى ذلك تتبع حركة مرتكب الجريمة عبر الخوادم والمضيفات بقصد الوصول إلى الحاسوب الذي انطلق منه النشاط التقني في الجريمة). والشهادة الرقمية نص المادة (85) حيث تنص (أداء الشهادة رقمياً مقبول في كافة الأحوال , سواء كانت الوقائع المنسوبة للمتهم مادية أو رقمية , ولو كان الشاهد خارج الحدود الإقليمية ما دام الشاهد يدلي بشهادته تحت إشراف قضائي ليبي أو أجنبي محلف , ويجب أن يتم تحليف من حضر الإدلاء بالشهادة اليمين بأنه يقر بأن الشاهد الذي يدلي بشهادته هو المقصود وأنه تعرف على

شخصه وصفته وهويته وكذلك تكرار أقواله , وإذا كان الشاهد صغيراً أو عاجزا أو في حالة الاستعجال يجوز أن تكون الشهادة مسجلة رقميا وفي غير الزمن الفعلي شريطة أن تكون ثابتة التاريخ). و في نص المادة (86) الغاية من التفتيش حيث تنص علي انه: (ليس في هذا القانون ما يبرر الخروج على المادة (39) من قانون الإجراءات الجنائية , ومع ذلك فإن اكتشاف جريمة ما بطريق الصدفة يبرر اتخاذ إجراء التحفظ إلى حين اتخاذ الإجراءات الجنائية , ويجوز لكل إنسان اتخاذ إجراءات التحفظ المذكورة شريطة إبلاغ السلطات خلال مدة معقولة). وحماية الشهود في نص المادة (87) حيث تنص (يجوز وضع برامج أمنية لحماية الشهود , وإذا كان الشاهد صغير السن يجوز الاكتفاء بسماع شهادته أو الحصول على شهادته مسجلة أو الإدلاء بها رقمياً دون لزوم حضوره مع الاحتفاظ بسرية شخصيته). والبلاغ الرقمي في المادة (92) حيث نصت (تكون الجهة المختصة مسئولة عن عدم الالتزام الاستدلال في كل بلاغ رقمي يصل إليها , ويعاقب المسئول عن استلام البلاغات بالعقوبات المقررة في قانون العقوبات عن كل إهمال في الاهتمام بالبلاغ الرقمي , وتطبق في شأن المبلغ أحكام جريمة الافتراء والبلاغات الكذاب المقررة في قانون العقوبات إذا ثبت أن بلاغه غير صحيح, ويعفى المبلغ من العقاب إذا كان أساس بلاغه توقع معقول وفقاً للظروف العادية وبمعيار الرجل المتوسط أو العادي). وفي التشريع المقارن نجد أن هناك حكم للدائرة التاسعة الفيدرالية الأمريكية يقر بوجود التقاضي في جرائم العالم الافتراضي والاختصاص به حيث نص الحكم على أن«العالم الافتراضي (Cyberspace) يخضع التقاضي فيه لقواعد الاختصاص, فقط على القضاء توفير المناخ للبحث في مدى اختصاص المحاكم لقضاء العالم الافتراضي« .

ومن الأهمية بمكان في إطار دراسات الجريمة الافتراضية في هذا القسم التنبيه إلى حركة التطوير في دراسات الجريمة ككل بسبب هذا القسم، فقد ساهمت الدراسات والبحوث في مجال الجريمة الافتراضية في تنمية الفكر الجنائي المقارن باتجاه تطوير القاعدة الموضوعية والإجرائية في النظرية العامة في القانون الجنائي، وربما النظرية العامة للقانون ككل، ومن ذلك نورد مثال على نوعية من الجرائم الافتراضية التي جعلت فقه الحقوق والقانون الجنائي يتناولها بشيء من التأمل لمعرفة صداها وأثرها التطويري على القواعد التقليدية، ونعني بذلك جريمة الإرهاب الالكتروني.

الإرهاب الالكتروني:-

تعد جريمة الإرهاب الالكتروني من الجرائم التي تم استنباطها كصياغة في ظل أفكار الجريمة الافتراضية. بل انه يمكن القول أنها أول أنواع الجرائم الافتراضية على اثر تطور دراسات علم الإجرام عبر الانترنت. فالشخصية محور الاهتمام في الإرهاب الالكتروني هو الهكر الخبيث الذي يستخدم وسائل تقنية المعلومات لارتكاب أفعال ووقائع تؤدي إلى إرباك الانترنت كأداة او وسيلة تواصلية بين الشبكات دون اعتبار للحدود الدولية. وكان المستهدف من تقرير هذه الجريمة هو بث نوع من الحذر العام عند استخدام الانترنت، في الوقت الذي يسمح إقرار مثل هذه الجريمة الأخذ في الاعتبار الدور

الأمني فيها.

وماحدث فعلا ان موضوع الإرهاب الالكتروني تطرق إلى اخطر التعديلات في قانون عقوبات الانترنت Cybercrime وهو القانون الوطني الأمريكي The Patriot Act الصادر على اثر أحداث سبتمبر في الولايات المتحدة الأمريكية2001م. حيث أصبغ هذا القانون كافة جرائم الانترنت الواردة في القسم 1030 من تقنين الولايات المتحدة الأمريكية USCODE والذي يمثل قانون عقوبات الانترنت بصبغة الإرهاب. مما أضفى على جرائم الانترنت الصبغة الإرهابية وبالتالي سمح هذا الأمر باختصاص الجهات الأمنية دون القضائية بالجريمة الافتراضية.

على إن الأمر لم يقف عند هذا التوجه المنتقد. إذ للقانون الوطني الأمريكي وجهاً مطلوباً في الحقيقة , فمن الأهمية بمكان الاعتراف بان القانون الوطني الأمريكي أتاح الفرصة أمام فقه الإجراءات بالتطرق إلى موضوعه من حيث مدى تجاوب تطوير قواعد الإجراءات الجنائية وفقه المرافعات. فظهر علينا مبدأ جديد في إطار قاعدة التفتيش وهو (إذن التفتيش الممتد) الذي يعد مدرسة جديدة تأخذ في الاعتبار حركة التفتيش عن الدليل الرقمي في المزودات والخوادم بتبرير مقنع وجدير بالاهتمام. ولقد توسع الاهتمام بهذا الاجراء إلى إعادة بحث وتفسير المعادلة القديمة التي كانت مضمونه بقانون الإجراءات الجنائية وهي قاعدة الحق في الخصوصية وحرمة الحياة الخاصة. فقد أعاد الفقه النظر في هذه القواعد الجامدة. من حيث دراستها وإعادة تفسيرها مع التطورات الجديدة المصاحبة لثورة تقنية المعلومات.

كذلك ساعدت أفكار الفقه حول الإرهاب الالكتروني في إبراز الطابع الأكاديمي للتقسيم الوارد حول ضرورة إبراز خصائص الإجرام الافتراضي ومجرم الحاسوب. وهو تمييز يقودنا الى أحداث مفارقة بين مجرم الانترنت ومجرم الحاسوب. وبالتالي وبطبيعة الحال يمكن استحداث تصنيف للجرائم الافتراضية من حيث جرائم النظام التراسلي التي تستلزم حسبما اقر القضاء المقارن ان تتم بين الشبكات و بين جرائم التخزين الممثلة في الحاسوب كجهاز منفرد غير مرتبط بالانترنت وتقرر أيضا ان الأصل ان القانون لا يطبق إلا على النظام التراسلي اي الحاسوب المرتبط بالانترنت Protected Computer وان تطبيق القانون على نظام التخزين ونعني به الحاسوب او الحواسيب غير المرتبطة بالانترنت Standalone Computer يعد نوعاً من الاستثناء الذي لابد أن ينص عليه صراحة في القانون.

واذا كانت صيغة التهديد والفزع الذي تمثل الصورة المثالية في جرائم الإرهاب بشكل عام تأخذ الطابع الإنساني فانه ينسب إلى دراسات الانترنت انها تتولي دراسة ظاهرة تقنية إنسانية. ومما يستدعي القول ان استخدام تقنية المعلومات في ارتكاب جرائم تهديديه وخطرة وكارثيه أمر قريب الاحتمال دائما.. وتعطي جريمة العدوان الفيروسي تطبيقا مثاليا لجرائم الإرهاب الالكتروني، فالتهديد بإرسال فيروسات عبر الشبكة يمكن ان يصيب العالم الافتراضي بفزع كبير وتهديد تتعطل به حركة المصالح الإنسانية عبر الانترنت.

إن تناول الإرهاب الالكتروني يستدعي ضرورة التطرق إلى علم الإجرام عبر الانترنت كما ذكرنا فيما سلف من حيث التقرير بدراسة أجيال الهكرة والتاريخ الشخصي للهكر مرتكب هذه الجريمة وإعداد دراسات اجتماعية حول تداخل هذه الجريمة في النسيج الاجتماعي والاقتصادي للمجتمعات. فدراسة هذه الجريمة من الأهمية بمكان حتى يمكن استعادة التوازن الاجتماعي والاقتصادي في دراسات الجريمة وبالتالي أجادة فن التمييز بين العدوان الإرهابي عبر الانترنت وارتكاب جريمة افتراضية.

ولقد كان من أهم سمات البحث في الإجرام الافتراضي وربطه بالإرهاب هو القدرات الخارقة للهكرة في التعامل مع حركة الحوسبة والرقمية. ومثل هذا الأمر قاد فقه الانترنت الى البحث في استحداث تقسيم لأنواع الهكرة، وبالفعل اوجد الفقه تقسيم للهكرة يستند الى أجيال الهكرة وبشكل جعل البحث في تفاعل الهكر مع التطورات الحادثة وسعة انتشارها ودرجة احترافيتهم على النحو التالي:-

أ-المطورونDevelopers: وهم الذين ساهموا في تطوير الحوسبة والرقمية. ولقد وصل البحث في قياس كفاءات التطوير الى ضم فئات من الهكرة ممن يضعون تصاميم للمواقع، حين استخدامهم لأبواب خلفية Back Doors. والجميع يعلم استخدامات الأبواب الخلفية. فقد تجاوزت فكرة التطوير القدرات البرمجية الى القدرات التصميمية للمواقع.

ب-مخترقو نظم الهاتفPhreakers: وانتشر مصطلح الهكر لكي يطلق على فئة من الناس استطاعوا باستخدام الإمكانيات التقنية للحوسبة والرقمية في اختراق نظم الهاتف. والاستيلاء مجانا على تلك النظم لمصلحتهم. مستهدفون بذلك الانتهاك والعدوان على نظم الاتصالات. فتداخل العامل الاجرامي في تقنية المعلومات بالاتصالات من هذا الجانب.

ت-القراصنةPirates: وهنا حدثت نقلة هامة في نشاط الهكرة. فعندما بدأت حركة النشر الالكتروني باستخدام شبكة المعلومات الدولية وتطورات آليات الحوسبة والرقمية بدأت حركة العدوان على الملكية الفكرية. والاستيلاء على المصنفات وانتشر هذا المصطلح كثيرا أيضا عندما تخصص البعض بفك كلمات المرور للألعاب الالكترونية التي تستخدم في الحاسوب. وساعد الإعلام على نشر مصطلح القرصنة بحيث تم التحوير في المصطلح ذاته لكي يطلق على الهكرة. خاصة مع وجود قصور أكاديمي عربي في القاموس. فما يشكله هذا المصطلح في الحقيقة هو ان هذا المصطلح وإطلاقه على الهكرة هو خطأ شائع يلزم التصحيح.

ث-الهكرة Hackers: بدأ توجه الاتجاه الوظيفي يأخذ مجراه الطبيعي والصحيح في دراسات قانون الانترنت مع ظهور فقه النظرية والتنظيم القانوني للعالم الافتراضي. وكان من تداعيات هذا التوجه هو الاهتمام بوظائف واستخدامات تقنية المعلومات في القانون. فقدرات الحوسبة والرقمية لابد ان تؤخذ في الاعتبار لكي يمكن تطبيق القاعدة القانونية. وعندما بدأ القضاء المقارن يعتمد الاتجاه الوظيفي في تفسير الوقائع والقواعد القانونية ذات العلاقة بالحوسبة والرقمية بدأ ذلك اكثر اقناعا للنظام الاجتماعي والاقتصادي على السواء ومن ذلك اقتناع القضاء بضرورة التمييز بين جرائم الحاسوب Computer Crime وجرائم الانترنت او الجريمة الافتراضية في المعنى الدقيق لها Cybercrime. وتطور الحال لكي

يصل القضاء حين اعتماده للاتجاه الوظيفي الى وضع طرح معدل جديد للمصطلحات القانونية مثل مصطلح Telecommuter وهو مصطلح يشير الى العاملين او المتعاقدين عبر الانترنت على القيام بأعمال محددة. كما لو اتفق شخص مع اخر عبر الانترنت على اعداد موقع او توثيق ترجمة. وفي النهاية تم الاعتراف بهذا المصطلح كمهنة من المهن في قانون العمل المقارن.

ولم يقف الامر عند هذا الحد بل تجاوز ذلك بمراحل عند قيام القضاء المقارن بدراسة معيارية الهكترة والهكر وبنى تعريف الهكترة والهكر على المهارة الخاصة التي يتميز بها الفرد حال قيامه بارتكاب وقائع عبر الانترنت. فظهر معيار المهارة الخاصة لكي يضفي على نشاط الهكرة الصبغة الاجرامية فلا يكفي مثلا قيام الشخص بارتكاب جريمة عبر الانترنت وانما يجب ايضا ان يتمتع هذا الشخص بمهارات خاصة لا يملكها غيره من الناس. ومن هذا الجانب بدأت تتضح معالم نشاط الهكرة. فاذا اضفنا الى هذه المهارات الخاصة قدرات الهكر واي هكر على احداث الفزع فانه يمكن تصور جريمة الارهاب الالكتروني والأمثلة على ذلك كثيرة فمثلا قيام الشخص بانتهاك منظومة الكهرباء والتحكم فيها يعد ذلك عملا ارهابيا خاصة اذا كانت مثل هذه المنظومة تعتمد الحوسبة والرقمية في نشاطها. ويمكن ان نشير هنا الى قضية شهيرة في القضاء المقارن وهي تشكل مرجعا في هذا الاطار ومع ذلك لم يتم التوصل قضاءا الى وصف مرتكبها بالإرهاب وهي قضية المواطن الانجليزي Gary Mckinnon الذي انتهك عبر الانترنت قاعد بيانات قاعدة عسكرية أمريكية مستخدمة للتموين بولاية نيوجيرسي الأمريكية.

المبحث الخامس

اتجاهات مدارس قانون الإنترنت

على المستوى القانوني نشأ خلاف يتعلق بإمكانية التعامل القانوني مع الإنترنت بين مؤيدي وجود التنظيم القانوني للإنترنت يقابله أتفاق بين علماء التقنية على ذلك ويبدو إن الخلاف يدور حول الاكتفاء بالتنظيم القانوني التقليدي للإنترنت أم أن الأمر يحتاج إلى رؤية جديدة تصاحب الحدث وكان رأي الاتجاهات كالآتي:-

أولاً/ التعامل التقليدي مع الإنترنت

برزت المطالبة بالتعامل القانوني التقليدي مع الإنترنت في العقود بالتحديد، وبسبب ظهور التعامل بالعقود من خلال العديد من المواقع على الإنترنت، كمثال على ذلك إذا تطلب شخص ما أن يفتح بريداً إلكترونياً مجانياً Free Email أو تصورياً فإن عليه أن يوافق على العقد أو الاتفاق المعد والمطروح من قبل الشركة أو المؤسسة التي تعرض هذا النوع من الخدمة على مواقعها فالعقد أو الاتفاق سبق إعداده على نموذج جاهز غير قابل للنقاش أو تبادل الإرادة الموضوعية من الطرف المقابل، بحيث يمكن للشركة أو المؤسسة أن تضع الشروط التي تريدها وتتماشى مع مصلحتها. وبعد مسألة العقود تطور الأمر وأصبحت هناك تعليمات ومثالها أن الدخول لبعض المواقع يستلزم الإقرار بتوافر شروط مسبقة في الشخص مثل شرط السن أو الأهلية فإن لم تتوافر فيه هذه الشروط عليه أن يمتنع عن الدخول هو أمر يبني على افتراض الأمانة والمصداقية في الأشخاص مستخدمي الإنترنت ومخالفة إجراءات العقد والتعليمات تجعل الشخص مسؤولاً وفقاً للنظم التقليدية القائمة وبهذا التعامل التقليدي أصبح عاجزاً عن التصدي لظواهر مخالفة تلك النظم والتي منها قوة الإلتزام في القاعدة القانونية تمتد إلى شخص يقيم في ذات الإقليم الذي ينطبق فيه القانون والحقيقة تخالف ذلك، كذلك غياب الإرادة في العقود والموجودة على الإنترنت هي محل طعن وفقاً للتعامل التقليدي.

أن الإستخدام التقليدي للقانون لمواجهة ظواهر اختراق الإنترنت بات أمراً غير ذي جدوى لذلك لجأت بعض المواقع إلى وسائل تقنية حديثة ومتطورة ومثالها كلمة المرور وإقامة الحواجز النارية والحقيقة أن القواعد القانونية التقليدية وقفت عاجزة عن مسايرة التطور العلمي والتقني مما حدا بظهور اتجاه فقهي يؤيد ضرورة التجديد الشامل للقاعدة القانونية التقليدية بما يتمشى مع التقنية وإشكالياتها.

ثانياً/ تعامل جديد مع الإنترنت

أن عملية التشريع التي تنظم ظاهرة حديثة بداية من الأمور الصعبة إلا أنها ليست مستحيلة ويرجع سبب صعوبتها إلى أن هذه الظواهر لم تعرف بعد بالشكل الجيد من جانب سلوكياتها واقتناع السلوك البشري بالمنهج الجديد كما أنها تحتاج إلى وقت. إن فلسفة التغيير تسود بقوة في الفكر البشري وهو الاتجاه الذي ينادي بالتعامل القانوني الجديد مع الإنترنت، وهذا الاتجاه نجد له مقدمات في خصائص الإنترنت التي ذكرناها سابقاً والتي من ضمنها سهولة تطويرها ولقد برز هذا الاتجاه القانوني الجديد. ونادى بضرورة إدماج فصل جديد في القانون الجنائي القائم يتعامل مع تقنيات الحاسوب وهو أمر أقره المشرع المقارن

ومن ذلك المشرع الفرنسي في قانون العقوبات النافذ عام «1994م»، والقانون الأمريكي في القسم 1030 من الموسوعة الأمريكية لتقنين الولايات المتحدة الأمريكية.

ثالثاً/ الاتجاه الراجح

ما بين التعامل القانوني التقليدي مع الإنترنت وبين المطالبة بالتعامل الجديد مع هذه الظواهر، أتخذت الأمور في الواقع اتجاها جديداً وهو شعور الجميع بضرورة الارتقاء بالمعلومة لكي يصبح لها مدلول وقيمة تتفق مع الجانب الاقتصادي وقد تساوت جميع الشعوب والدول في عملية الصراع بين التقليد والتجديد في الإنترنت، وحتى الدول التي أخذت خطوات قانونية ولم يتم وضع جديد يذكر وإنما حاولت في نطاق نظمها التقليدية التجديد في مظاهر تعاملها مع الظواهر الجديدة والحقيقة إن اتجاهات التعامل التقليدي مع الإنترنت لم يكتب لها النجاح ما لم تأخذ بمبدأ التطور، وحتى محاولات إصدار تشريعات خاصة فهي محاولات لم تضع حلولاً تتناسب مع قيمة الحدث العلمي للإنترنت إضافة إلى القصور الذي شابها وخير دليل التعديلات المتكررة التي أجريت عليها ومن ذلك التشريع الأمريكي, وكل ذلك يقودنا إلى ضرورة بروز اتجاهات جديدة في التعامل القانوني مع الإنترنت وإن التطور العلمي في مجال قانون الإنترنت يوحي بجدارة موضوعها وأهميته في المستقبل للأجيال القادمة , ويكفي أن نورد أن النظام القانوني الأمريكي أستغنى مرحلياً عن نظام السوابق القضائية مستعيضاً بآليات نظام التقنين لكي يوائم بين الحركة القانونية والتشريعية وبين ظاهرة الأنترنت فاليوم بعد مرور سنوات من الاستعانة الأمريكية بمدرسة التقنين، ظهر فقه أمريكي يطالب بالعودة وإعادة الثقة في نظام السوابق لديهم , خاصة بعد قيام الاجتهاد القضائي عندهم بدوره الطبيعي في معالجة كافة القضايا والمنازعات ذات العلاقة بالانترنت ومن اشهر الفقه في هذا الإطار كتاب البروفيسور (أورن كير) أستاذ قانون الانترنت (نطاق الجريمة الافتراضية) الذي طالب فيه صراحة بالعودة إلى نظام السوابق وإعادة الثقة فيه , وقد قام أستاذنا الدكتور/ عمر محمد بن يونس من ليبيا بترجمة هذا الكتاب إلى العربية خلال سنة 2004م وقد أثرى المكتبة العربية بهذا الكتاب.

المبحث السادس

مدارس قانون الانترنت

من خلال تتبعنا لمراحل تتطور قانون الانترنت ومدارسه المختلفة نجد أن هذه المدارس بنيت عل فكرة المصلحة في تطورها التاريخي, ويمكننا أن نحصر أهم المدارس التي تناولت قانون الانترنت وهي :-

أولا :- مدرسة قانون الحاسوب Computer law .

بدأ ت هذه المدرسة على يد نائب في الكونجرس الأمريكيRIBIKOFF عندما تقدم بمشروع قانون الجريمة إلى الكونجرس الأمريكي سنة 1977م, وتم رفض هذا المشروع لأنه تحدث عن الحاسوب كأداة تخزين فقط في الوقت الذي كانت فيه مسألة تنفيذ بوادر النظام التراسلي في الأفق , إلا أنه وإن كان هذا المشروع قد رفض على المستوى الفدرالي فإنه تم تبنيه على المستوى الولائي فقد أخذت به ولاية فلوريدا, وكان ذلك نتيجة ظهور الحاسوب وبروز إمكانيات تقنية المعلومات التي خلفت واقعاً جديداً ترتبت عليه أثار قانونية مختلفة سواء إجرائية أو موضوعية لذلك كان ظهور هذه المدرسة لأجل حماية البيانات الشخصية المخزنة بالحاسوب، والذي يوفر الحماية للحق فيالخصوصية للأفراد مستخدمي الحواسيب , وتوفير الحماية للمعلومات والتي تشكل قيمة اقتصادية ومواجهة أثار ومخاطر القرصنة (الاختراق لهذه البيانات والمعلومات).

ثانياً :- مدرسة التقنيين

بعد ارتفاع مؤشرات استخدام الحوسبة والرقمية في الأنشطة الاقتصادية المختلفة على المستوى التجاري والاقتصادي وظهور مهن جديدة إثر ثورة تقنية المعلومات والرقمية ومثالها مهنة تصميم وتطوير البرمجة وبروز معالم الأقتصاد الرقمي، ولقد ظهرت هذه المدرسة بعد مدرسة قانون الحاسوب في الفترة ما بين سنة1993م و1997م إلا أن هذه المدرسة لم يكتب لها الاستمرار إذا أخذ في الاعتبار نقص الوعي القانوني للتقنيين عامة ومثل هذا الأمر جعل مساحة الإباحة تطغى على قاعدة الإدارة والقانون.

ثالثاً :- مدرسة التنظيم الذاتي للعالم الافتراضي

مع انتشار الانترنت وظهور فكرة العالم الافتراضيCyber Space واعتراف الفقه المقارن به، بدأ الجدل الفقهي حول مسألة تنظيم هذا العالم وكان فقه القانون الأمريكي أول من بدأ بهذه الدعوة. وظهور هذه المدرسة كان على يد الفقيه اللاهوتي John Perry Barlow مايعرف Self-Regulator وهوا أستاذ في كلية الحقوق - جامعة هارفارد – ومرجعية كبيرة لدى فقه قانون الانترنت , وهو الذي أصدر إعلان استقلال العالم الافتراضي عام 1997م – على إثر انعقاد مؤتمر دافوس (سويسرا)عام 1996م وتضمن الإعلان ضرورة عدم تداخل النظم الحكومية في عمل الانترنت وتركها تنظم ذاتها بذاتها , وقد ذكر هذا الإعلان بعض مبادئ هذه المدرسة وكان أهمها :-

1. الفضاء الاجتماعي العالمي الذي نقوم ببنائه يكون طبيعاً مستقلاً عن مظاهر التسلط علينا.
2. العالم الافتراضي لا يقع في حدود.

3. سوف تبرز هذه الحكومة الذاتية على أساس شروط عالمنا.
4. عالمنا هو عبارة عن كل مكان ولا مكان.
5. نحن نقوم بابتكار عالم يكون لأي كان الدخول آلية بدون امتياز أو أحكام مسبقة مبنية على اساس عرقي أو سلطة اقتصادية أو قوة عسكرية أو مكان ميلاد.
6. نحن نقوم بابتكار عالم يكون لكل فرد وفي أي مكان أن يعبر فيه عن معتقداته دون أهمية لمدى فرديته بدون خوف من أن يتعرض للإكراه على الصمت.
7. إن المفاهيم القانونية للملكية والتعبير والشخصية وما إلى ذلك لا تنطبق علينا فهي كلها تم وضعها بشكل مادي، وهناك لا يوجد مادة.
8. تحاول الحكومات حذف فيروس الحرية بتنصيب حارس على حدود العالم على حدود العالم الافتراضي ومثل هذا يمنع العدوى لبعض الوقت.
9. سوف نبني حضارة للعقل في العالم الافتراضي يمكن أن تكون أكثر إنسانية وعادلة غير ذلك العالم الذي تم إعداده في السابق.

ويلاحظ على هده المدرسة أن أساسها سياسي لدعم موقف الولايات المتحدة الأمريكية , إلا أن هذه المدرسة لم تنتشر الانتشار المقرر لها ودلك للأسباب التالية :-

1-أن التوجه في مدرسة التنظيم الذاتي هو سياسي يخدم أغراض الولايات المتحدة الأمريكية بطريقة أو بأخرى، ويمكنها من الاقتصاد الرقمي.

2-أن اقتناع فقه القانون بمسألة الإدارة الرشيدة والحوكمة لم تكن محل اتفاق أو أجماع , وإنما كانت لغرض تقوية موقف الولايات المتحدة الأمريكية اتجاه منظمة تحديد الأسماء و الأرقام عبر الانترنت الايكان ICANN.

رابعاً /مدرسة التنظيم القانوني و الاقتصادي للعالم الافتراضي:-

على أثر الصراع الفقهي والقانوني حول دور الانترنت تحديداً وخاصة مع انتشار العقود الرقمية والجريمة الافتراضية، انبرى بعض الفقه القانوني والاقتصادي وفقه الإدارة للتصدي للظواهر السلبية ودراسة تطوير الظواهر الإيجابية عبر الانترنت، وكان لدور المحامين ورجال النيابة العامة في النظم القانونية المقارنة (الولايات المتحدة الأمريكية) الدور الكبير في نشأة أتجاه يراعي ضرورة التدخل القانوني وكان لنشاط الأدب المعلوماتي الدور الملموس في مد الحركة القانونية والقضائية المذكورة بمصطلحات جديدة ساهمت في تزكية وكينونة هذه المدرسة التي اعتمدت على التمييز بين النظام التراسلي واعتباره الأصل وبين نظام التخزين وهو استثناء , وتقوم هذه المدرسة على أساس المعيار الوظيفي للحوسبة والرقمية وهي المدرسة السائدة في العالم الآن.

ومن تداعيات مدرسة التنظيم القانوني ما نلاحظه في التشريعات المقارنة وأحكام المحاكم والتي منها على سبيل المثال ما قضت به الدائرة الثالثة الفيدرالية الأمريكية في حكمها والذي قضى (لقد قضت

المحكمة بأنه إذا كان الكونجرس قد حصر قيام الحكومة بتنظيم الانترنت في الحد الأدنى المطلوب فإنه يجب الأخذ في الاعتبار أن سياسة الولايات المتحدة الأمريكية هي ضمان تنفيذ القانون الجنائي الفيدرالي لمنع وعقاب الاتجار بالفحش و الإزعاج العاكسات أو المطاردات باستخدام الحاسوب) كذلك من تداعيات هذه المدرسة عدم تطبيق تشريعات الهاتف على جرائم الانترنت، وفي حكم للمحكمة الإستئنافية الفيدرالية الأمريكية قضى (مثار التساؤل في هذه القضية النظر فيما إذا كان قانون حماية المستخدم الهاتف (TCPA) وهو قانون فيدرالي ينطبق على البريد الإلكتروني الدعائي المحظور Spam أم لا؟. بعض الفقهاء عقدوا مقارنة بين خدمات الهاتف وبين البريد الالكتروني والمحكمة تنتهي إلى الأخذ بالرأي القائل بالاختلاف) كذلك قامت هذه المدرسة بوضع مجموعة تعريفات للمصطلحات التي ظهرت أثر التنظيم القانوني للانترنت ومثالها التوقيع الالكتروني فقد عرفته المحكمة الإستئنافية (الدائرة التاسعة الفيدرالية الأمريكية) حيث قضت (أن مصطلح التوقيع الالكتروني تم تعريفه في القانون الفيدرالي بأنه صوت أو رمز أو معالجة الكترونية ملحقة أو مشتركة منطقياً مع عقد أو أية تسجيل تم إعداده وتنفيذه من قبل شخص بقصد التوقيع على السجل). بل أجازت التشريعات المقارنة استخدام الانترنت في التحقيق وجمع المعلومات باعتبارها أداة تواصلية، ونلاحظ ذلك بوضوح في حكم المحكمة الأستئنافية لولاية نيويورك 1998م – حيث نص الحكم على الآتي (قررت المحكمة في القضية أن استخدام الانترنت كأداة تحقيق من قبل النائب العام في الولاية لا يخالف القانون) , ولقد فرض الواقع العملي في التشريعات المقارنة القبول بالدليل الالكتروني أمام القضاء الأمريكي وفي حكم للمحكمة الاستئنافيه الأمريكية الدائرة التاسعة الفيدرالية، حيث قضى الحكم على أنه (أمكانية قراءة شهادة الشاهد أن لم يكن هناك إمكانية لحضوره في الجلسة). و برزت عدة اتجاهات لتفسير قانون الانترنت سنتعرض له في المبحث القادم.

المبحث السابع

اتجاهات التفسير في قانون الإنترنت

عندما برز مصطلح العالم الافتراضي شرع الفقه في بحث مسألة تحديد هذا المصطلح الجديد وتوصل الفقه المقارن إلى فكرة العالم الافتراضي كحقيقة باعتباره العالم الذي خلقته الإنترنت ليكون أرضاً جديدة يخترقها الإنسان، وفي إطار تفعيل فكرة وجود قانون لهذا العالم الافتراضي برز اتجاهان الأول/ هو الاتجاه المجازي والثاني الاتجاه الوظيفي.

أولا/ الاتجاه المجازي

وهو اتجاه المحكمة العليا الأمريكية في أول حكم لها في موضوع مواءمة الدستور الأمريكي مع الحيز الذي تشغله الإنترنت باعتباره مكان خارج الحدود الإقليمية وليس له نطاق جغرافي محدود ولكنه متوافر لكل شخص في كل مكان حول العالم ولقد تفرع عن نطاق الإنترنت أو عالمها الافتراضي الكثير من المصطلحات المرتبطة به مثل المستقبل في العالم الافتراضي- مجال العمل عبر العالم الافتراضي- الحكومة الافتراضية- الجغرافية الافتراضية- تاريخ العالم الافتراضي- المكان الافتراضي- الزمن الافتراضي – العقود الافتراضية...إلخ على أن أهم مصطلح تفرع عن نطاق الإنترنت ويعد أحد مصادره هو النطاق القانوني للإنترنت والمعروف ((Cyber law) وهو مصطلح مبتكر ويشير إلى ((ذلك الفرع من فروع القانون الذي يهتم بالموضوعات القانونية المرتبطة بالإنترنت وخدمات الاتصالات ,على أن هذا الاتجاه اندثر الآن وذلك بسبب ان توجه الفقه إلى استخدام التفسير التقليدي في القواعد الجديدة في هذا الاتجاه في التفسير ثبت فشله فلا يمكن مثلاً تفسير البريد الالكتروني أو طريقة عمله على ضوء التفسير المعطى للهاتف وحركة الاتصالات عبره لمجرد أنه في زمن سابق كان خط الهاتف يربطنا بالانترنت.

ثانياً/ الاتجاه الوظيفي

ويرى مؤيدو هذا الاتجاه أنه ليس من الضروري أن يتم الاعتماد على التفسير التقليدي للإنترنت بأنها نتيجة لتطوير في حركة الاتصالات بل هي في الحقيقة من تداعيات تطوير تقنية معلومات فمثلاً بسبب وجود بدائل مختلفة عبر الإنترنت فإنه لا يمكن تشبيه الإنترنت أو غيرها من وسائل الاتصالات ووفقاً للاتجاه الوظيفي فإن تفسير قانون الإنترنت أو التفسير الذي يتم في إطار موضوعات تتعلق باستخدام الإنترنت والتعامل بها يجب أن يأخذ طابعاً وظيفياً مستمداً من فهم آلية عمل الإنترنت ووظائفها دون تشبيهاً بأي مظاهر من العالم المادي المحسوس.

لذلك ظهرت فلسفة جديدة تتبنى فكرة استقلالية التنظيم القانوني للعالم الافتراضي الذي نشأ جراء تواصل الحواسيب والشبكات فيما بينها وهذا الاتجاه ينظر إلى الإنترنت من خلال أدائها لمجموعة من الوظائف والمهام فيعد نطاقاً لقانون الإنترنت كل مكان بحيث يتم التراسل وإعداد الصفحات والبوابات حول العالم وهذا الاتجاه أكثر شيوعاً في الاستخدام.

أن ظهور الاتجاه الوظيفي للتفسير في قانون الانترنت كان من تداعيات مدرسة التنظيم القانوني للانترنت وانتشارها بشكل سريع، ونلمس هذا الاتجاه من خلال التشريعات والأحكام في النظم المقارنة، وأهمها أحكام المحاكم الأمريكية فقد ساعدت في إرساء مفاهيم ومصطلحات قانون الانترنت والتنظيم القانوني لها وتفاعلت مع هذه المصطلحات بشكل سريع وقانوني، ومنها على سبيل المثال تعريفها للمستخدم ففي حكم للمحكمة الأمريكية قضى بأن(المستخدم user كلمة تعود إلى الحاسوب ذاته وليس إلى عضو الانترنت في الصورة الدقيقة لهذا المصطلح). وفي حكم للدائرة التاسعة الفيدرالية الأمريكية أنه (عند زيارة أي موقع فإن ملفات ما تهبط آلياً إلى ذاكرة التخزين المؤقت للانترنت Temporary Internet Cache في القرص الصلب للحاسوب دون أن يتوقف ذلك على رضاء مستخدم الانترنت). وفي حكم للدائرة التاسعة الفيدرالية الأمريكية عرفت فيه مصطلح التوقيع الالكتروني حيث قضى الحكم على أنه (مصطلح التوقيع الالكتروني تم تعريفه في القانون الفيدرالي بأنه صوت أو رمز أو معالجة الكترونية ملحقة أو مشتركة منطقياً مع عقد أو أية تسجيل تم إعداده وتنفيذه من قبل شخص بقصد التوقيع على السجل). كذلك عرفت الدائرة العاشرة الفيدرالية الأمريكية مراسل الانترنت في حكم لها حيث قضت (مراسل الانترنت Internet Messenger هو خدمة برمجية تقدمها شركة AOL، وهي خدمة تسمح للأفراد بالاتصال باستخدام الرسائل المكتوبة التي تظهر عند إرسالها في قائمة مراسلات المرسل إليه).

ولقد عرفت الدائرة الفيدرالية الثالثة الأمريكية العدوان الفيروسي عن بعد من خلال حكم لها خلال سنة 2001م , حيث قضى الحكم (لكي يمكن القول بوجود عدوان فيروسي عن بعدRemote Access باستخدام الدودة عبر الانترنت فإنه يجب أن يكون هناك إدعاء بأن تخريب النظام الحاسوبي قد تم عن بعد أيضاً)أما الدائرة الثانية الفيدرالية الأمريكية فقد تعرضت لتعريف الملف المضغوط في حكم لها بتاريخ 2002م وقضىالحكم (أن الملف المضغوط بنظام Zip يمكنه أن يحمل في محتواه مئات الملفات الأخرى وبما يسمح للمستخدم بإنزال الملفات دون حاجة بعد ذلك لإعادة حفظ كل ملف على حده).

وهناك حكم للدائرة التاسعة الفيدرالية الأمريكية سنة 2002م يتعلق بذاكرة المتصفح على الانترنت حيث جاء في نص الحكم « أن ذاكرة المتصفح Browser Cache تحتوي بشكل آلي على صور (ملفات) تم تخزينها في الحاسوب بمجرد قيام المستخدم بزيارة الموقع ومن تم فإنه حين يقوم المستخدم بزيارة الموقع مرة آخري فأن الحاسوب لن يقوم بإنزال الملفات مرة أخرى « .

ولقد عرفت الدائرة الأولى الفيدرالية الأمريكية سنة 2001م المودم من خلال حكم لها الآتي (المودم هو

أداة الكترونية تجعل تراسل البيانات ممكناً من وإلى الحاسوب عبر خطوط الهاتف والاتصالات) وفي مسألة أن الذاكرة الإلزامية للحاسوب لا تعتبر دليل إدانة ما لم يتم إنزال المحتويات في ذاكرة الحاسوب وحفظها وهي من المسائل التي ظهرت نتيجة انتشار الجرائم عبر الانترنت ولقد صدرت الدائرة الثامنة الفيدرالية الأمريكية خلال سنة 2002م حكماً يتعلق بهذه المسألة حيث قضى الحكم (لا يجوز إدانة الشخص عن مجرد قيامه بالإبحار في مواقع دعارة عبر الانترنت وبالتالي لا يعد دليلاً جنائياً وجود نسخ في الذاكرة الإلزامية للمتصفح(Browser Cache), ولا يعد ذلك حيازة لصورة دعارة ما لم يتم إنزالها بشكل تقليدي وحفظها في الحاسوب) , ومن ضمن مصطلحات الحاسوب (Delete) والتطهير erase ولقد عرفتها الدائرة الثالثة الفيدرالية الأمريكية سنة 2001م , في حكم لها قضى (أن كلمة (Delete) في نظام الحاسوب تتشابه ورمي ورقة في سلة المهملات، أما كلمة تطهير أنها تتشابه مع أخذ الورقة التي تم رميها في سلة المهملات والقيام بتقطيعها إلى قطع صغيرة ثم قذفها في الهواء). ومن ابرز ما توصل إليه الاتجاه الوظيفي المعاصر هو البحث بدقة في تفسير عبارة المستخدم user حيث انتهى إلى نظرية الشخص الرقمي التي نعرض لها في الفقرة التالية :-

الشخص الرقمي:-

كان البناء التقليدي لنظرية القانوني يتناول الشخص الطبيعي والشخص الاعتباري باعتبارهما نقطة الارتكاز في كافة المعاملات القانونية والاقتصادية. وحتى بداية الألفية كان هذا الرأي القانوني قد مضى عليه قرن كامل تكامل به الفكر القانوني واثرى معالم النقاش في إطار المسئولية القانونية واثار جدل كبير حول المسئولية القانونية و تحديدا الجنائية فيما يتعلق بالمسئولية الجنائية للأشخاص المعنوية حيث اجتهد الفقه الجنائي والمشرع في هذا الإطار اجتهادات نالت حظها أيضا من النقاش المتواصل. ومع بداية الألفية ظهر علينا القضاء المقارن بنوعية جديدة من الأشخاص تضاف إلى ما ذكر سابقاً ممثلة في الشخص الرقمي في قضية أمام القضاء الأمريكي هى قضية Double Click ولكن تم الاعتراف في وقت مبكر كنتاج للحوسبة والرقمية. حيث قرر القضاء الأمريكي الاعتراف بالشخص الرقمي مطبقا ذلك على مواقع شبكة المعلومات الدولية الويب. وتطرق الامر لابعد من ذلك حين تناول تلك المواقع من حيث الاختصاص في قضية أخرى شهيرة هي قضية ليدوف Lidov التي جعلت الاجتهاد القضائي محلا لتطوير الدراسات والأبحاث. ففي القضية الأولي بدأ الاجتهاد القضائي يتناول موضوع التمييز بين المستخدم User وتحليل هذا المصطلح لكي يتوصل إلى المعنى الحقيقى له من خلال الاتجاه الوظيفي في قانون الانترنت حيث وجد ان البشري او الإنسان ليس مستخدما وإنما المستخدم الفعلي هو الحاسوب ذاته. ولقد أثيرت على اثر هذا الاجتهاد العديد من الاستفسارات حول تحديد طبيعة الدور الذي يقوم به البشري او الإنسان هنا ومداه ويكاد ينتهي الرأي الى ان الإنسان هو المستفيد من حركة تقنيات المعلومات بصفة عامة فليس هو المستخدم، على أن أهم ما في هذا الموضوع من إشكاليات مثارة تجعل إضافته الى دراسات

المدخل لنظرية قانون الانترنت امراً لازما وحيويا لكي يتاح للفقه القانوني المجال لبحث ودراسة لمثل هذا الموضوع. فالمسألة فيما يبدو تحتاج الى إجابات كثيرة يتمثل اغلبها في طرح الأفكار سعيا إلى تحقيق اجتهاد يتفق مع إدخال تقنية المعلومات في النسيج الاجتماعي والاقتصادي للمجتمع الإنساني. وهذا أمر فرضه التكيف الذي يكاد يكون طبيعيا بين البشر وبين الحوسبة والرقمية، فقد أمكن للفقه تحديد معالم الشخص الطبيعي و المعنوي بصورة قننها المشرع المقارن في التشريعات المعاصرة. فمثلا تبدأ حياة الشخص الطبيعي من واقعة الميلاد وتنتهي بالوفاة وعلى الراجح بتوزيع ارثه بين ورثته من الناحية الاقتصادية. والشخص المعنوي تبدأ حياته من اشهاره وتنتهي بالتصفية. والسؤال يثار على اثر الاعتراف القضائي بالشخص الرقمي في مثل هذه الامور. ميلادة ووفاته وطبيعة نشاطه واثر كل ذلك في القانون وعلى المجتمع. على ان الامر لم يتوقف عند هذا الحال. بل ازداد الأمر صعوبة حين اجتهد القضاء المقارن لكي يضع الاجابة حول قواعد فنية عميقة ذات علاقة بمصالح الناس خاصة مع بروز سمات الاقتصاد الرقمي وهو ما يمثل القيم المالية في اصول تقنية المعلومات ككل ومن ذلك قواعد الاختصاص القضائي التي سمح فيها القضاء بالدخول في حومة تقنية المعلومات لكي يقنن العديد من المفاهيم فتناول موضوع الاختصاص الرقمي وتقسيماته الجديدة إلى اختصاص ايجابي ويتناول الاختصاص بالمواقع الايجابية وذلك السلبي الذي يمتد فقط إلى المواقع السلبية.

لذلك يعد مجنيا عليه او متضررا من الجريمة كل من الشخص الطبيعي والاعتباري وكذلك الرقمي بحسب تطوره, والسعي الحثيث لدى فقه نظرية التنظيم القانوني والاقتصادي للانترنت يستهدف إثبات تلك العلاقة بين الشخص الاعتباري والحوسبة والرقمية. كما ان هناك منطقة أضحت مفقودة في تركيبة الشخص ككل في نظرية القانون (طبيعي- اعتباري) منذ حكم القضاء المقارن هنا. فنظرية الشخص الاعتباري التي تنبأ بسطوتها العديد من الفقهاء العالميين ومن بينهم الفقيه العربي البارز المرحوم/ عبد الرزاق السنهوري في نظرية العقد عام 1934م بدأت تتقلص مع بروز نظرية الشخص الرقمي والتي طبقها القضاء المقارن في عام 2001م على صفحات شبكة المعلومات الدولية/ الويب تحديدا معتبرا اياها مستخدما مما جعل مسألة المستفيد تظهر في الأفق. فالمستفيد هو الشخص الطبيعي حتى الان. والمستخدم هو الشخص الرقمي. والحاسوب لا يعرف بذاته في الحقيقة ما اذا كان موجودا في منزل او في مؤسسة وكل ما يدركه الحاسوب هو ان هناك من يصدر اليه الأوامر فيقوم بتنفيذها اذا كانت المعطيات الموجودة فيه تحتمل ذلك.

أن قدرات الحوسبة والرقمية وصلت الى أن اعترف القضاء المقارن بالشخص الرقمي وهو غير الطبيعي والاعتباري وكذلك الاعتراف بعلاقات الشخص الرقمي بقدرات المثلث العالمي الجديد (خريطة الجينوم- الحوسبة والرقمية- الاقتصاد الثالث). وهو المثلث الذي يحكم العصر الرقمي، إن الأمر يتطور أيضا الى تقرير مسألة ذات مكانة خاصة ازاء تنوع السلع وكثرة حركة الإنتاج واستخدام سياسات خاطئة لتسويق المنتجات والسلع والخدمات..الخ كنتيجة طبيعية لعدم وجود تنظيم للتسويق

والتوزيع التجاري وتتعلق هذه المسألة بحماية المستهلك. والحقيقة أن مسألة المستهلك Consumer في اطار علاقات قانون الانترنت والتجارة الالكترونية تتنازعها مشكلات مقابلة هذا المصطلح بمصطلح المستخدم User. وحتى الأن فإن القدر المتيقن في هذا الاطار أن عبارة المستهلك تم استنباطها من الفكر الاقتصادي لعبارة المستخدم، في الوقت الذي لم يتم شمول عبارة المستخدم بتعريف جامع مانع، حيث تداخلت في تكوين عبارة المستخدم فضلا عن الشخص التقليدي (الطبيعي- الاعتباري) الشخص الرقمي أيضا، ولقد تضمن مشروع الجرائم الافتراضية والدليل الرقمي في ليبيا النص على الشخص الرقمي ومن ذلك ما تقرر في نص المواد 58 و61 و لقد وضحت المذكرة الإيضاحية للقانون المادة (58) على النحو الأتي:-

(تبنى فكرة المسئولية الرقمية على منهجية الاعتراف بالرقمية تحديدا، وهو ما تقرر في المادة (1/2) من مشروع القانون الليبي بقولها (الرقمية منهج) وهو المعنى الذي يمكن من خلاله تفسير التشريعات النافذة بما يتواءم مع الرقمية. وبحيث يتم التخلي عن الاتجاه المجازي في التفسير قدر الإمكان والدخول في حومة الاتجاه الوظيفي الذي يتفاعل واقعيا مع حركة الحوسبة والرقمية ووظائف النظام التراسلي وكيفية عمل نظام التخزين..الخ. وهذه كلها أمور تجعل من المقبول أن يترتب على الخطأ فيها مسئولية ما. ولكن لا يمكن نسبة هذه المسئولية كمطلق إلى المسئولية المدنية او الجنائية مباشرة وإنما يجب أن ينظر الى هذه المسئولية على أن لها طبيعتها الخاصة. وهذا الأمر على درجة من الأهمية لأن بناء هذه المسئولية يجعلها مختلفة نسبيا عن المسئولية المدنية او الجنائية التي يعرف إبعادها وطبيعتها فقه القانون والتي لها تاريخ كبير معتمدة في بناء القاعدة القانونية عموما. ويكفي في هذا الشأن التقرير كسند لوجود هذا الشكل الجديد من المسئولية (الرقمية) أنه ليس كل نشاط رقمي تسبب في ضرر للغير يلزم مرتكبه بالتعويض.. ذلك أن البناء المنطقي للحوسبة والرقمية يجعل خطواتها المتعددة والمختلفة، بما في ذلك الافكار التي بدأت تأخذ مجراها قضاء وفقها حول الشخص الرقمي، تجعل من المستحيل التخلي عن فكرة وجود المسئولية الرقمية).

ونصت المادة 61 (تسري نصوص هذا القانون على الشخص الطبيعي والشخص الاعتباري. وليس في هذا القانون ما يبرر عدم الاعتراف بالشخص الرقمي).

ولقد وضحت المذكرة الإيضاحية هذه المادة علي النحو الأتي:-

السير الطبيعي للمفاهيم القانونية أن الترتيب لنظرية الشخص في القانون أنها تأخذ الوضع التالي:

-الشخص الطبيعي.

-الشخص الاعتباري.

على أن الأمر في الواقع ليس كذلك، فليس هناك سطوة للشخص الطبيعي في مواجهة الشخص الاعتباري. وهذا الأمر كشف عنه الفقيه عبد الرزاق السنهوري في كتابه (نظرية العقد) الذي أصدره عام 1934. حيث غلب على هذه الدراسة تحديد الطبيعة المستقبلة (آنذاك) للشخص الاعتباري. ومن هذا الكتاب الرائد نستطلع أن ترتيب الأشخاص في نظرية القانون يجب أن تكون على النحو التالي:

-الشخص الاعتباري.

-الشخص الطبيعي.

على أن الأمر لا يقف عند هذا الحد. فمع التطور والانتقال إلى العصر الرقمي أصبحت الحاجة ملحة إلى استيضاح دور الآلة هنا. ففي عام 2001م. وضع القضاء المقارن أساسا جيدا للاعتراف بالشخص الرقمي. ونرى ذلك في هذه الجزئية من الحكم التالي:

In re DOUBLECLICK INC. PRIVACY LITIGATION, This Document Relates To:) NRB) UNITED STATES DISTRICT) 0641 .Civ 00 .ALL ACTIONS. Master File No ;497 2d .F. Supp 154 COURT FOR THE SOUTHERN DISTRICT OF NEW YORK at 2005 .Filed available on line in Nov ,2001 ,29 March 3498 U.S. Dist. LEXIS 2001 readings/doubleclick.html/ "DoubleClick argues that/http://cyber.law.harvard.edu/is02 its conduct falls under this exception. It contends that the DoubleClick-affiliated Web sites are «users» of the Internet and that all of plaintiffs› communications accessed by DoubleClick›s cookies have been «of or intended for» these Web sites. Therefore, it a)›s)2701 § asserts, the Web sites› authorization excepts DoubleClick›s access from were DoubleClick-affiliated Web sites «users» of this (2)…general prohibition service?;…. This court takes judicial notice of the fact that all people and entities that utilize Internet access subscribe to ISPs or are ISPs. Although the vast majority of people who sign-up for Internet access from consumer-focused ISPs such as America Online every Web site, company, university, and government [32] ,and Juno are individuals agency that utilizes Internet access also subscribes to an ISP or is one. These larger entities generally purchase «Internet access» in bulk from ISPs, often with value-added services and technologically advanced hardware. Nevertheless, they purchase the same underlying Internet access as individual users. Therefore, plaintiffs fail to distinguish class members from Web sites and servers based on whether they subscribe to an ISP for Internet access…. Again, plaintiffs seem to ignore the statute›s a) embodies plaintiffs› position that)2701 § plain language. The general rule under only those authorized to use a «facility» may consent to its access. Nevertheless, s‹(2)(c)2701 § a)›s general rule subject to)2701 § Congress explicitly chose to make electronic [33] exception for access authorized by authors and intended recipients of communications. Thus, plaintiffs› argument is essentially that this Court should ignore because Congress failed to take adequate account of «basic property and (2)(c)2701 §

privacy notions.» However, it is not this Court›s role to revisit Congress› legislative judgments. One final point bears mention, even though plaintiffs did not raise it. One could imagine a facially sensible argument that Web sites are not «users» of Internet access because they are passive storage receptacles for information; the human is the «user» and the Web site is what is used. However, the Internet›s engineering belies this description. Because the Internet functions through packet-switching and dynamic routing, human users do not in any sense connect to a passive receptacle and obtain information. Indeed, no direct connection ever exists between the human user and the Web site. Rather, the human user sends a request to which the Web site must actively respond: processing the request, deciding whether to provide the information sought, obtaining the document from the server, translating the document into TCP/IP protocol, sending the packets and awaiting confirmation of their arrival. Indeed, in a practical sense, Web sites are among the most active «users» of Internet access -- their existence and utility depend on it, unlike humans. Therefore, we find as a matter of law that the DoubleClick-affiliated Web sites are «users» of Internet access under the ECPA.".

والحقيقة لقد أحدث هذا الحكم في القضاء المقارن (الأمريكي) نوعا من تطوير الارتباك. وهو ارتباك تواجد في قوة الشخص الاعتباري في مواجهة الشخص الطبيعي لمرحلة طويلة من الزمن كان فيها البحث العلمي مرتكزا على الترتيب التقليدي لنظرية الشخص في القانون. وبحيث تعد الافضلية للشخص الطبيعي في الوقت الذي لم يكن ذلك صحيحا في الواقع العملي. ومع التطور الجديد أصبح من المفترض أن ينظر الى ترتيب نظرية الشخص في القانون على النحو التالي:-

-شخص اعتباري.

-شخص طبيعي.

-شخص رقمي.

على أن الأمر ليس كذلك في الحقيقة. فهذا الترتيب هو ترتيب نظري يحقق محاولة غير ناجحة في ترتيب نظرية الشخص في القانون. وذلك لسبب جوهري لاحظه الباحثين هنا. وهذا السبب يتلخص في كون ان نظرية الشخص الاعتباري قد لا يكون لها محل على الإطلاق في إطار البحث في علاقات الترتيب المذكورة. فالحاسوب لا يعرف على وجه التحديد أين موقعه وما اذا كان يتواجد في شركة او مؤسسة او منزل او طائرة او في غير ذلك. لذلك تراجعت نظرية الشخص الاعتباري في إطار الحوسبة والرقمية وأصبح الاعتماد الجوهري يتم بناءه على أساس قوة القطاع الفردي/ الشخص الطبيعي والشخص الرقمي. وإزاء خطورة هذا التراجع على اقتصاديات الدول نهض الرأي السياسي في محاولة لإعادة الحال بالنسبة لقوة الشخص الاعتباري فصدر إعلان

التجارة الالكترونية الأمريكي في عام 1997م معبرا عن أهمية دور القطاع الخاص هنا. ولكن مثل هذه المحاولات لا يمكن الاعتماد على العنصر القهري في القانون لتأكيد وجودها. واذا تأملنا الموقف لوجدنا أن المصادفة لعبت دورا كبيرا في تأكيد قوة الشخص الاعتباري، فقد قامت مسألة على درجة من الأهمية تتعلق بموضوع الحكومة الالكترونية، وهي مسألة الشراء الحكومي الالكتروني الذي ينصب التوعية فيه على أساس مكافحة الفساد ونشر الشفافية وأفكار الإدارة الرشيدة..الخ. وهذا المدخل يصلح في الوقت الحالي لطرح دور المؤسسة ككل. وبالتالي عودة مفاهيم الشخص الاعتباري من جديد الى نظرية القانون في العالم الرقمي. على أن الجزئية التي قد يصاحبها خلل ألان هي مسألة ترتيب الأشخاص في نظرية القانون ولمن السطوة الواقعية.

لذلك جاء نص هذه المادة لكي يقرر الاعتراف بكل الأشخاص في الوقت الذي يقرر أنه ليس هناك في هذا القانون ما يبرر عدم الاعتراف بالشخص الرقمي. ومن ثم تم ولأول مرة اعتراف القانون الليبي بما تقرر في القضاء المقارن. ومثل هذا الاعتراف لا يعد وضعا أو انضماما إلى حل أو رأي دون الأخر بقدر ما يعد تقرير بأن دور القضاء الليبي في نظر هذا النص قد بدأ بالفعل. ويبنى على ما سلف القول بأن كل دفع أمام القضاء بعدم وجود الشخص الرقمي هو دفع في غير طائل. بل أن هذا الشخص تم الاعتراف به وسوف تبين التطبيقات القضائية وجوده. الا أنه يظل مع ذلك دفعا موضوعيا جوهريا تلتزم محكمة الموضوع بالتعرض له والاجاوزت حدود التسبيب.

وإذا تأملنا مسألة الشخص الرقمي هنا. وهذه المسألة الأخيرة جعلت منطق او هيكلة نظرية الشخص في القانون محل اعادة نظر خاصة فيما يتعلق بهيكلة الشخص الاعتباري بالمقارنة للشخص الرقمي والطبيعي. فالغلبة للشخص الرقمي وفق الاتجاهات الحديثة في القضاء المقارن. والمسألة يمكن النظر اليها على ان المعادلة التي تم إرسائها في اطار القانون التقليدي في حاجة الى إعادة قولبة وصنع منهجية اخرى تسمح بمزيد من الاستيعاب لفكرة الشخص الرقمي ووضعيته الجديدة في نظرية القانون وبطريقة تسمح بعدم إهمال هذا الشخص، فإهماله قد يسبب كارثة حقا قد تكون نتائجها وتداعياتها سلبية على النواح الاجتماعية.

الفصل الخامس العالم الافتراضي في الإطار القانوني

الإنترنت هي وسيلة أو أداة تواصلية بين الشبكات دون اعتبار للحدود الدولية ، وهي بهذا المعنى يجعلها ذات طبيعة تقنية تؤدي مهمة الربط التقني بين شبكات الحاسوب من أجل إحداث أو تكوين تواصل معلوماتي والاتصال هذا يكون متفاعل بين عالم الشبكات المختلفة والذي يؤدي إلى توافر المعلومات للجميع دون تمييز حتى في ظل بعض الأفكار التي تدعو إلى سيطرة لغة محددة على الإنترنت فما أن توضع أي معلومة في العالم الافتراضي حتى تكون في حينها متاحة لكل شخص يرغب في التطرق إليها أو الإطلاع على محتواها وعندما تفاعلت تقنية المعلومات مع الاتصال تمكن العلماء من وضع الأساس الأول لموضوع حديث على موضوعات القانون المعروفة والتي في حقيقتها لم تستوعب الموضوع الجديد بطريقتها التقليدية فتبين ضرورة تطويرها بما يتلائم مع الفرع الجديد من القانون لذلك أدرك المشرع المقارن أن تطوير النصوص التقليدية في القانون يمكن أن يبدأ من فكرة تطوير النصوص التقليدية إلى مرحلة تجديدها كلياً بل أتسع فكر المشرع لبحث موضوعات جديدة ترتبط بهذا الفرع الجديد وهو قانون الانترنت.

وإذا كانت فكرة العالم الافتراضي Cyber Space قد ظهرت كفكرة مع أدب الخيال العلمي والتي كانت محض خيال لدى العامة من الناس فإنها الآن حقيقة واقعة تدل على وجود عالم جديد تبدأ حـــدوده(الافتراضية) بمجرد انتهاء حدود الدولة وإن الاتصال بحدود العالم الافتراضي لا يكون عبر الاتصال بالحدود المادية المعروفة، وإنما من الممكن الاتصال بحدود العالم الافتراضي من داخل أية دولة دون عناء يذكر، وهذا العالم محل خلاف فقهي ليس بين مؤيد ومعارض فهي مسألة حسمت لصالح تقنين الإنترنت وتنظيمها القانوني على أثر قيام المشرع المقارن بحركة إصدار تشريعاته حول موضوعاتها المختلفة بل أن بعض التشريعات انبثقت عندما تناولت منطقة العالم الافتراضي بأسلوب التطوير القانوني وهو منهج يعتمد استكشاف الحدث بعد وقوعه وهو منهج المشرع الجنائي المقارن وبالتحديد الأمريكي الذي يعتبر مثال لمدى تفاعل المشرع مع موضوع جديد وكيف أنه تفرد بأساليب مواجهة إشكالياته ولا شك أن الإمكانيات اللآمحدودة لتقنية الإنترنت ساهمت في تكوينها عدة أسباب رغم عدم قدرتنا على حصرها بالتحديد، لذلك نذكر أمثلة منها مسألة عدم وجود سوابق قانونية للإنترنت يمكن من خلالها التعمق في محتوياتها والإطلاع على أسرارها ومسألة عدم إمكانية تحديد الخيال الإنساني الذي يتجدد بشكل يومي كذلك مسألة التطوير المستمر والذاتي التي تستند فيها إلى حرية المنهج مما يترتب عليه ظهور أفاق جديدة في حركة التعامل بين الإنسان وتقنية المعلومات مستقبلاً، وقد أحدث تأثير في الفقه القانوني في دول القانون العام حيث نشط اتجاه قانوني يدعو إلى عدم قدرة القانون العام على التصدي للبحث عن حلول قانونية لإشكاليات العالم الافتراضي. إن القيمة والفائدة التي يمكن أن يجنيها العالم العربي كما فعل العالم الغربي كبيرة إذا أستوعب وأدرك أهمية العالم الافتراضي في توفير المعلومات والبيانات والفائدة التي يمكن أن تقدمها تقنية المعلومات للمواطن العربي أينما

كان وفي كل نواحي الحياة والدفع بالمشرع العربي والأجهزة التنفيذية للقيام بخطوات عملية من الناحية التشريعية والتنفيذية والقضائية لتواكب ما يحدث في العالم الافتراضي فالأثر الذي تركته تقنية المعلومات، أصبح بالعلم يملك العالم ويتحكم فيه. وأن أي قيمة يمكنها أن تتحول إلى العالمية فلم تعد الوسائل التي تلزم للوصول إلى العالمية كما كانت سابقاً تدعمها المنظمات الدولية أو المكانة الدولية للدول أو إتباع قنوات معينة للحصول على اعتراف عالمي بهذه القيمة.

أن منطق العالم الافتراضي خلقته تقنية متفاعلة مع المعلومات ولذلك فالعالم الافتراضي هو العالم الموجود في فرضية حلقة الاتصال الكبرى بين مجموعة الحواسيب متصلة بعضها ببعض في شكل عنكبوتي ليس له شكل محدد يجعل المعلومة ذات أثر امتدادي يسمح بتناولها سواء أكانت تحقق قيمة إستردادية أو إسترجاعية متكررة لها ومثل هذا الأمر الذي يجعل إمكانية وضع المعلومة الواحدة في العالم الافتراضي ، وفي ذات الوقت يمكن أن تحقق استرجاعها أو استردادها بحيث يمكن استدعائها من قبل أكثر من حاسوب في نفس الوقت ومن مختلف أنحاء العالم ولتحديد منطقة العالم الافتراضي للعقل البشري يمكن تفسير حدوده على أنه أول خطوة بعد الحدود الدولية لدولة ما، وهذا المنطق يؤدي إلى انتهاء مفهوم أمن العالم الافتراضي والذي نادى به البعض وهذا الرأي يؤدي إلى وجود نتائج تعكس ما هو مقرر لهذا العالم من سعي إلى إثبات صفته الشعبية أي أنه متاح للجميع.

وترتكز فكرة العالم الافتراضي على ثوابت ومتغيرات، فالثوابت هي الأساس في دخولنا إلى العالم الافتراضي المختفي في تقنية المعلومات وبدونها نبقى في عالمنا المادي وتتمثل هذه الثوابت في الحاسوب بما يحويه من عناصر ثلاث هي القطع الصلبة والمرنة والمعلومات أو في عبارة أكثر حداثة تتفق مع الاتجاه الوظيفي للإنترنت وهي عبارة المحتوى Content أما التغيرات فهي الظروف التي يجب توفيرها للاتصال بالعالم الافتراضي ممثلة في خطوط اتصالات نشطة عن طريق وسيط هو مزود الدخول مهمته إيجاد تواصل قائم بين الحاسوب وبين العالم الافتراضي، ومثالها خطوط الاتصالات التي يتغاير مضمونها بين أسلوب اتصال غير مباشر ومباشر بالإضافة إلى اكتساب مهارة عادية في تشغيل الحاسوب وإحداث الاتصال لكي تكون في ثوان معدودات في عالم افتراضي مثير نسبح فيه بحرية تامة. والعالم الافتراضي حقيقة واقعة ليس هو صورة من واقعنا المادي الملموس بقدر ما يعد صورة من خيالنا الذي نأمل تحقيقه في عالمنا المادي فهو نقطة الالتقاء المثالية التي تصور كل ما يمكن أن نرغب في تحقيقه وكانت هناك بدايات لمسألة التنظيم القانوني للعالم الافتراضي.

الفصل السادس مظاهر الاهتمام القانوني بالعالم الافتراضي

نتيجة الأبحاث والدراسات فقد لاحظ الفقه أن مسألة الحقوق والحريات الأساسية المقررة للإنسانية والتي تأخذ مظهراً دستورياً في المراحل المعاصرة اتجهت إلى فكرة أن يتم الامتداد في التفسير من العالم المادي إلى العالم الافتراضي وبدأ ذلك في القضاء الأمريكي مع قضية Renov.Aclu عندما قضت المحكمة العليا الأمريكية بعدم دستورية قانون أخلاق الاتصالات لعام «1996م» الصادر بشأن تعديل قانون الاتصالات لعام «1934م» وذلك فيما يخص نصوص مكافحة الإباحية على الإنترنت لتعارضها مع التعديل الأول للدستور الأمريكي وهو منطق مثالي يعطينا انطباع بإمكانية وجود هذا المنطق في العالم الافتراضي، وفي فرنسا قدم المجلس الدستوري الفرنسي نقض مشروع قانون قدمه النائب الفرنسي (Fillon) لعام «1996م» بشأن مسؤولية مزود الدخول إلى الإنترنت لوجود تناقض بين الدستور الفرنسي والإعلان الفرنسي لحقوق الإنسان والمواطن وبين المشروع المقدم من النائب .

كذلك مسألة الاختصاص القضائي عبر الإنترنت، فالقضاء الفرنسي أقر بوجود الاختصاص في المشكلات التي تكون لفرنسا علاقة بها على أية شاكلة. أن منطق الحقوق والحريات هي أنها نهج فكري قبل أن تكون مجرد وثائق تقنية، والوثيقة ما هي إلا ضامن لما هو مقرر للإنسان في مرحلة زمنية معينة، ولذلك أقر المجلس البلجيكي مبدأ قبول التصويت عبر الإنترنت في الانتخابات المحلية لمدينة بروكسل وهو لا يتعارض مع العهد الدولي للحريات المدنية والسياسية ولا يتعارض مع الدستور البلجيكي، وكمظهر من مظاهر الاهتمام القانوني بالعالم الافتراضي وأمام أتساع فكرة هذا العالم ومجاله اللامحدود في تقديم خدماته، نشأ اتجاه جديد في تقنية المعلومات ينادي بفكرة الحكومة الإلكترونية والتي بدأت عام «1955م» في أمريكا عندما استلمت مؤسسة الضمان الاجتماعي الأمريكي أول حاسوب لحفظ المعاملات والسجلات المتعلقة بالمشتركين ،وفي عالمنا العربي الفكرة الأولى لما يسمي برنامج ميكنة الإدارة، كانت في ليبيا عام 1972م على يد أستاذنا / محمد أبوبكر بن يونس رحمه الله عندما قدم هذا المشروع لمجلس التخطيط الأعلى آنذاك. أن الإمكانيات الهائلة التي تتمتع بها تقنية المعلومات في قدرتها على حفظ البيانات أظهرت فكرة إمكانية اختزال البيانات إلكترونياً أول بأول للحفاظ على نوع التقنية وتراسلها. وأن فكرة الحكومة الإلكترونية وفق نظرة المبرمجين لا بد من تطويرها لأحداث تواصل بين العالم الافتراضي وبين التشريع. أن وجود المؤسسة عبر الإنترنت لم يتعدى دور الاعتراف بها في العالم الافتراضي ويحتاج إلى إعادة تفعيل الدور المؤسسي المتواجد في عالمنا المادي عبر العالم الافتراضي، وكمثال على ذلك لو حدث عدوان أو سلوك غير مشروع في العالم الافتراضي على صفحة أو موقع مؤسسة ما أو سرقة بيانات أو ملفات منها فكيف يمكن تقبل هذه الفكرة ، لذلك كان الحل الحقيقي في تطوير الطابع المؤسسي لتحميل فكرة المؤسسة ككل وانتقالها إلى العالم الافتراضي هو اللجوء إلى فكرة تجاوب الآلة مع التطوير الإداري، وحدوث تفاعل في القرار مع

عملية مواءمته القانونية بالمشروعية ومن ثم تجاوبه آلياً مع سنده الذي يقوم عليه، كما لو كان سنده القانوني هو التشريع يتطلب ذلك وجود قاعدة بيانات تشريعية متكاملة متوافرة بحيث تكون متفاعلة مع عملية صدور القرار وتكون قاعدة البيانات التشريعية المذكورة هي المعبر الرئيسي إلى عمليات بحث مدى تجاوب القرار المتخذ مع تنفيذه وقد نجحت هذه الفكرة إلى حد ما فيما يتعلق بتجاوب رجال القانون مع مسألة متابعة أحدث التطورات القضائية عبر نظام الاشتراك في المراسلة الإلكترونية التي تبثها منظمات قانونية عبر الإنترنت مثل نظام المراسلة الإخبارية للعديد من المنظمات التي تسمح بالمتابعة القانونية لآخر تطورات الأحكام والبحوث القانونية والتشريعية وأخيراً، أن التنظيم القانوني للعالم الافتراضي هو نتيجة طبيعية لنجاح هذه المدرسة وشعور مؤيدها في فترة قصيرة بعدم إمكانية نجاح مدرسة التنظيم الذاتي للإنترنت وحدها في إرساء معايير تنظيمية لها تكفي بذاتها لكي تقوم بأعمال تنظيم هذه الظاهرة الإنسانية التقنية، بل لاحظ فقهاء القانون أيضاً عدم نجاح فكرة قانون الحاسوب Computer law في إرساء معايير وضوابط قانونية يمكن أن تضبط العالم الافتراضي، لذلك يمكننا القول أن فكرة قانون الإنترنت أو قانون العالم الافتراضي هي الفكرة التي تتواءم مع التطور القانوني الذي يصاحب عملية تنظيم الموضوعات المختلفة عبر الإنترنت.

المراجع

1. د. عمر محمد بن يونس - الجرائم الناشئة عن استخدام الإنترنت. ط 1 – دار النهضة العربية – القاهرة 2004م.
2. المجتمع المعلوماتي والحكومة الإلكترونية – ط 2 مؤسسة آدم للنشر والتوزيع – مالطا – 2008م.
3. أشهر المبادئ المتعلقة بالإنترنت في القضاء الأمريكي ط 1- دار النهضة العربية– القاهرة 2007م.
4. إعلان استقلال العالم الافتراضي - ترجمة إلى العربية – أعمال المؤتمر الدولي الأول لقانون الإنترنت برعاية المنظمة العربية للتنمية الإدارية – الغردقة – مصر.
5. العالم الافتراضي في الإطار القانوني – بحث مقدم إلى دورة حول تطبيقات التنظيم القانوني للإنترنت – شرم الشيخ مصر – خلال الفترة من 26-2006/7/30م – غير منشور.
6. القانون الوطني الأمريكي – المؤتمر الدولي الأول لأمن المعلومات – مسقط – سلطنة عمان – منشورات موسوعة التشريعات العربية.
7. الحصة الرقمية – أصول تقنية المعلومات والمعرفة – الإسكندرية 28-2005/8/31م – المنظمة العربية للتنمية الإدارية – جامعة الدول العربية.
8. د. مصطفى مصباح أدبارة – الإرهاب (مفهومه وأهم جرائمه في القانون الدولي الجنائي) رسالة ماجستير – جامعة قاريونس – ط 1 – 1990م – منشورات جامعة قاريونس – بنغازي ليبيا.
9. عبد الباسط محمد الزوام – منهجية قانون الإنترنت – بحث مقدم لدورة الإنترنت والعدوان الفيروسي خلال الفترة من 24-2009/5/25م – طرابلس ليبيا.
10. مقال منشور حول التنظيم القانوني للإنترنت على موقع (www.Kashada.com) تاريخ الزيارة 2010/6/19م.
11. مشروع قانون الجرائم الافتراضية والدليل الرقمي (مقترح موسوعة التشريعات العربية) ليبيا.
12. المذكرة الإيضاحية لمشروع قانون الجرائم الافتراضية والدليل الرقمي في ليبيا – (مقترح موسوعة التشريعات العربية).
13. السجل القومي المجلد 31 – الجزء الأول منشورات المركز الليبي – ليبيا 2000م.
14. السجل القومي المجلد 31 – الجزء الثاني منشورات المركز الليبي – ليبيا 2000م.
15. السجل القومي- المجلد 31- الجزء الثالث منشورات مركز الليبي – ليبيا 2000م.
16. صحيفة الفجر الجديد – العدد (12819) الصادرة بتاريخ 2010/11/30م.
17. القانون رقم 1 لسنة 2005م/ بشأن المصارف مدونة التشريعات – العدد منشورات مؤتمر الشعب العام.
18. القانون رقم 12 لسنة 2010م. بشأن علاقات العمل مدونة التشريعات العدد 7 – السنة العاشرة منشورات مؤتمر الشعبي العام.
19. قانون الجمارك رقم 10 لسنة 2010م مدونة التشريعات العدد (5) السنة العاشرة منشورات المؤتمر الشعبي العام.

20. قانون التسجيل العقاري وأملاك الدولة رقم 17 لسنة 2010م ومدونة التشريعات – العدد.
21. القانون رقم 20 لسنة 2010م بشأن التأمين الصحي مدونة التشريعات العدد (10) السنة العاشرة منشورات مؤتمر الشعب العام.
22. القانون رقم 22 لسنة 2010م بشأن الاتصالات – مدونة التشريعات – العدد 10 – السنة العاشرة مؤتمر الشعب العام.
23. المجلة العربية لقانون الإنترنت – العدد (1) السنة الأولى 2005م منشورات المنظمة العربية للجنة الإدارية القاهرة - 2006م.
24. القانون رقم (3) لسنة 2014م بشأن مكافحة الإرهاب.
25. المراجع الأجنبية:

• In re DOUBLECLICK INC. PRIVACY LITIGATION, This Document Relates To: ALL ACTIONS. Master File No. 00 Civ. 0641 (NRB) UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK 154 F. Supp. 2d 2001 ;497 U.S. Dist. LEXIS 3498 March 2001 ,29, Filed available online in Nov. 2005 at http://cyber.law.harvard.edu/is02/readings/doubleclick.html

• OLIVER "BUCK" REVELL, v. HART G.W. LIDOV, App US District Court For the Northern District of Texas December 2002 ,31.

• Michaël MALKA - Les contrats de distribution et Internet- DEA de Droit des affaires Université des Sciences sociales – Toulouse I Mémoire réalisé sous la direction de Madame le professeur S. POILLOT-PERUZZETTO Septembre 2002 P. -11 Para15-.

(ورقة عمل)

عبدالباسط مصباح إنويقص
ماجستيرفي قانون الانترنت

مقدمة:

من الموضوعات التي يتعين علينا رصدها و الأهتمام بها، تلك التطورات التكنولوجيا وما أحدثته من تأثير في مناحي الحياة الاجتماعية، ولا شك في أن ما يمكن أن نطلق عليه « ثورة الانترنت « تتنامى في تأثيرها في مختلف جوانب الحياة المعاصرة بما يمكنها إحداثه من تحول في الانشطة البشرية والتفاعل بين البشر في حياتهم مما يسهم في زيادة الثقة في مستقبل الانسانية، وفي نفس الوقت فإن الانترنت طرحت تحديات حضارية وأقتصادية وثقافية وقانونية لم يتضح بعد مداها الكامل.

ولا شك أن الجانب القانوني من هذه التحديات يتمتع بأهمية خاصة، حيث يمثل تجاوب الفكر الانساني من هذه التحديات بما يحقق الجوانب الايجابية ويحمي معاملات المؤسسات والأفراد بما تتضمنه من خصوصية، ومن الطبيعي أن ينصرف الفكر الأنساني إلي تدارس التحديات في ضوء المعاملات الرقمية، وفي هذا المجال تظهر بوضوح أهمية إتاحة المعلومات التشريعية والقضائية والفقهية للباحثين عنها بما ييسر لهم الجهد المطلوب في محاكاة الظواهر الجديدة بالاشكال التقليدية وصولاً إلى تفهم أبعادها ومن ثم إلي أفضل صيغ التعامل معها.

والقانون بطبيعته كأحد العلوم الاجتماعية التي تتفاعل مع البيئة أصبح في حاجة إلي ملاحقة التطورات التقنية الحديثة حتى يتمكن من ضبط وتنظيم العلاقات الاجتماعية بشكلها الحديث.

ومن أبرز التحديات القانونية التي صاحبت تكنولوجيا المعلومات والأتصالات هو تنفيد فكرة تحميل « البرامج الحاسوبية « في الحاسوب ذاته الأمر الذي أحدث انعكاس وأضح عاى الحاسوب من جهة، وعلى أحدى نظريات القانون من جهة أخرى، فالأنعكاس الدى طراء على الحاسوب تمثل في إحداث تغاير في المهام الموكولة اليه وعدم قصرها على مهمة واحدة فقط، كما كان عليه الحال في الجيل الأول حيث أصبح في الأمكان تنويع هده المهام عن طريق إضافة برامج حاسوبية ذات وظائف محددة كلما احتاج الأمر.

وفيما تعلق بنظريات القانون، فقد حدث الأنعكاس على نظرية أشخاص القانون تحديداً بما تتضمنه من بناء وقواعد قانونية. كل ذلك أدى إلي حدوث جدلاً فقهياً واسع، لا سيما بعد الحكم الذي نطق به القضاء المقارن حيال مسألة غاية في الأهمية وهي مدى أمكانية إضافة شخصية قانونية جديدة غير متعارف عليها من قبل إلي أشخاص القانون، وهي الشخص الرقمي، المتجسدة في تطبيقات الحاسوب والانترنت المعتمد عليها أعتماد شبه كلي من قبل أفراد المجتمع المعلوماتي، وأصبحت العديد من الافعال والتصرفات التي يجريها الأفراد تتم بمساعدة برامج الحاسوب سواء كانت هذة المساعدة كلية او جزئية.

كل ذلك كان كافياً لدفع الفقه القانوني الي بحث مسألة مدى تمتع برنامج الحاسوب بالاستقلالية والذاتية في أتخاد القرار والتصرف، ومدى نسبة التصرف له من عدمه، وبالتالي مدى أمكانية أكتسابه للشخصية القانونية.

وبناء علي ما تقدم سأبحث فكرة الشخص الرقمي من خلال تقسيم هده الورقة الي:-

أولاً: مدلول الشخص الرقمي:

ثانياً: خصائص الشخص الرقمي:

ثالثاً: رؤية الفقه القانوني لفكرة الشخص الرقمي:

أولاً: مدلول الشخص الرقمي

الشخص الرقمي : هو مصطلح قانوني يطلق على البرامج الملحقة بالحاسوب لأداء مهام محددة.

فالأجيال الأولى من البرامج الحاسوبية كانت تقوم بمهام بسيطة كالبحث عن المعلومات للمستخدمين، ولكن نتيجة لحاجات التجارة الالكترونية ومتطلبات السرعة، ظهرت البرامج الحاسوبية التي تعمل باستقلال عن تدخل الأنسان، فقد أزداد تدخل هذه البرامج في أبرام المعاملات التجارية والمدنية، ولم تعد تستخدم في البحث عن المعلومات فقط، بل أصبحث هي التي تقوم بأغلب المعاملات الرقمية للانسان، حيث قيل في معرض الحديث عن هذه البرامج وتطورها أن الأنسان لم يعد يقوم باستخدام البرامج لإتمام معاملاته بل هي التي أصبحث تقوم بإتمامها دون تدخل منه، حيث يكتفي الشخص الطبيعي ببرمجة البرنامج الحاسوبي على نحو معين، بحيث يتصرف هذا البرنامج بعد ذلك دون حاجة إلي تدخل مباشر من جانب الشخص الطبيعي.

فقد بداء مالكي المواقع الالكترونية (الويب) بالأستعانة بالأنظمة الحاسوبية (البرامج) لتنفيذ وتنظيم عمليات الأشتراك والتسجيل بالمواقع، وكذلك لإتمام المعاملات الرقمية بما فيها التعاقد الرقمي، ويتم أستخدام البرامج الحاسوبية في المزاد الالكتروني، حيث يتولى البرنامج الخاص بالموقع بإدارة المزاد الالكتروني كتلقي عطاءات المزايدين، وإرساء المزاد على صاحب أكبر عطاء تم تقديمه. كذلك الأمر في الألعاب الالكترونية التي يتم ممارستها مع الحاسوب حيث يقوم الشخص الطبيعي بضبط مستوى اللعبة عند مستوى معين، تم يقوم هو باللعب مع برنامج الحاسوب الذي يتحكم في اللعبة،

نظراً لما تتمتع به هذه البرامج من سرعة ودقة وقدرة على إتمام وإبرام ما لا يحصى و لا يعد من المعاملات، يعجز الشخص الطبيعي عن القيام بها، بالرغم من أنه هو من قام بتصميم وبرمجة تلك البرامج.

ومن خلال البحث في أساليب التعاقد وكيفية أستخدام البرامج الحاسوبية بأختلاف أنواعها وجدنا أنها لا تخرج عن ثلاثة أشكال ، مع ملاحظة أن هذة الاشكال تختزل بداخلها كافة النمادج التطبيقية للأدوار التي يمكن أن تؤديها البرامج الحاسوبية، في التعامل والتصرف بأستقلال عن الشخص الطبيعي الذي يستخدمها.

الشكل الأول: التعاقد الالكتروني الشخصي:INTER PIERSONAL LECTRONIC CONTRACTING

وفيه يستخدم الافراد الطبيعيين البرامج الحاسوبية داخل الانترنت كوسيلة أو أداة للتفاعل بينهم كإرسال وإستقبال الرسائل الالكترونية، حيث تتيح هده البرامج أسلوبين للتعاقد.

أ-أسلوب التعاقد الحضوري الآني، كما هو الشأن في غرف الشات Chat ومؤتمرات الفيديو Video Conference.

ب-أسلوب التعاقد غير الآني، ومثال دلك التعاقد بنظام لبريد الالكتروني E-mail و الرسائل المكتوبة بالهاتف الذكي.

الشكل الثاني:التعاقد الالكتروني التفاعلي: INTERACTVE ELECTRONIC CONTRACTING.

في هذا الشكل يسمح للبرامج الحاسوبية بالتدخل في التفاعل مع الأنسان، بمعنى أن طرفي العقد (الأفراد) يتعاقدان بشكل مباشر غير متعاصر، حيث يتوسط العملية التعاقدية هنا طرف ثالث، وهو البرنامج، وبالتالي تكون أحتمالية عدم إدراك أحد الأطراف للزمن اليقيني الدي يتعاقد فيه البرنامج متوافرة، كما هو الحال عندما يتعاقد شخص مع أخر أو مع شركة عبر موقع الويب، لشراء منتج معين تم عرضه على موقع الشركة عبر الانترنت، فالموقع هنا ما هو إلا أحد البرامج الحاسوبية التي تقوم بالتعاقد مع الأفراد، وفي أغلب الأحوال لا يكون مالك الموقع مدركاً أن هناك عملية تعاقدية ما تتم في لحظة بعينها.

الشكل الثالث: التعاقد الالكتروني النظامي: INTER-SYSTEMIC ELECTRONIC CONTRACTING.

في هذا الأسلوب من التعاقد يختفي العنصر البشري ولا يكون له أي وجود في العملية التعاقدية، بحيث يكون أطراف التعاقد هنا الحواسيب وبرامجها، كما أن درجة تدخل الأنسان تختلف من وضع لآخر كما يلي:

أ-الوضع الأول: يقتصر تدخل الأنسان على عملية الأعداد والبرمجة المسبقة للبرنامج بوضع العمليات المراد تنفيذها، وبعدها تبدأ البرامج في التصرف آلياً من تلقاء نفسها.

ب-الوضع الثاني: وهو الوضع الذي تتفاعل فيه البرامج الحاسوبية مع بعضها البعض بعد عملية

البرمجة الأولى، بسبب ما تملكه هذه البرامج من قدرة وذكاء اصطناعي يمكنها من التصرف والتعلم وأكتساب الخبرات من البيئة الرقمية التي تبحر فيها، من خلال العمليات و المبادلات التي تدور حولها ومعها ومع غيرها من البرامج عبر الانترنت.

فوفقاً لأشكال التعاقد السابق عرضها نلاحظ أن معيار السيطرة يختلف بأختلاف درجة التطور التقني الذي يعتمد عليه البرنامج وبرمجته، فالبرامج المبرمجة تبعاً لتعليمات محددة للقيام بتصرف ما في ظروف معينة، يكون المستخدم هو المسئول لأنه يسيطر على البرنامج سيطرة كاملة، كما هو الحال عند أستخدام برنامج البريد الالكتروني للتعبير عن الأرادة في أبرام عقد من العقود.

أما في البرامج التي يزداد فيها تدخل الحواسيب وأنظمتها، ويتقلص فيها التدخل البشري، وهي البرامج التي تتمتع بالذكاء الاصطناعي الذي يمكنها من التفاعل مع بعضها دون أي تعليمات مباشرة من الفرد المستخدم لها، وهذا النوع من البرامج هو الذي يمثل إشكالية كبيرة لمسألة التعبير عن الأرادة.

ومن الاهمية بمكان التذكير بأن برمجيات الحاسوب نالت هذه المكانة المتميزة في مجال تقنية الحاسوب، بعد أن احتدم الصراع بين صانعي العتاد Hardware ومطوري البرمجيات Software. ومن أبرز شواهد ذلك الصراع ما حدث في مجال الحاسبات الشخصية بين شركة IBM الرائدة في مجال صناعة العتاد وشركة Microsoft رائده صناعة البرمجيات.

ومن هنا كان مطور البرمجيات، هو الذي يلهم صانع المكونات بالمواصفات ويحدد لمصّنع الحاسوب أسلوب عمله، وهو الوضع الذي يجوز معه القول أن تكنولوجيا المعلومات تعيش حاليا عصر ((ديكتاتورية البرمجيات)). فالبرمجيات التي تطورت من كونها عنصرا تابعا ومكملا للعتاد إلى العنصر الذى يدين له الجميع بالولاء والطاعة، ورمزا لسيطرة الفكر على المادة، واحدثت تحولا جذري في صلب علاقات الانتاج، الأمر الذي يؤكد تفوق رأس المال الذهني على رأس المال المادي.

ثانياً: خصائص الشخص الرقمي

لكي نتمكن من إبراز الخصائص التي يتمتع بها الشخص الرقمي يتعين علينا التطرق الي ما ورد من تعريفات لبرنامج الحاسوب في التشريعات المقارنة.

تعريف قانون): UETA)

عرف هذا القانون برنامج الحاسوب في المادة (6) من القسم (2) منه (تعريفات) بأنه « برنامج حاسوبي أو أي وسائل إلكترونية أو أدوات آلية اخرى تعمل بشكل مستقل للبدء في التصرف أو الاستجابة للسجلات الالكترونية أو الأداءات بشكل كلي أو جزئي، دون مراجعة أو آجراء من الفرد.

تعريف قانون UCITA:

عرف هذا القانون برنامج الحاسوب بأنه « برنامج حاسوبي أو أي وسائل إلكترونية أو آلية تستخدم مستقلة للبدء في التصرف أو للاستجابة لرسائل إلكترونية أو أي أداءات دون مراجعة أو عمل من قبل الفرد في وقت التصرف أو الاستجابة أو الاداء».

بالتدقيق في التعريفين السابقين نستطيع إستخلاص الخصائص التي يتمتع بها برنامج الحاسوب وهو (الشخص الرقمي) وهي :

1-الشخص الرقمي هو برنامج حاسوب.

2-الشخص الرقمي يبرمج بمعرفة الشخص الطبيعي.

3-الشخص الرقمي يعمل بشكل مستقل عن الشخص الطبيعي.

ثالثاً: رؤية الفقه القانوني لفكرة الشخص الرقمي

أنقسم الفقه القانوني حيال مسألة الاعتراف بالشخصية القانونية من عدمه الي ثلاثة أراء، ولكل راي من تلك الأراء حجج و أسانيد تدعم موقفه، وإنتقادات تقلل من حجية تلك الأسانيد، نتعرض لها بالتفصيل فيما يلي:

الرأي الأول:

ينادي أنصار هذا الأتجاه بوجوب منح برنامج الحاسوب الشخصية القانونية مثله في ذلك مثل الشخص الطبيعي والشخص الاعتباري. وأستند هولاء فيما ذهبوا اليه على الاسانيد التالية:-

1-لا يوجد في القانون أي عائق يحول بين برنامج الحاسوب وبين منحه الشخصية القانونية، لاسيما وأن هذا الكيان الجديد قادر على إتخاذ القرار والقيام بالتصرف بمفرده، علاوة على ان هناك تنوع في الكيانات المتمتعة بالشخصية القانونية إنطلاقاً من الشخص الطبيعي ممثلاً في الأنسان إلي الشخص الاعتباري كالشركة، الجمعية، الدولة، المنظمة الدولية.

2-قدرة برنامج الحاسوب على ان يصبح (حقيقة أجتماعية)، وهي المعول عليها من قبل القانون لكي يمنح أي شخص غير طبيعي الشخصية القانونية، ويتضح ذلك عندما نجد الاشخاص الطبيعيين يتعاملون معه على انه وحدة اجتماعية مستقلة، ومثال ذلك ما يقوم به الفرد عندما ينسب أي تصرف صادر من برنامج الحاسوب إلي البرنامج نفسه وليس إلي من قام ببرمجة البرنامج الحاسوبي، مثلما يحدث في الالعاب الالكترونية.

غير أن هذا الرأي لم يسلم من النقد، ووصفت الفكرة التي ينادي بها بأنها فكرة غير معقولة وذلك للأعتبارات الأتية :-

1-من الصعوبة بمكان تشبيه برنامج الحاسوب بالأشخاص التي منحها القانون الشخصية القانونية، الشخص الطبيعي و الشخص الأعتباري.

2-برنامج الحاسوب لا يمتلك ذمة مالية مستقلة، وبالتالي لا يمكن تصور تمتع هذا البرنامج بالحقوق، ولا بتحمله للألتزامات.

3-إذا منح برنامج الحاسوب الشخصية القانونية، سيؤدي ذلك إلي مسئوليته في حالة الأخلال بأي ألتزام عقدي، وبالتالي كيف يمكن إقامة مسئولية برنامج الحاسوب؟

.

الرأي الثاني:

يذهب أنصار هذا الرأي إلي أن برنامج الحاسوب ما هو إلا نائب يتصرف وفقاً لتعليمات محددة، فالشخص الطبيعي هو من يقوم ببرمجة برنامج الحاسوب ويحدد له المهام التي يقوم بها، بمعنى أنه يخول للبرنامج سلطة محددة في التصرف.

إلا أنه تم الاعتراض على ما ذهب اليه هذا الرأي للأسباب الاتية :-

1-لكي يمكن القول بأننا أمام عقد وكالة، يتعين أن يقبل الوكيل الوكالة، وحيث أن برنامج الحاسوب لا يتمتع بالشخصية القانونية، فهذا يعني بأنه ليس لديه الأهلية القانونية لقبول عقد الوكالة.

2-من شروط النيابة أن تحل إرادة النائب محل إرادة الأصيل، وبالتالي فان النائب يعبر عن إرادته هو لا عن إرادة الأصيل، لان العبرة بارادة النائب وليس بأرادة الأصيل، والمشكلة هنا هي عدم وجود إرادة أصلاً لبرنامج الحاسوب، وذلك لعدم وجود شخصية قانونية، الأمر الذي يحتم توافر الشخصية القانونية أولاً حتى يمكن الأعتراف بأمكانية أن يكون برنامج الحاسوب نائباً.

الرأي الثالث:

يقول أنصار هذا الرأي بأن برنامج الحاسوب ما هو إلا وسيلة أو أداة يستخدمها الشخص الطبيعي للقيام بمهام وتصرفات محددة، بمعنى أن الشخص الذي يقوم بإعداد وبرمجة برنامج الحاسوب ليعبر عن إرادته يعتبر هو مصدر كل التصرفات التي يقوم بها البرنامج، وهو ما يؤكد مسئوليته عن تنفيذ الالتزامات الناتجة عن هذة التصرفات.

وأستند أنصار هذا الرأي فيما ذهبوا اليه إلي ما جاء في قانون اليونسترال النموذجي الخاص بالتجارة الالكترونية، ويظهر ذلك في موضعين :-

1-جاء في المادة 12/ 2 / ب من القانون على إنه « في العلاقة بين المنشيء والمرسل إليه، تعتبر رسالة البيانات أنها صادرة عن المنشيء إذا أرسلت :

ب – من نظام معلومات مبرمج على يد المنشيء أو نيابة عنه للعمل تلقائياً « وهذا يعني أن الفقرة أسندت رسالة البيانات إلي الشخص الذي قام ببرمجة هذا البرنامج أو يتم برمجته لحسابه.

2-في تعليق دليل التشريع على المادة 2/ ج والخاصة بتعريف منشيء رسالة البيانات، حيث جاء في الفقرة ج « لا ينبغي إساءة تفسير القانون النموذجي على انه يتيح المجال لجعل الحاسوب صاحب حقوق والتزامات. وينبغي أعتبار رسائل البيانات التي تنشئها الحواسيب تلقائياً دون تدخل بشري مباشر ناشئة عن الكيان القانوني الذي شغل الحاسوب نيابة عنه « .

الا أن هذا الأتجاه لم يسلم من النقد هو الأخر وأخذ عليه ما يلي :-

1-لم يأخذ في الأعتبار الصفات و المميزات الخاصة ببرامج الحاسوب التي تقوم بأجراء التصرف أو الاداء، فهذه البرامج ليست تحت السيطرة الكاملة طيلة الوقت لمن قام ببرمجتها، فهي في بعض الأحيان تخرج عن نطاق سيطرة الأنسان.

2-بما أن برنامج الحاسوب هو مجرد أداة في يد الشخص الذي يبرمج البرنامج لحسابه، فهذا يعني ان ذلك الشخص مسئول عن أي تصرف يقوم به البرنامج حتى ولو كان هناك خلل فني في برنامج الحاسوب، مما يعني أن الشخص الذي برمج البرنامج الحاسوبي لحسابه يكون ملتزماً بأي إلتزام يتولد عن أي تصرف أو إجراء يقوم به البرنامج، ويجب عليه تنفيذه.

وتجذر الاشارة هنا إلي أن انصار هذا الاتجاه حاولوا الدفاع عن رأيهم بالقول، وإن كان الشخص الذي تم برمجة البرنامج الحاسوبي لحسابه ملتزماً بما يتولد عن التصرفات التي يجريها البرنامج الحاسوبي من التزامات ، إلا أن هناك أستثناءات على ذلك، تلك الاستثناءات تجعل الشخص الأخر المناظر لبرنامج الحاسوب مسئولاً مسئولية جزئية، وذلك إذا أستقبل ايجاب او قبول يعتبر غير مقبول وفقاً للظرف المحيطة.

الحماية الرقمية

من إعداد :
م. زكريا اسلام الدين الصيد الزويكي

عندما نسمع بمصطلح أمن المعلومات يتبادر للكثير من الناس أن الأمر متعلق بالمتخصصين بالتقنيات والحاسوب وتكنولوجيا المعلومات لكن الواقع أن أمن المعلومات أصبح ضرورة للجميع بسب انتشار الأجهزة الذكية وهذه المادة مخصصة لجميع الأفراد من كافة المستويات للوقوف على كيفية حماية معلوماتهم سواء كانت على الهواتف النقالة أو أجهزة العمل أو الأجهزة الخاصة.

مقدمة عن الأمن المعلوماتي

منذ فجر التاريخ وحتي اليوم، نشأت على الدوام علاقة وطيدة بين المعلومات والأمن كجبهتين لا غنى لإحداهما عن الأخرى، ففي عصور ما قبل التاريخ كانت صرخة الانسان البدائي في الغابة تحمل خطر يهدد أمن وسلامة الفرد أو الجماعة، ومع تتالي العصور تغيرت الأمور على الجبهتين، فالأمن لم يعد معادلاً للحماية من الهجمات المفاجئة من قبل الأعداء أو حتى وحوش الغابة، بل أصبح نظريات وقضايا معقدة، والمعلومات لم تعد مجرد دلالة على أشياء يجري التعبير عنها بصرخة من الفم، بل انطلقت من مكانها التقليدي داخل الأوراق والكتب والمخطوطات والأفلام والميكرو فيلم، بل والنقوش على الأحجار وجدران المعابد التقليدية واذهان الناس، واتخذت لنفسها شكلاً رقمياً نمطياً موحداً، وراحت تجري كالأنهار الهادرة التي تتدفق بلا انقطاع عبر غابة مترامية الأطراف من الاسلاك والموجات اللاسلكية التي تلف الكرة الأرضية برمتها، وهكذا، دفعت الثورة الرقمية والتطورات الجارية في الاتصالات والمعلومات إلى الساحة بالعديد من المتغيرات الجديدة فيما يتعلق بأمن المعلومات بعد تحولها إلى شكل رقمي، وجعلت منها قضية ضاغطة على صناعة القرار السياسي والجمهور المتخصص والعام معاً.

مفهوم امن المعلومات

تتعدد تعريفات أمن المعلومات وتتنوع حسب زاوية الرؤية، فنحن إذا نظرنا من زاوية علمية سنجد أنه العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها.

ولو نظرنا من زاوية تكنولوجية وفنية بحتة يمكننا تعريفه على أنه (الوسائل والأدوات والإجراءات المطلوب توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية)، ومن الزاوية القانونية نجد التعريف قد أخذ منحى أخر لكونه يركز علي التدابير والإجراءات التي من شأنها حماية سرية وسلامة وخصوصية محتوي، وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة المعلوماتية، وبشكل عام يمكن القول إن أمن المعلومات هو تلك الرؤى والسياسات والإجراءات التي تصمم وتنفذ على مستويات مختلفة التي تضمن أن تحقق للمعلومات السرية أو الموثوقية، أي التأكد من أن المعلومات لا تكشف ولا يُطلع عليها من قبل أشخاص غير مخولين بذلك.

وتكاملية وسمة المحتوى أي التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به، وبشكل خاص لن يتم تدمير المحتوى أو تغييره أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات، أو عن طريق تدخل غير المشروع.

واقع امن المعلومات

إن الفاتورة الاجمالية لجرائم أمن المعلومات عالمياً وعربياً في سنة 2011 وحدها تقدر 388 مليار دولار امريكي، أما التكلفة النقدية المباشرة لهذه الجرائم والمتمثلة في الأموال المسروقة ونفقات إزالة اثار الهجمات فتقدر بحوالي 114 مليار دولار ومعنى ذلك أن القيمة المالية لجرائم المعلومات أكبر من السوق السوداء لمخدرات الماريجوانا والكوكايين والهيروين مجتمعين، والتي تقدر بحوالي 288 مليار دولار، وتقترب من قيمة السوق العالمية للمخدرات عموماً والتي تصل إلى 411 مليار دولار، وأعلى من الانفاق السنوي لمنظمة الأمم المتحدة للأمومة والطفولة اليونيسيف بحوالي 100 ضعف، حيث تصل ميزانيتها إلى 3,65 مليار دولار، كما تعادل هذه الخسائر ما تم انفاقه خلال 90 عام على مكافحة الملاريا وضعف ما تم انفاقه على التعليم في 38 عاماً.

وقد بلغ المعدل الزمني لوقوع جرائم المعلومات حول العالم 50 ألف جريمة واعتداء في الساعة، تأثر بها 589 مليون شخص، وهو رقم أكبر من عدد سكان الولايات المتحدة وكندا وغرب أوروبا مجتمعين، ويعادل 9% من اجمالي سكان العالم.

وقد وزعت هذه الجرائم ما بين جرائم الفيروسات والبريد الالكتروني الملوث الضار، وجرائم الاحتيال والنصب والاصطياد (الحصول على معلومات بنكية سرية)، والجرائم المتعلقة باختراق الهواتف المحمولة.

الحوادث والمواجهات في عالم أمن المعلومات، حملت الكثير من الدلائل على أن الأمر تخطي كل الحدود المعتادة، وصار جولات صراع مكشوفة بين الدول وبعضها البعض، حتى أن جرائم المعلومات باتت أداة جديدة في الصراع السياسي والاقتصادي.

العلاقة بين الأمن المعلوماتي والأمن القومي

يمكننا القول إن اتساع قضية أمن المعلومات وتطورها على هذا النحو الخطير عالمياً وعربيا يعود إلى أمرين.

الأول : أن أغلب دول العالم بما فيها الدول العربية، رفعت شعار التحول إلى مجتمع المعلومات والمعرفة، ونفذت خطط واسعة النطاق لتحويل هذا الشعار إلى واقع، وفي خضم هذه الخطط يتم إنشاء سلاسل من قواعد البيانات القومية الكبرى، كما يجري تطوير شبكات الاتصالات ونشر الإنترنت عبر خطوط الاتصالات العادية والسريعة، وتنشط الدول في نشر مفاهيم وخدمات الحكومة الالكترونية، وتصدر القوانين و اللوائح التي تسهم في تفعيل أنشطة التجارة والأعمال الإلكترونية على نطاق واسع، وتتوسع في مبادرات توفير الخدمات الرقمية لفئات المجتمع المختلفة بالمنازل والمدارس وللمهنين كما تتبني عشرات من برامج التنمية المعلوماتية المتكاملة في مختلف الوزارات والهيئات والمؤسسات.

الثاني: أن تشييد بنية معلوماتية وطنية واسعة المجال وتبني التوجه نحو مجتمع المعلومات نقل المجتمع والدولة والمؤسسات إلى مرمي المخاطر، وحتم عليها مواجهة التحديات الشاملة والواسعة النطاق في أمن المعلومات، بمعنى أن تحديات أمن المعلومات في مجتمع يمتلك بنية معلوماتية واسعة يجعله يواجه تهديدات في أمن المعلومات تتسم بالشمول والاتساع وعمق التأثير وتنوع الأدوات وتعدد مصادر الهجوم وأدواته وغزارة الأهداف التي تشكل إغراء ومناطق جذب لمن يستهدفونه.

مخاطر أمن المعلومات في عصر (مجتمع المعلومات) تضم مستويين:

الأول : مستوي تعقب وجمع المعلومات : ويشمل الوسائل التقليدية لجمع المعلومات التي تعتمد بشكل كبير على العناصر البشرية من الجواسيس أو ما يعرف بالطابور الخامس ووسائل الاستطلاع الحديثة وفي مقدمتها الأقمار الصناعية التي تتطور بشكل كبير، حيث بلغت الصور والمعلومات الواردة منها حدا فائقاً من الجودة والدقة لم تبلغها من قبل: كما يشمل هذا المستوي العديد من أدوات تعقب وجمع من داخل البنية المعلوماتية الأساسية للجهة المستهدفة ومنها البوابات الخلفية، ويقصد بها الثغرات او نقاط الضعف الأمنية التي توجد بالشبكات وأنظمة التشغيل والبرامج المختلفة، و « الرقائق الالكترونية » التي تعتبر الجزء الحيوي بجميع أجهزة التعامل مع المعلومات من حاسبات ومعدات بناء شبكات ووسائط تخزين وغيرها والتي يمكن استخدامها في تعقب وجمع المعلومات، وأدوات التجسس علي شبكات المعلومات وعمليات الاعتراض.

الثاني: مستوي يستهدف افساد وتعطيل المعلومات، وتستخدم فيه العديد من الأدوات كفيروسات الحاسب والاختراق المباشر لشبكات المعلومات والهجوم بفيض الرسائل وطلبات وهجمات اغراق الخوادم على نطاق واسع وغيرها.

وكما هو واضح فإن هذه الاخطار لا تتوقف عند كونها تهديداً لأمن المعلومات داخل شركة أو مؤسسة منشأة، بل تعد تهديدات جدية للأمن القومي للدول والمجتمعات ككل.

الهندسة الاجتماعية Social engineering

في سياق أمن المعلومات والأمن الرقمي، الهندسة الاجتماعية هي فن استخدام الحنكة والحذاقة لخداع الشخص بحيث يقوم بشكل إرادي بكشف معلومات سرية أو بإعطاء المهاجم الفرصة للوصول للمعلومات السرية، بحيث لا تعتمد أساليب الهندسة الاجتماعية على معرفة تقنية عميقة بالتالي يستطيع أي شخص يتوافر لديه قدر معين من الحنكة والدهاء القيام بهجمات الهندسة الاجتماعية.

التعريف:

هناك عدة تعريفات للهندسة الاجتماعية ومن أشهرها: إن الهندسة الاجتماعية هي طريقة الهجوم المستخدمة من قبل العديد من المهاجمين، والتي تستفيد من طبيعة البشر ونقاط الضعف فيها، للتلاعب عليهم وخداعهم بكسب ثقتهم وذلك من أجل الحصول على معلومات سرية سواء كانت كلمات المرور الخاصة بالأشخاص أو أي معلومة حساسة مالية أو غيرها من المعلومات الشخصية الحساسة، وقد يكون الغرض منها هو تثبيت برامج تجسس بشكل سري أو أي برامج أخرى خبيثة، أو دخول الأشخاص الغير مخول لهم إلى نظام الكمبيوتر.

وفي الغالب نجد إن المهندسين الاجتماعيين (المهاجمين) لا يملكون أية مهارات تقنية وإنما يستغلون الجانب البشري أضعف جزء في أمن الشركة أو المنظمة حيث يستخدمون مهارات التعامل مع البشر لاستدراجهم وسؤالهم ويعتمدون على خداعهم.

الهدف من الهندسة الاجتماعية:

نستنتج من التعريف السابق، إن هدف المهندسين الاجتماعيين (المهاجمين) هو خداع الأشخاص للحصول على المعلومات السرية كما سبق ذكره، أو للدخول الغير الشرعي للأنظمة واختراقها أو تدميرها.

أنواع الهندسة الاجتماعية:

يمكن أن تصنف الهندسة الاجتماعية إلى نوعين:

النوع الأول: يعتمد على الجانب البشري، وهو الغالب والأكثر شيوعاً، حيث يتفاعل المهاجم مع الأشخاص للحصول على المعلومات المطلوبة.

النوع الثاني: يعتمد على تقنية الكمبيوتر، حيث يستخدم برامج يمكن من خلالها التخمين عن المعلومات المطلوبة مثل عمليات التخمين على كلمات المرور وغيرها.

أساليب الهندسة الاجتماعية:

نحاول فيما يلي سرد لأهم الأساليب الهندسة الاجتماعية التي يعتمد عليها المهاجمون لإيقاع ضحاياهم، ونتمنى من القراء بعد معاينة هذه اللائحة محاولة التفكير بأساليب أخرى قد يعتمدها المهاجمون، فالمهاجمون يفكرون ايضاً بشكل مستمر بأساليب جديدة لخداع الضحايا.

استغلال الشائعات:

تعتمد أغلب عمليات الاحتيال للحصول على كلمات السر أو للسيطرة على الحواسيب على تغليف برنامج خبيث أو رابط خبيث في غلاف جذاب يغوي الضحية إلى تشغيله أو فتحه.

يكون الغلاف الجذاب عادة مصمما للضحية أو مجموعة الضحايا. في كثير من الأحيان يستغل المهاجمون الشائعات بغض النظر عمن وراء الشائعات، كغلاف جذاب لتمرير المحتوي الخبيث.

تنتشر الشائعات بشكل سريع جداً ضمن شبكات التواصل الاجتماعي ومنها فيسبوك، وبالتالي تكون مساهمة في نشر الشائعات بشكل أو بأخر مساهمة في تسهيل عمل ينوي استغلال الشائعات لتغليف روابطهم الخبيثة.

تؤثر أيضاً الشائعات على العالم الحقيقي، فقد تؤدي بأصحاب القرار لاتخاذ قرارات مبنية على معلومات خاطئة ما يؤدي إلى انكشاف مزيد من المعلومات التي يمكن استغلالها لمزيد من هجمات الهندسة الاجتماعية أو غيرها من الهجمات الخبيثة.

استغلال عواطف الضحية وطِباعه الشخصية:

يقصد باستغلال العواطف استخدام نصوص أو صور تخاطب عاطفة الضحية تؤدي إلى سقوطه في فخ فتح وتشغيل الملف الخبيث أو فتح رابط خبيث.

من العواطف التي قد يستغلها المهاجم، على سبيل المثال - وليس الحصر عواطف: الحقد، الانتقام، الحزن، الكره والنقمة، الحب، والشوق، الحنين، الاعجاب، يضاف إلى ذلك المشاعر الدينية او الطائفية او الاثنية والعشائرية والقومية وغيرها...

يمكن أيضاً للمهاجم استغلال فضول المستهدف أو غروره أو بحثه الذي لم ينته عن الحبيب أو عن علاقة عاطفية مشروعة أو غير مشروعه.

استغلال المواضيع الساخنة:

بشكل مشابه لاستغلال الشائعات، يستغل المهاجمون المواضيع الساخنة لتمرير عمليات احتيالهم بعكس الشائعات، فالمواضيع الساخنة أخبار حقيقية ولا تحتوي على تضخيم أو افتراء، تنتشر عادة بسرعة على وسائل الإعلام ذات المصداقية العالية بشكل أخبار عاجلة.

كل هذا يجعلها طعماً مناسباً لإيهام الضحية بأن الرابط المرفق مع الرسالة مثلاً هو أيضاً «وديع» وإن صاحب الرابط المرفق «صادق» في ادعائه حول محتوى الرابط كما أن الرسالة صادقة في نقل الاخبار الساخنة.

استغلال موضوع الأمن الرقمي وضعف الخبرة التقنية للضحية:

في هذا النوع من الهندسة الاجتماعية يدعي المهاجم أن رابطا ما أو ملفا ما سيسهم بحماية جهاز الضحية، في حين إنه في الحقيقة الملف يكون ملف خبيث أو رابط خبيث.

انتحال الشخصية Identity theft

يمكن للمهاجم أن ينشي مثلاً حساب على فيسبوك، أو حساب ايميل، أو حساب سكايبي، باسم مستعار أو باسم مطابق لاسم صديق لك او لاسم شخص تعرفه بنية انتحال الشخصية.

يمكن لمنتحل الشخصية استغلال الثقة للحصول على معلومات ما أو لاستدراجك لإضافته إلى مجموعة سرية معينة وما إلى ذلك.

في كثير من الأحيان يستطيع منتحلو الشخصية خداع ضحاياهم باستخدام مهارات تحايل دون الحاجة لمقدرات تقنية لذلك يعتبر انتحال الشخصية من أساليب الهندسة الاجتماعية Social Engineering.

بالطبع الحصول على كلمة سر لحساب شخص ما في فيسبوك واستغلال حسابه لانتحال شخصيته يسهل مهمة الحصول على معلومات بشكل كبير جدا، كما يسهل ايضاً استغلال الحساب المخترق لاختراق حسابات جديدة عبر استخدام الحساب المخترق لسرقة كلمات السر بالاحتيال مثلاً.

استغلال السمعة الجيدة لتطبيقات معينة

هنا يدعي المهاجم إن رابطاً أو ملفاً هو نفسه النسخة المحدثة مثلاً من تطبيق معين، ولكنه في الحقيقة يتضمن ملفاً خبيثاً وهناك أيضاً حالات أخرى يقوم فيها الرابط بتحميل الملف الخبيث وتنصيبه ثم تحميل التطبيق الحميد الحقيقي وتنصيبه بحيث يعتقد الضحية أنه قام بتنصيب التطبيق الحميد ولا يعلم أنه قام بتنصيب ملف خبيث، اما الحالات الأكثر دهاء نسخة معدلة عن التطبيق ذو السمعة الجيدة يبدو يعمل كالتطبيق الحقيقي لكنه يتضمن في الوقت نفسه جانب خبيث.

عوامل نجاح الهندسة الاجتماعية علي الافراد والشركات والمؤسسات الحكومية ؟

- عدم وجود تدريب أمني للموظفين
- ضعف في سياسة الخصوصية والامان
- عدم مواكبة التطورات

ما مدي تأثير الهندسة الاجتماعية ؟

- صعوبة التعرف عليها
- لاتوجد طريقة للحماية منها الا عن طريق التوعية الامنية والتقنية.
- لاتوجد اي برامج او اجهزة للحماية منها والدفاع ضد الهندسة الاجتماعية

طرق وأساليب الهندسة الاجتماعية

للهندسة الاجتماعية طرق وأساليب مختلفة ومنها اصطياد كلمات السر Password Phishing

هي طريقة للحصول علي كلمة السر مستخدم لخدمة ما أو موقع ما علي الانترنت، تعتمد الطريقة علي إيهام الشخص المستهدف بأنه علي الموقع الصحيح المعتاد حيث يدخل كلمة السر عادة للدخول الى حسابه علي الموقع (كموقع البريد الالكتروني) لكن في الحقيقة يكون الموقع موقعاً مزيفاً يديره احد لصوص كلمات السر، بالتالي إذا خدع المستخدم ودخل كلمة سر في ذلك الموقع تصل كلمة السر بكل بساطه الي اللص، للمزيد تظهر الصورة التالية من الصفحات اصطياد كلمة السر أعدها احدهم بهدف اصطياد كلمات سر مستخدمي Facebook لاحظ العنوان هذه الصفحة مختلف عن عنوان موقع Facebook الرسمي.

استغلال التواجد الفيزيائي للمهاجم قريباً من الضحية

نقصد بذلك أن يكون المهاجم والضحية مثلاً في نفس القاعة أو نفس الفندق. في هذه الحالة قد يستخدم المهاجم حنكة للوصول إلى حاسب المحمول للضحية مثلا أو لهاتفه.

خيانة الثقة

في كثير من الاحيان يكون المهاجم صديقاً او زميلاً للضحية، يستغل المهاجم ثقة الضحية به بسبب طبيعة علاقة الصداقة بينهما او بسبب الزمالة في المهنة او المؤسسة حيث يعملا، فقد يطلب المهاجم من الضحية ببساطة كلمة سر حسابه، أو يطلب منه فتح رابط معين يرسله عبر البريد الالكتروني او يطلب منه فتح رابط او ملف معين يمرره له علي فلاش ميموري USB، قد يقوم المهاجم بالتلصص علي زميله من خلال ادخاله كلمة سر حسابه، استغلال الثقة أحد أكثر الأساليب الهندسة الاجتماعية شيوعاً كما ينصح خبراء بعدم الثقة بأحد. لكن هناك ايضاً مساوي كثيرة لعدم الثقة بأحد، لذلك ننصح بتوخي الحذر دائماً من الجميع مع التغيرات الكبيرة في طبيعة العلاقات الاجتماعية التي اتت بها ثورة تقنية المعلومات الي عالمنا المعاصر.

أمثلة على هجمات الهندسة الاجتماعية ونصائح تفاديها

مثال 1 : انتحال شخصية صديق لإرسال رسالة لإصابة جهاز الضحية ببرنامج خبيث يريد المهاجم الحصول على معلومة معينة من السيد م س.

يقوم المهاجم بجمع بعض المعلومات عن السيد م س مثل من هم اصدقاؤه المقربين، وماهي اهتماماته، ويجمع المعلومات كافية عن أحد الاصدقاء م س وليكن السيد ط ع الذي لا ينشر كل شيء عن نفسه ببساطة على الانترنت على حسابه علي فيسبوك بدون اي اهتمام بخصوصية المعلومات.

يقوم المهاجم بنشاء حساب بريد الإلكتروني مزيف ينتحل شخصية ط ع صديق من اصدقاء م س.

(يستخدم المهاجم لإنشاء الحساب المزور معلومات حقيقة عن ط ع تشبه معلومات حساب بريده الالكتروني)

يستخدم المهاجم لإنشاء حساب البريد الالكتروني الذي ينتحل شخصية م ط لإرسال رسالة بريد الالكتروني تحتوي على ملف خبيث.

م س بما انه يثق في صديقه ع. ط وبما أنه لم يلاحظ أن الحساب هو ليس حساب صديقه الحقيقي، يقوم بفتح الملف الخبيث مصيبا جهازه.

لتجنب الوقوع ضحية هذا النوع من الهجمات

احرص على خصوصيتك وعدم نشر معلومات شخصية عن نفسك لان المهاجم قد يستخدمها لانتحال شخصيتك.

لا تثق بأحد.

-انظر بعين الحذر الي كل بريد الكتروني أو رسالة ما تصلك تحتوي علي ملفات وروابط مرفقة في حال رغبتك بفتح اي ملف او رابط يصلك قم قبل ذلك بالتأكد من انه ليس خبيث عبر استخدام موقع فايروس توتالvirus total https://www.virustotal.com/ar/.

- عند شعورك أنك اصبت بفيروسات أو مخترق قم بإعلام شخص مختص لفحص جهازك ونصحك فيما يتعلق بمعالجة هذه الازمة.

- أبلغ اصدقائك بكل صراحة أنك وقعت ضحية لاختراق حسابك كي يكونوا حذرين بدورهم في حال حاول المهاجم انتحال شخصية السيد م س لخداع المزيد من الاشخاص.

- قم بتنصيب برامج حماية من الفيروسات سواء في أجهزة الحواسيب أو الهواتف.

- مثال 2 : انتحال شخصية موظف في قسم أخر في مؤسسة أو في شركة

- يريد المهاجم الحصول على كلمة سر السيد ر ح على حسابها في مكان عملها في المؤسسة

- لدي المهاجم رقم هاتف عمل ر ح

- يتصل المهاجم بالسيدة ر ح قائلاً إنه مختص IT وان مديرها في المؤسسة طلب منه التحقق من وجود اختراق في حساب ر ح ويطلب منها ذكر اسم حسابها وكلمة سرها على الهاتف.

- السيدة ر ح تصدق القصة وببساطة تعطي المعلومات إلي المهاجم معتقدة ان كل شيء بخير.

- يقوم المهاجم باستخدام اسم الحساب وكلمة السر لوضع باب خلفي إلى حساب السيدة ر ح يستخدمه

حتى لو غيرت السيدة ر.ح كلمة السر.

- يتصل المهاجم مجدداً بالسيدة ر.ح (وهنا العبقرية) قائلاً لها إنه تحقق من الحساب وأن كل شيء على ما يرام وأنه سيعلم المدير بذلك ويشكرها ويتمني لها يوماً طيباً.

لتجنب الوقوع ضحية هذا النوع من الهجمات

- تحقق من شخصية كل شخص يدعي أنه يعمل في المؤسسة في قسم أخر.
- لا تعطي كلمة السر خاصتك ولا أسم حسابك لأي شخص.
- أستفسر من مديرك عن الموضوع.
- قم أنت بالاتصال بالقسم الذي يدعي الشخص تمثليه وأسأل مدير القسم عن الموضوع.
- قم بإعلام مديرك بأي شي من هذا النوع حتى لو لم يكن عندك إي شك بموضوع الاختراق.
- إذا شعرت أن حسابك قد تم اختراقه على اعلام مديرك والتأكد من الوصول الموضوع لمدير قسم ال IT بأسرع وقت ممكن لتفادي المزيد من المشاكل.

الوقاية من الوقوع ضحية للهندسة الاجتماعية:

- بناء على أساليب الاحتيال المفصلة أعلاه وبناء على الأمثلة المذكورة في الفقرة السابقة يمكن إدراج النقاط التالية كأسلوب للوقاية من الوقوع ضحية لهجوم باستخدام الهندسة الاجتماعية.

- كي لا تكون ضحية سهلة راعي النقاط التالية:

- أحرص على خصوصيتك وعدم نشر معلومات شخصية عن نفسك لان المهاجم قد يستخدمها لانتحال شخصيتك ومهاجمة صديق لك أو قد يستخدم المعلومات ليصيغ الهجوم عليك بشكل مقنع أكثر.
- لا تشارك كلمة السر الخاصة بك واستخدم كلمة مرور طويلة ومعقدة وتحتوي على رموز وأرقام مختلفة.
- لا تشارك أسماء أو عناوين حساباتك مع غير المعنيين.

كي لا تقع ضحية للخدع أو الاحتيال

- لا تثق بأحد
- ابق حذر دائماً
- تحقق من شخصية من يراسلك سواء عبر البريد الالكتروني Email أو برامج المراسلة مثل Skype أو عبر وسائل التواصل الاجتماعي فيسبوك Facebook او توتير Twitter
- قم بتفعيل المصادقة الثنائية لحساباتك
- أنظر بعين الشك الي كل بريد الكتروني أو رسالة أو تعليق يصلك يحتوي على ملفات او روابط مرفقة.
-عند الشك برسالة ما أو بجهة اتصال مشبوهة، لا تقم بفتح الملفات أو الروابط المرفقة في الرسالة. ثم قم بالاتصال بالقسم المسؤول في المؤسسة او بخبير في أمن المعلومات.
- في حالة رغبتك بفتح إي ملف أو رابط يصلك قم قبل ذلك بالتأكد من أنه ليس خبيث عبر استخدام مواقع لفحص الفيروسات أو المواقع المزيفة مثل virus total https://virustotal.com
- عند شعورك أن جهازك أصيب او أن حسابك تم اختراقه قم بإعلام الشخص المسؤول في المؤسسة، أو قم

بإعلام أحد معارفك المختصين في أمن المعلومات.

- إذا شعرت إن حسابك قد تم اختراقه عليك إعلام مديرك والتأكد من أنه تم التواصل مع مسئول تقنية المعلومات في المؤسسة بأسرع وقت ممكن لتفادي المزيد من المشاكل.

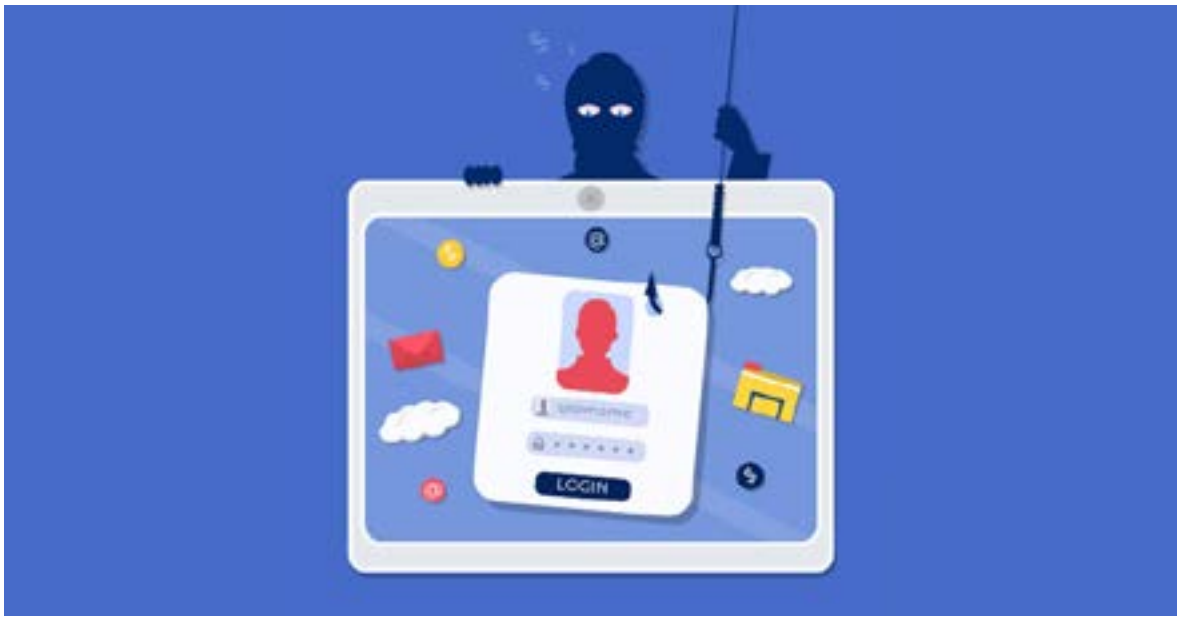
ماذا افعل عند الوقوع ضحية الهندسة الاجتماعية

عادة يترافق الهجوم بأساليب الهندسة الاجتماعية بهجوم اخر ببرمجيات خبيثة مثلاً، لذلك عندما يقع المستخدم ضحية للهندسة الاجتماعية عليه أن يقوم بخطوات تختلف تبعا لنوع الهجوم.

لكن بشكل عام يمكن القيام بالخطوات التالية:

- إعلام الشخص المسؤول عن الامن الرقمي في المؤسسة أو الزميل المختص بموضوع الأمن الرقمي.
- تقييم الضرر والأشخاص المتأثرين
- إزالة أثار الهجوم
- إعلام الجهات (مؤسسات، زملاء، اصدقاء، معارف، افراد عائلة) والتي من الممكن أن تكون قد تضررت او تأثرت بسبب وقوع المستخدم ضحية للهجوم.

يترافق الهجوم بالأساليب الهندسة الاجتماعية بهجوم حصان طروادة للتحكم عن بعد remote administration Trojan



التصيد الإلكتروني Phishing

التصيد الإلكتروني هو شكل من أشكال الاحتيال على الأخرين للحصول علي بعض المعلومات السرية الخاصة بالضحايا، كاسم المستخدم، أو كلمة السر، أو البيانات الخاصة ببطاقة الائتمان المالية، أو الحصول على المال بطريقة غير مباشرة.

تمت تسميته بالتصيد الإلكتروني لاستعانة المخترق بطعم للإيقاع بضحيته، ناهيك على أن التصيد الاحتيالي بمفهومه العام لا يوجه لفئة معينة إنما لكافة الناس فيكون بذلك شبيهاً لتصرف الصياد الذي يلقي طعمه وليس لديه علم مسبق بما هي السمكة التي سيلتقطها طعمه.

وفقاً لتقرير MCSI (Microsoft computing safer index) الصادر في فبراير من عام 2014، فإن التأثير العالمي السنوي للتصيد الإلكتروني قد يصل إلى 5 مليارات دولار!

ووفقاً لدراسة عالمية صادرة عن مجموعة عمل التصيد الالكتروني "APWG:Aniti phishing working Group لنفس العام، فإن 54% من رسائل التصيد تستهدف زبائن وعملاء كل من الشركات التالية : , Apple paypal, Chinese taobao وغيرها من المواقع والشركات.

تتم عملية التصيد بإرسال رسالة الكترونية للضحية إما عن طريق البريد الإلكتروني، أو باستخدام تقنية الرسائل الفورية الالكترونية سواء أكانت تطبق برتوكول « نظير – نظير. peer – peer: أو بروتكول الخادم – المستخدم. "client – server" بحيث يقوم المخترق بالتنكر في هذه الرسالة لتبدو رسالته مرسلة من قبل منظمة موثوقة أو بانتحاله لشخصية أحد أصدقاء الضحية، ولوثوق الضحية بهذه المنظمة أو هذا الصديق فإنه يستجيب لمحتوى الرسالة!

إما أن تحتوي الرسالة على مرفق أو رابط خبيث يقوم بتحميل برامج (Malwares) على جهاز الضحية، أو أن يقود الضحية لموقع الإلكتروني خبيث يتم عبره الاحتيال على الضحية بأن يطلب منه إدخال بعض البيانات

فيقوم الموقع بدوره بتجميعها وتحليلها كي يستخرج منها المعلومات السرية ككلمات المرور الخاصة بمواقع معينة، أو معلومات البطاقة الائتمانية..الخ.

يصنف التصيد على أنه شكل من أشكال الهندسة الاجتماعية، إّن الخطوة الأساسية لنجاح العملية هي إقناع الضحية بالنقر على الرابط المضمن في نص الرسالة، أو فتح المرفق وذلك كله يتم بأسلوب يشعر الضحية بالأمان.

كذلك فإن المخترق ليس في صدد دراسة عميقة لعملية اختراق أنظمة حماية جهاز الضحية والبحث في ثغراته، فهو لا يحتاج سوى إقناع الضحية بالنقر على الرابط فيتم تحميل البرامج الخبيثة التي ستقوم بعملية الاختراق بسهولة لأنه بعملية النقر والذي يعتبر المسؤول عن الجهاز أي انه ال admin على الرابط وسيعطي بذلك صلاحيته للبرنامج ويعطيه كافة المعلومات التي يحتاجها مثل عنوان IP.

ينتشر هذا النوع من الاختراقات أثناء المناسبات، ذلك أن الجميع يحتفلون بإرسال بطاقات التهنئة عبر البريد الإلكتروني والرسائل الفورية أو الرسائل حتى عبر الهاتف SMS فيشكلون بذلك الظروف المثالية للمخترقين بنشر رسائلهم للعامة بأغراض التهنئة والقرصنة «الاختراق» أيضاً بعد صدور أخبار عاجلة لإحداث هامة أو ربما استخدام وسائل الإعلام الاجتماعية كفيسبوك، بتضمين الروابط الخبيثة على منشورات ذات إقبال جيد من المستخدمين.

تتم عملية إقناع الضحية بعدة أساليب، فيجب على المخترق أن يتمتع بذكاء اجتماعي ليقوم بتزوير المظهر العام للرسالة الإلكترونية لتبدو وكأنها مرسلة من جهة موثوقة كشركة مشهورة، وذلك بإدراج شعار الشركة وبعض البيانات الخاصة بالتواصل معها ضمن الرسالة الالكترونية، حيث بإمكان المخترقين الحصول على هذه البيانات من موقع الشركة الرسمي، إما عن الروابط الالكترونية فإن المخترق يقوم بتزوير الرابط بطريقة غير ملحوظة او تزوير المظهر الخارجي له كما سيوضح لاحقاً

تصنف هجمات التصيد الالكتروني بناء على الفئة المستهدفة والتقنية المستخدمة بالتالي:

1 – **التصيد بالرمح** (spear Phishing)

عوضاً عن إرسال رسالة الإلكترونية خبيثة لآلاف الضحايا، يقوم المخترق هنا باستهداف أفراد أو شركات معينة ومن هنا جاءت تسميتة بالتصيد بالرمح. إذ أن الهدف هو شخص أو جهة محددة، وهذا الأمر يتطلب من المخترقين بذل جهد إضافي في عملية جمع المعلومات عن الشخص أو الجهة المستهدفة ليثري ذلك محتوي رسالتهم فتزداد نسبة نجاحهم، وهذه التقنية أثبتت نجاحاً واسعاً على شبكة الإنترنت بما يمثل 91% من الهجمات.

2- **تصيد بالاستنساخ** (Clone Phishing)

عند حصول المخترق على نسخة أصلية لرسالة الإلكترونية ولديه علم بأنها مرسلة أيضاً لمستخدم أخر. عندها سيقوم بانتحال شخصية المرسل الأصلي وإرسال الرسالة عينها للمستخدمين بعد إرسالها لهم من قبل المرسل الاصلي بادعاء ان هناك تعديلات قد طرأت على محتوي الرسالة أو أن هناك إجراء يجب استكماله بالنقر على رابط أو بتحميل ملف مرفق (حيث أن المخترق قام بالتعديل على الرابط أو المرفق ليتناسب مع أهداف اختراقه)

3- تصيد الحيتان: (Whaling)

هنا يتم استهداف كبار المسؤولين، أو المدراء التنفيذيين، أو الشخصيات التي تلعب دوراً هاماً في كيان الشركات أو الجهات السيادية في الدول، حيث يتم استدراجهم نحو موقع خبيث بواجهة رسومية ذات طابع تنفيذي بمستوى متقدم.

أما عن محتوى الرسالة الذي قادهم للموقع، فإما أن يكون استدعاء قانوني، أو قضية تنفيذية.... إلخ.

مثال: تقوم مجموعة صائدو الحيتان (Whaling phisher men) بتزوير رسالة استدعاء قضائي لمكتب التحقيقات الفيدرالي FBI وتتضمن الرسالة رابط الإلكتروني خبيث والذي يتطلب من المسؤول النقر عليه لتحميل برامج خاصة لعرض أمر الاستدعاء كما يدعون.

4- التصيد بتعديل الرابط الإلكتروني (URL manipulation phishing)

يجب على المخترق استخدام أساليب الخداع الفني في تصميم، فيقوم بالتعديل على الرابط الإلكتروني الخبيث ليبدو كالرابط الأصلي لموقع موثوق، وأدناه مثال على عملية تعديل الرابط:

بإمكان المخترق إستبدال الحرف O بالرقم 0 بالرابط www.google.com لتبدو www.g0ogle.com فيصعب على المستخدم ملاحظة الفرق، هنا يقوم الرابط الخبيث بإرسال رسالة الضحية لموقع خبيث ذو واجهة رسومية مطابقة لموقع Google الرسمي.

تكمن شدة خطورة هذه الطريقة بتزوير الرابط الخاص بالبنك وإرسالك لموقع خبيث بواجهة رسومية مطابقة وبعد ذلك يقوم الضحية بإدخال بياناته الخاصة من كلمة المرور واسم المستخدم! كما في المثال أدناه.

في هذا الرابط www.ba nk o far ne r ic a.com تم استبدال حرف M بكل من ال r,n وبذلك يتم خداع المستخدم بصرياً ظانا ان الحرف هو M أو أن يقوم المخترق بإدراج رابطاً خفي خبيث وراء رابط اخر موثوق، باستخدام خيار إدراج رابط -https://www.google.com هنا نلاحظ بوضوح موثوقية الموقع الذي سيقودنا إليه الرابط ولكن بمجرد إسقاط الفأرة عليه نري اسم النطاق الفعلي الذي سيرسلنا إليه يختلف عن الموضح في الرابط

5- التصيد بتزوير الموقع الإلكتروني (web site spoofing phishing)

بعد زيارة الضحية للموقع الخبيث فإن عملية الخداع والتزوير لم تنته بعد، بعض عمليات التزوير تتم باستخدام أوامر java script لتغير شريط العناوين، ويتم ذلك بوضع صورة للعنوان الأصلي على عنوان الموقع الخبيث فيظن الضحية بذلك أنه في الموقع السليم، أو بإغلاق الشريط الأصلي وفتح الشريط جديد بالعنوان الموثوق ويمكن للمخترق الاستعانة بثغرات المواقع واستخدام cross site scripting " xss " للإيقاع بالضحية، إذ أن الرابط الخبيث سيقوم فعلياً بأرسال المستخدم للموقع الموثوق فيظن أن الأمور الأمنية متحققة والعنوان الظاهر في شريط العناوين هو عينه العنوان للموقع الأصلي، إلا أن المخترق قد يلجأ لاستخدام ثغرة في الموقع من نوع XSS و بذلك يستطيع الحصول على البيانات التي سيدخلها الضحية للموقع، وتم استغلال هذه الثغرة مع موقع PayPal الشهير سنة 2006.

6- التصيد بالمكالمات والرسائل عبر الهاتف (Phone Phishing)

التصيد الاحتيالي لا يقتصر على استخدام المواقع الخبيثة، إذ أن المخترقين يقومون بإرسال الرسائل عبر شبكات الاتصال لهواتف المستخدمين بداعي إرسال بياناتهم لاستكمال إجراءات معينة أو لحاجة البنك لتثبيت بعض البيانات، ويلجئون في بعض الأحيان لمكالمتهم هاتفياً لاستدراجهم بالهندسة الاجتماعية لإرسال بياناتهم الخاصة بحساباتهم البنكية، أو من خلال إرسال رسالة نصية تحتوي على رابط معين أو رسالة تأكيد لضغط عليها فيتم الإيقاع بك.

تقنيات أخري:

- يستخدم المخترقون طريقة فعالة لتصيد وهي إرسال رسالة لضحية لموقع البنك الأصلي وظهور رسالة نصية تطلب من المستخدم إدخال بيانات الحساب البنكي، وبهذا يظن المستخدم أن الطلب هو من موقع البنك الرسمي.

تقنية التوأم الشرير: تقنية تصيد احتيالي يصعب اكتشافها. إذ يقوم المخترق بصنع شبكة لاسلكية مزيفة والتي تبدو كشبكة طبيعية موجودة في مكان عام كالمطارات أو المقاهي، أو الفنادق...إلخ. فور استخدام الضحية لهذه الشبكة فإنه باستطاعته المخترق التقاط البيانات بأشكالها (سرية أم عامة) التي يتناقلها المستخدم مع أي موقع أخر من خلال هذه الشبكة.

وللتصدي لهذه الاختراقات فهناك العديد من التقنيات التي تقوم بعملية ترشيح (filtering) الرسائل الإلكترونية أو المواقع الخبيثة، وعليه يلجأ المخترقون لتضمين محتوى الرسالة في الصورة وإرسالها لضحية كي لا يتم اكتشافها من قبل البرامج التي تتصدي لها عن طريق قراءة محتوي الرسالة النصية والحكم عليها إن كانت رسالة تصيدية أم لا، وذلك قاد إلى عملية تطوير على تقنيات وبرامج ترشيح البريد التصيدي ليقوم بعملية استعادة النص من الصورة أو التشريح بناء عليه.

أما عن الية عمل المرشحات فهي إما أن تستخدم ال optical character recognition والذي يقوم بعملية شاملة للصورة (Scan) وبعد ذلك استعادة النص منها ثم تحليل المحتوي.

ونذكر أيضا "IWR: intelligent word recognition" إذ لا يتم استبدال الطريقة السابقة بهذا النوع ولكنه فعال في التعامل مع الصور التي تحتوي نصوص بخط اليد، أو النص مع الخلفية ملونة. أو النصوص المستديرة، (rotated) وكذلك المشوهة كأن تكون مموجه.

ولإخفاء المواقع الخبيثة عن البرامج الترشيح، فقد قام المخترقون باستخدام مواقع إلكترونية تعتمد في عملها على تنقية flash فتبدو المواقع أقرب ما يكون من الموقع الموثوق وقدرة اكتشاف هذه المواقع الخبيثة ضئيلة لإخفائها نصوص التصيد (والتي يتم الترشيح بناء عليها) ضمن كائنات الوسائط المتعددة.

- كيفية التعرف على رسائل البريد الإلكتروني الخاصة بالتصيد أو الروابط الخبيثة أو المكالمات الهاتفية بقصد التصيد؟

من الجيد أن يخطئ المخترقون بترك بعض البصمات الدالة عليهم، ومنها:

1-الكتابة والأخطاء القواعدية السيئة. إذ لا يتقن المخترقون الكتابة القواعدية بشكل دقيق، فوصول رسالة بريد الكتروني تحتوي على أخطاء قواعدية دليل علي أن الرسالة تصيدية.

2-الروابط الالكترونية، في حال وصول رابط إلكتروني مضمن في نص الرسالة، يجب التحقق من موثوقية الرابط وعدم النقر عليه مباشرة، يجب على المستخدم تمرير مؤشر الفأرة على الرابط ورؤية المحتوى المضمن داخل الرابط، فإن لم يكن هوا ذاته فيجب الحذر منه وعدم النقر عليه كما هو موضح في الصورة أدناه.

- التهديد في الرسائل، عادة ما يتضمن نص الرسالة التصيدية على تهديد للضحية بأهمية الاستجابة لمحتوى الرسالة والا سيتم تعطيل حساب المستخدم المالي على سبيل المثال، وشدة الإلحاح بالاستجابة للبريد بأقصى سرعة ممكنة وإلا فأنه سيتم تعطيل الحساب أو ما شابه.

- مكالمات هاتفية من شركات عالمية، ليس من الاعتيادي للشركات العالمية إجراء مكالمات هاتفية لعملائها لتوفير خدمة أو منتج!، وذلك يجب الحذر من هذه المكالمات وعدم تصريح أي معلومة كاسم المستخدم وكلمة المرور عبر الهاتف، وعادة ما يتم الحصول على رقم هاتف الضحية بظهور رسالة فور دخول الضحية إلى الموقع الإلكتروني الخبيث طالباً من الضحية إدخال رقم الهاتف لتوفير خدمة معينة كإصلاح الجهاز أو توفير رخصة برنامج ما.

كيفية التعامل مع هجمات التصيد:

يجب على المستخدم التحقق بصورة جيدة من المرسل ومن الرابط المرسل إن كان مطابقاً لرابط الموقع الموثوق، أيضاً عدم النقر على الرابط قبل إسقاط الفأرة عليه والتحقق من أن الرابط يرسلك للموقع نفسه، وإن كان هناك لبس ما، وسارت بك الشكوك، فقم بزيارة الموقع شخصياً باستخدام محركات البحث وتتبع لوائح الموقع والارشادات للذهاب للصفحة التي طلب منك البريد الالكتروني الذهاب إليها، أو الدخول لحسابك البنكي من موقع البنكي نفسه دون اللجوء لاستخدام الرابط المتواجد في البريد الالكتروني، أما في حالة ظهور دليل قاطع على ان البريد الالكتروني هو بريد تصيدي، فبادر بحذف الرسالة وإعادة توجيهها لأي جهة معنية بالتحقق من مصداقية المرسل والمحتوى وتسجيل الحدث الحاصل كي يعتبر محاولة تصيد.

وايضاً يجب الحذر من تحميل أي مرفق لبريد الالكتروني مشكوك في مصداقيته، وذلك تحسباً من تحميل

ملفات تنفيذية قابلة للتنفيذ فور استكمال تحميلها (ذات امتداد، (EXE) واحياناً يكون ذات امتداد docx ولكن مدموج معه ملف خفي عند التنزيل وهو ملف PDF بتغير ICON فقط ولكن في محتواه EXE.

الاختراق والحماية الالكترونية

من هم (المخترقون)؟

المخترقون (الهكرة) هم أشخاص كرسوا حياتهم في تعلم كل الطرق الممكنة للوصول إلى كسر الجدران الامنية وكسر الخصوصية مهما بلغت حمايتها ويتقنون كل شيء من اللغات البرمجية وحتى طرق الاستدراك والاساليب المتعددة وبالإضافة إلى الحيل باستخدام فن الهندسة الاجتماعية.

وهناك نوعان من المخترقين ولكن الاسماء تختلف حسب ما يتم ذكرهم فيه، فمثلاً لو تكلمنا عن المخترقين من الناحية العادية المعروفة، وهي ناحية الحياة الطبيعية التي ينطبق عليها صفات الطيب والشرير فسيتم تسمية النوعين بأصحاب القبعات البيض والسود.

في حالة أن المخترقين هم من يصلحون فهم أصحاب القبعات البيض أما إن كان هم من يفسدون فهم حتماً أصحاب القبعات السود.

وأحياناً يتم وصفهم بالفريق الأحمر والفريق الأزرق في هذه التسمية الفريق الأحمر ليس العدو، ولكنه ليس صديق ايضاً.

الفريقان يحملان نفس المهمة وهي اكتشاف الثغرات والتبليغ عنها، ولكن الفريق الأحمر يجد ثغرة ويستغلها ويسيطر على الشبكة أو على الأقل يحاول قبل أن يتم اكتشافه، والفريق الازرق يبحث عن الثغرة ويحاول سدها ويمنع الفريق الاحمر من الوصول إليها.

هنا الفريق الأحمر المكلف بالاختراق والفريق الأزرق مكلف بالحماية، ولكن لكلاهما نفس الهدف إيجاد الثغرات.

كيف تتم عملية الاختراق؟ وكيف نحمي أنفسنا منها؟

عملية الاختراق تختلف من جهاز إلى أخر ومن أجهزة إلى شبكات، فالاختراق يختلف نوعاً ما عن اختراق الشبكات.

فمثلاً ليتم اختراق جهازك يقوم المخترق بتنفيذ خطوات أساسية وهي:

1- جمع المعلومات وإيجاد نقاط الضعف

2- الاستهداف واستغلال نقاط الضعف

3- الاختراق والتحكم بشكل كامل

في الخطوة الأولي: يقوم المخترق بجمع أي معلومات عنك، من تاريخ ميلادك بالكامل (اليوم – الشهر- السنة) ورقم هاتفك، ومكان السكن، وفريق الكرة الذي تشجعه أو أي معلومة يتم إيجادها ستشكل فرقاً لديهم.

بعد جمع المعلومات يبدأ الاستهداف، أنت هدف سهل لأنك منحتهم معلومات يحتاجونها لاختراقك ومن أهمها رقم هاتفك وتاريخ ميلادك ومكان السكن أو مكان الذي ولدت فيه.

ومن ثم يبحث المخترق على نقاط ضعفك، فأحياناً تكون كلمة المرور هي نقطة الضعف الوحيدة عندك، ولو كان رقم هاتفك هو كلمة السر الخاصة بك، فانت الأن في الخطوة الثالثة.

الخطوة الثالثة والأخيرة هي الاختراق والتحكم بشكل كامل فمن خلال حسابك على الفيسبوك يمكنهم الوصول لكل خصوصياتك كصورك الشخصية التي تود مشاركتها إلا مجموعة معينة من الناس، أو ربما لا تكون صورة شخصية بل تكون محادثة شخصية بينك وبين شخص أخر أي أنه لا يجب أن تصل إلى أي شخص ثالث مهما كانت الأسباب، فعند وصول المخترق إلى صورك الشخصية السرية أو المحادثات السرية فإنك عرضة للابتزاز الإلكتروني مما يعني التحكم بشكل كامل والذي يصل المخترق لطلب أعمال غير أخلاقية منك ويصل الأمر بطلب فدية منك أو ارغامك على القيام بأفعال مخالفة للقيم أو تقديم تنازلات على حساب الأمانة الوظيفية وغيرها.

ولكن ليس حسابك على فيسبوك أو صورك أحياناً هي الهدف!
قد يكون جهازك هوا الهدف

الاختراق كيف يحدث؟

الاختراق نوعان: -

1 – داخلي

2- خارجي

النوع الأول يسمي داخلي لأنه يعتمد على الشبكة الداخلية للضحية بمعني أنه قد يتم اختراقك عند اتصالك بنقطة واي فاي المفتوح أو حتى واي فاي المحمي بكلمة المرور.

فمثلاً الأجهزة التي تعمل مع نظام تشغيل ويندوز Windows هي عديمة الحماية لإمكانية استغلال ما يعرف بالثغرات الأمنية.

أما عن نصيب الأجهزة التي تعمل بنظام أندرويد Android فهو أقل لكون المهاجم يحتاج إلى تحميل تطبيق لاختراقه أما أجهزة ويندوز فلا حاجة للتحميل إذا ما تم استغلال ثغرات خطيرة كثغرة Enternal blue.

أما الاجهزة التي تعمل بنظام IOS مثل (IPhone، iPod، iPad) تعتبر محمية من الاختراق عن طريق تحميل البرنامج ولكن أحياناً تظهر لها ثغرات خطيرة.

ففي سنة 2015 ظهرت ثغرة في تطبيق البريد الالكتروني التي تمكن المخترق من إرسال رسالة بالبريد لهذه الاجهزة ولكن بدل الرسالة تظهر شاشة تسجيل الدخول لحساب ICloud وهي تطابق التسجيل الحقيقي مما يؤدي بك لتصديقها وتسجيل الدخول ولكن يتم سرقة حسابك ومن ثم بياناتك.

فحسابات iCloud تقوم بنسخ كل بيناتك بما فيها صورك وحسابات التواصل الاجتماعي وقائمة الاسماء لديك.

أما عن الاجهزة التي تعمل بنظام ال Linux , mac ,فهي تعتمد اغلب الوقت على تنزيل برامج خبيثة حيث انها لا تحتوي على ثغرات كثيرة تتيح الوصول إلى الشبكة الداخلية.

والنوع الأخر، وهو الاختراق الخارجي، هو على الأغلب يعتمد على تنزيل فيروسات على جهازك أو تغيير سيرفر DNS (Domain name server) هو العصب الرئيسي للاتصال بالأنترنت.

فعند اتصالك بموقع الفيسبوك مثلاً أنت لا تتصل بي facebook.com بل أنت تطلب عنوان Ip الخاص بالفيسبوك عنون ال IP internet protocol هو بمثابة رقم الهاتف الخاص بك.

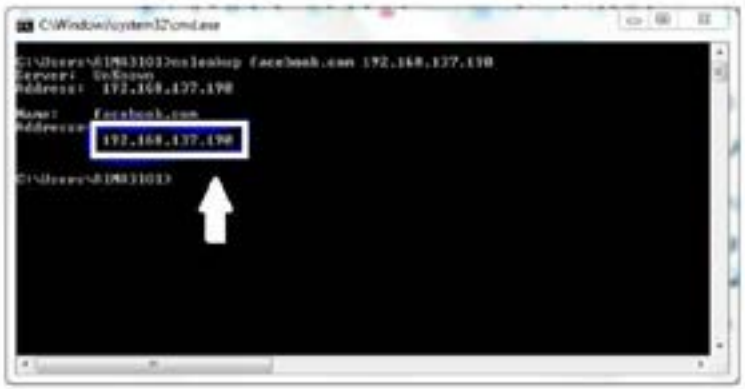
هنا لدينا مثال على عنوان ال IP الخاص بفيسبوك والذي قمنا باستخراجه من سيرفر ال DNS الخاص بشركة GOOGLE.

فإذا قام المخترق بتغيير هذا السيرفر لسيرفر أخر يقومون هم بالتحكم به، فإنك تصبح عرضة لما يمسي هجوم DNS Spoofing

إذا ما هو هجوم DNS Spoofing؟

DNS Spoofing هو هجوم يتم من خلاله تغيير عناوين IP للمواقع التي تريد زيارتها ومن ثم ارسالك إلى نفس الموقع، ولكنك لم تعد تتصل بعناوين IP الخاصة بهذه المواقع, بل بعناوين اخري قد تكون مفخخة او قد تكون فقط لمجرد مراقبتك.

وهنا مثال اخر لعنوان IP الخاص بفيسبوك ولكن بعد هجوم DNS Spoofing



نلاحظ أن العنوان قد اختلف ولكن مازال الاسم هو (الفيسبوك) في هذه الحالة قد تقع انت في المصيدة إذا تم استهدافك.

كيف يصاب جهازك بالفيروسات

الاصابة بالفيروسات أمر خطير، فعلى عكس هجوم DNS spoofing الاصابة بالفيروسات يعني ان جهازك أصبح كلياً للمخترقين.

الفيروسات أنواع وكل نوع له مزايا وحدود وسنذكرها بشكل مبسط:

1 – **فيروسات حصان طروادة** (Trojan)

هذا الفيروس يعتبر الأقوى بالنسبة للمخترقين لأنه ليس سهلاً على الضحية التعرف عليه، الاسم حصان طروادة مأخوذ من قصة حرب طروادة، التي وقعت تقريباً في القرن الثاني عشر او الثالث عشر قبل الميلاد وكيف قام الاغريق بإيقاع مدينة طروادة بخدعة الحصان الذي يحوي الجنود.

هذا النوع من الفيروسات يظهر للضحية في شكل برنامج عادي أو ملف عادي، بينما هو في الحقيقة فيروس، من خلال هذا الفيروس يستطيع المخترقين التحكم بشكل كامل في جهاز الضحية.

2- **فيروس الدودة** (worm)

دودة مورس (The Morris worm) ظهرت في 2 من نوفمبر 1988، وكانت واحدة من أولى فيروسات الكمبيوتر التي انتشرت عبر الإنترنت، ابتكرها روبرت تابان موريس، وهو طالب دارسات عليا في جامعة كورنيل (Cornell University)، وكان الهدف منها اختبار مدى انتشار البرامج الضارة، ولكن بسبب خطأ برمجي، انتشرت بشكل غير متوقع وتسببت في تعطيل آلاف الأجهزة، مما أدى إلى إبطاء الانترنت في ذلك الوقت.

3- **فيروس الباب الخلفي** (Back door)

هذا الفيروس يحمل هذه التسمية لمعناها الحرفي بل لقوة التشبيه هذا الفيروس يصنع لك طريقاً تدخل منه لجهاز الضحية دون أن يلاحظ الضحية أي شيء.

غالباً ما يستخدم هذا الفيروس ضد الانظمة التي لا تحتوي على ثغرات ولكن غاية المخترقون الوصول إليها، فيقوم المخترقون باستعمال هذه الفيروسات والتي توفر له الوصول متى يشاء.

4- فيروسات (Rootkit)

هذه الفيروسات هي عبارة عن مجموعة من الفيروسات وليس واحد فقط، الامر المميز لهذا الفيروس هوا انه يحمي نفسه تلقائياً من الكشف لأنه أساساً مصمم لهذا الغرض، ولكن الطريقة التي يحمي بها نفسه هي ميزة، فهو يحتاج لكي يشتغل ان يكون بأعلى صلاحيات ممكنة في النظام.

فعلى سبيل المثال على انظمة Windows يحتاج إلى تشغيل كمسؤول، أما على انظمة Lunix فهو يحتاج الي صلاحيات root، ما أن يتحصل على هذه الصلاحيات فهو الان يستطيع التحكم بشكل كامل في الجهاز وبالتالي يستطيع تعديل البرامج المثبتة على الجهاز بما فيها تلك المسؤولة عن اكتشاف هذا النوع من الفيروسات.

5- فيروسات الدعاية (Adware)

هذه الفيروسات تقوم فقط بإظهار دعايات إعلانية مزعجة للمستخدم بغرض التجارة وغيرها، وتعتبر هذه الأنواع من الفيروسات أكثرها تطفلاً، فهي تقوم أحياناً بتنزيل إضافات للمتصفحات وتغيير صفحة البدء للمتصفحات وأحياناً اخرى تقوم بتثبيت برامج دون علمك عند تحميل برامج مجانية أو زيارة مواقع غير موثوقة.

أعراض الإصابة بالفيروسات

الاصابة بالفيروسات لها أعراض على جهازك ومن أهمها:

- بطء عام في الجهاز.

الجهاز قد يصبح بطيء ولكن في بعض الاحيان يكون البطء سببه الفيروسات فهي تشتغل دون توقف ولكن في الخلفية.

- ظهور إشعار تفيد بوجد ملفات بانتظار كتاباتها:

احياناً يظهر لك إشعار من Windows عن وجود ملفات في انتظار كتابتها على القرص المضغوط، هذا الشعار يظهر إذا ما كان هناك ملف ينتظر الكتابة على القرص المظغوط ولكن من أين أتي؟

لقد سبق وذكرنا فيروس الدودة، ولقد ذكرنا أنها تنتشر فقد صممت لهذا الغرض. هذا الملف الذي ينتظر الكتابة هو عبارة عن دودة نفسها فهي تقوم بنسخ نفسها على جميع الأقراص أو أجهزة ال USB ولكن أحياناً تفشل في معرفة إن كان القرص ليزري فيقوم ال Windows بوضعها في مكان القرص ويقوم بإعلامك أن هناك ملف ينتظر أن تتم كتابته.

- عدم القدرة على تشغيل بعض البرامج:

كما ذكرنا فهناك نوع من الفيروسات يسمي rootkit وهو يقوم بتعديل البرامج المثبتة ليحمي نفسه من أن يكشف ولكن أحياناً يقوم بدمج نفسه في برنامج أخر او حتى يضع نفسه مكان البرنامج وهنا يفشل البرنامج في التشغيل.

- تغيير صفحة البدء في المتصفح الذي تستخدمه:

عندما تقوم بتشغيل المتصفح قد تلاحظ ان المتصفح يقوم بتوجيهك إلى موقع غريب دون إذنك، فور التشغيل. لقد سبق وان ذكرنا في انواع الفيروسات ان هناك فيروس دعائي يقوم بهذا النوع من التطفل.

- وجود برامج جديدة في الجهاز:

احياناً قد تلاحظ وجود برامج لم تقم انت بتثبيتها، هذا ايضاً من عمل الفيروسات الدعائية فهي قد تقوم بتنزيل ملف على جهازك والذي بدوره يحتوي على صلاحية فور ان ينتهي سيطلب منك إما تجديده او تنزيل برنامج اخر.

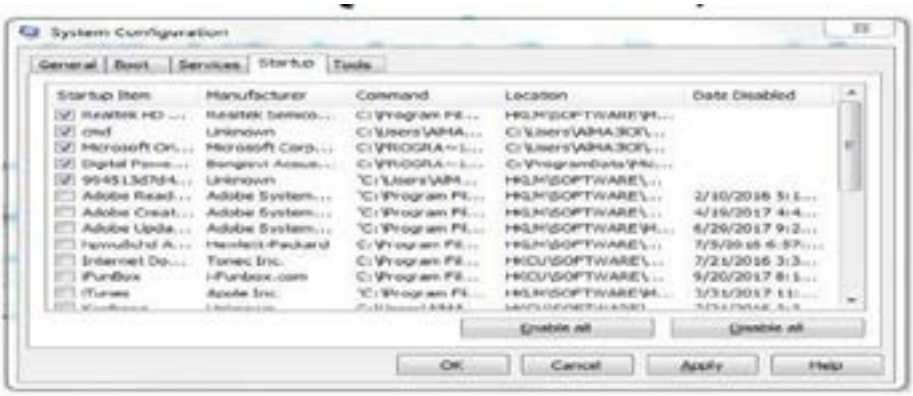
أوامر مساعدة في اكتشاف الاختراق

هناك العديد من الأوامر التي تساعدك على اكتشاف الاختراق ومنها ما يلي:

1- أمر MSCONFIG

هذا الأمر يقوم بفتح نافذة تحتوي على الكثير من الإعدادات الخاصة ب Windows ولكن نحتاج فقط لتعديل بدا التشغيل إن لزم الأمر ذلك.

فكما توضح الصورة يوجد هناك العديد من البرامج التي تشتغل مع بداء التشغيل ولكن كيف تتعرف على الفيروسات إن وجدت!



كما تلاحظ! توجد كلمة Unknown في عمود المصنع Manufacturer وهذا يعني أن المصنع غير معروف ولكن ليس هذا فحسب، فهناك أيضاً إشارة أخري وهي أن الأسماء تحت عمود الأسماء startup item توجد أسماء غريبة وأحياناً عشوائية فكما تلاحظون أن هناك «cmd » وهو موجه الاوامر لدى ويندوز ولكن لماذا قد يشتغل مع بدء التشغيل؟

الإجابة بسيطة، فهذا الفيروس يعتمد على موجه الأوامر في تشغيل نفسه كما أن هناك اسما أخر له ولكن هو عبارة عن أرقام عشوائية وحروف مختلطة.

والأن وقد تعرفنا على الفيروس وأصبح بإمكانك فحص جهازك بمفردك لذلك قم بإزالته بحذف علامة التصحيح ومن ثم قم بالضغط على زر OK في الأسفل.

2- **أمر** netstat –n

هذا الأمر يقوم بعرض الاتصالات الخارجية والداخلية في جهازك، وهنا يجب عليك أن تتعلم القليل عن اتصال الشبكة حتى تعلم كيف يتم التجسس عليك.

الاتصالات التي تراها في الصورة هي كل الاتصالات من وإلى جهازك، ولكن كيف تعرف ما إذا كان أحد هذه الاتصالات سببه الفيروسات!

حسناً الاتصال الأول والاتصال الثاني لهم نفس العنوان 127,0,0,1 وهو العنوان الداخلي لجهازك وهو ما يعرف ب loopback وهذا يعني أن الاتصالات هي اتصالات داخلية يقوم بها جهازك فلا داعي للخوف منها.

ونلاحظ ان الاتصال الثالث هوا لعنوان 129,168,1,48 وهو ليس عنوان وهناك بعد علامة «:" رقم المنفذ.

رقم المنفذ هو بمثابة رقم المدخل. فمثلاً في المطارات هناك العديد من البوابات وكل بوابة تحمل رقماً، الشبيه بين البوابات المطار وهذه الارقام هو الغرض فكلاهما يستخدم العبور.

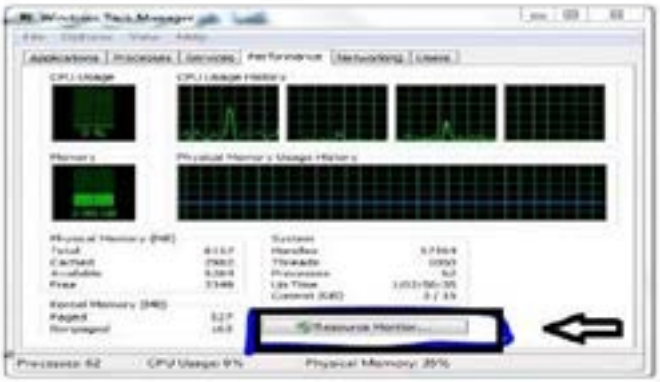
هذه النافذة هي عبارة عن بوابات اتصال بين العنوان الاول (أنت) والعنوان الأخر (الطرف الأخر)، ولكن هنا

الرقم يبدو عشوائياً قليلاً! فكما نلاحظ ان أغلب الاتصالات لها منفذين هما 80 و443.
هذه المنافذ هي عبارة عن منافذ خدمة المواقع (http/https) وهي تعتبر اماناً إلا في بعض الحالات الاستثنائية.
ولكن هناك اتصال غريب! وهو لا يتصل بخدمة المواقع!
أنه الاتصال 192,168,1,48:39905 المنفذ 39905 عشوائياً!

هذا يعتبر فيروس في أغلب الأحيان ولذلك سنقوم بإيقافه

اولاً: سنقوم بتشغيل مدير المهام عبر النقر بزر الفأرة الأيمن على شريط المهام واختيار تشغيل مدير المهام كما في الصورة أو اضغط على لوحة المفاتيح CLT+ALT+DEL

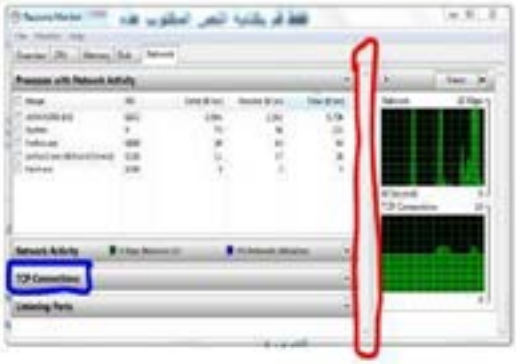
ومن ثم التوجه إلى الصفحة الرابعة كما هو موضح في الصورة، ومن ثم سيتغير شكل مدير المهام إلى هذا الشكل، قم بالضغط على هذا الزر كما في الصورة



وفي حالة اختلاف إصدار الويندوز الخاص بك عن المستخدم في الشرح فقط قم بكتابة النص المكتوب هذه الكلمة في البحث في قائمة ابدا Performance وسيظهر لك البرنامج.

نافذة البرنامج في الصورة تحتوي على جميع البرامج التي تشتغل، ولكن نحن نحتاج فقط للبرامج التي تجري اتصالات لنبحث عن ذلك الذي يقوم بالاتصال المشبوه.

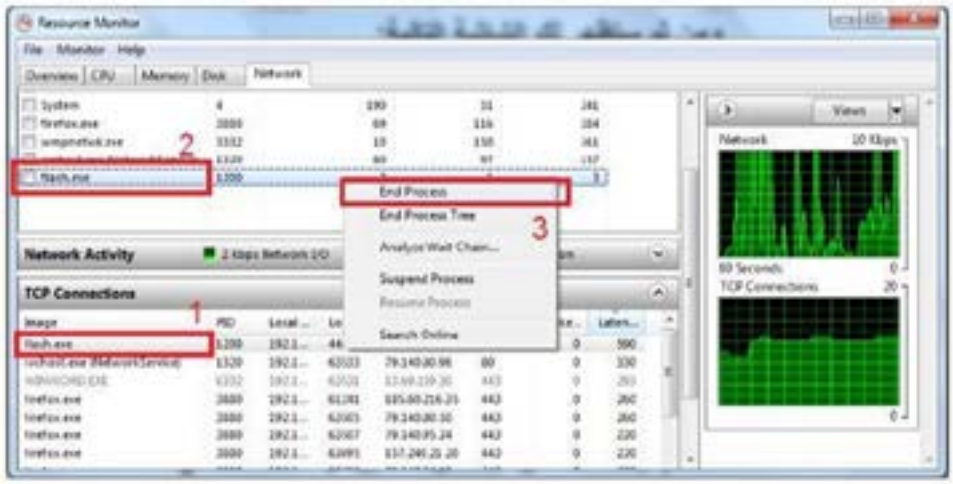
بعد الضغط على صفحة الشبكة كما هو مشار إليها في الصورة في الأعلى، سيتغير الشكل كما هو موضوح في هذه الصورة.



ولكن أنت تحتاج الأن إلى النقر على TCP connections المشار عليها باللون الأزرق.

وإذا لم تكن أمامك في الشاشة فحاول النقر بزر الفأرة الأيسر على منطقة المشار إليها باللون الأحمر ثم السحب إلى الأسفل، ومن ثم ستظهر لك الشاشة التالية:

حسناً، هنا ابحث عن الاتصال المشبوه وكما تلاحظ في الصورة لقد عثرت على ذلك الاتصال المشبوه بالبحث عن المنفذ الاتصال به كما ظهر في امر Netstat –n ، والأن تابع كيف سأقوم بإيقافه.



حسناً الأن هنا ثلاث خطوات يجب إتباعها:

- معرفة اسم البرنامج الذي يجري الاتصال كما هو موضح في الرقم 1 – في الصورة.
- النقر بزر الفأرة الايمن على البرنامج.
- الضغط على أول خيار من القائمة المنبثقة وهو خيار " End process " - هكذا تكون انهيت الاتصال المشبوه ومن ثم ارجع إلى الأمر Msconfig وابحث عن الفيروس يحمل نفس الاسم في قائمة التشغيل وقم بحذفه.

أهم الاحتياطات التي يجب اتخاذها

هناك احتياطات يجب اتخاذها لتفادي الوقوع فريسة للمخترقين ومنها ما يلي:

1- استخدام أحدث برامج الحماية من الفيروسات وقم بعمل الفحص والمسح الدوري.
2- لا تدخل على المواقع المشبوهة.
3- عدم فتح اي رسالة الالكترونية من مصدر مجهول.
4- لا تقوم بتثبيت برامج مجهولة المصدر.
5- لا تسمح لأشخاص مجهولين باستعمال اجهزتك الخاصة.
6- استخدم اخر التحديثات المتوفرة لجهازك.
7- قم بإغلاق الواي فاي في حالة عدم استخدامه او في وقت نومك.
8- لا تنشر معلومات عنك حتى يصبح من الصعب معرفة كلمة المرور الخاصة بك.
9- تأكد من اتصالك الصحيح في شبكة الواي فاي سواء كانت خاصة او عامة.
10 - قد تكون هناك شبكة تحمل نفس اسم الشبكة التي لديك احرص على عدم الربط معها.

أمن الهواتف الذكية

أصبح أمن الهواتف ذا أهمية كبيرة، وذلك بسبب التوسع في انتشار الهواتف النقالة (الذكية) ومما يثير القلق بشكل خاص هو أمن المعلومات الشخصية والتجارية والمخزنة الان على الهواتف الذكية، كما ان الكثير من مستخدمي الانترنت يستخدمون الهواتف الذكية مثل وسائل الاتصال، ايضاً كوسيلة لتخطيط وتنظيم عملهم وحياتهم الخاصة، الهواتف الذكية تحتوي على كمية كبيرة من المعلومات الحساسة التي يجب معرفة ان جميع الهواتف الذكية، وأجهزة الحاسوب هي الاهداف المفضلة للهجمات، وهذه الهجمات غالباً ما تستغل نقاط الضعف المتعلقة بالهواتف الذكية التي يمكن ان تأتي من وسائل الاتصال مثل خدمة الرسائل القصيرة SMS وخدمة الرسائل متعددة الوسائط MSS وجي اسم ام GSM وشبكات الواي فاي WIFI.

لماذا أمن الهواتف ذكية؟

- كثير من بياناتنا في الاجهزة الذكية

- لأنها معرضة للاختراق والتجسس

- لأنها أجهزة محمولة فمعرضة ايضاً للفقدان والسرقة

كشفت «فبراكود » للاختبارات الامنية، في أحدث تقرير لها ان حوالي 59 % من المؤسسات قد شهدت زيادة في البرمجيات الخبيثة لديها بسبب الهواتف المتنقلة غير الامنة والتي غالباً ما تنجم عن التطبيقات غير الامنة.

أهم طرق الاختراق تأتي عن طريق التطبيقات الغير آمنه
طرق حماية هاتفك الذكي من الاختراق

1- تحديث النظام والتطبيقات بانتظام

احرص على تحديث نظام التشغيل والتطبيقات دائمًا، لأن التحديثات غالبًا ما تتضمن إصلاحات أمنية تسد الثغرات التي قد يستغلها المخترقون.

2- تحميل التطبيقات من مصادر موثوقة فقط

لا تثبّت التطبيقات إلا من متجر Google Play أو App Store، وتجنب تحميل تطبيقات APK من مواقع غير معروفة.

3- استخدام كلمات مرور قوية وتفعيل المصادقة الثنائية

استخدم كلمة مرور قوية لهاتفك وتجنب الأنماط السهلة مثل ‹1234›. قم بتفعيل المصادقة الثنائية لحماية حساباتك.

4- عدم الاتصال بشبكات Wi-Fi عامة غير آمنة

تجنب الاتصال بشبكات Wi-Fi العامة، خاصة بدون VPN، لأنها قد تكون وسيلة لاختراق هاتفك.

5- الحذر من الروابط والرسائل المشبوهة

لا تفتح الروابط المرسلة عبر SMS أو البريد الإلكتروني من مصادر غير معروفة.

6- تقييد أذونات التطبيقات

قم بمراجعة أذونات التطبيقات واحذف التطبيقات التي تطلب صلاحيات غير ضرورية.

7- تفعيل ميزات الأمان المدمجة في الهاتف

قم بتفعيل ميزة ‹Find My Device› لأجهزة أندرويد أو ‹Find My iPhone› لاستعادة الهاتف في حال ضياعه أو سرقته.

8- تثبيت تطبيق أمني موثوق

يمكنك تثبيت تطبيق أمني موثوق مثل Bitdefender أو Norton للكشف عن الفيروسات.

9- تجنب توصيل الهاتف بأجهزة غير موثوقة

لا تقم بتوصيل هاتفك بأجهزة حاسوب أو شواحن USB غير موثوقة، فقد تحتوي على برامج ضارة.

10- أخذ نسخ احتياطية من بياناتك وقم بعمل نسخ احتياطي لبياناتك المهمة بانتظام لاستعادتها في حال الاختراق.

كيف تعرف أن هاتفك الذكي مخترق؟

1- استهلاك بطارية غير طبيعي.
2- سخونة الهاتف الزائدة دون سبب واضح.
3- زيادة استهلاك البيانات بشكل غير مبرر.
4- ظهور تطبيقات غريبة أو اختفاء تطبيقات دون تدخل منك.
5- نوافذ منبثقة وإعلانات غير طبيعية.
6- أداء الهاتف أصبح بطيئًا فجأة.
7- ظهور رسائل أو مكالمات لم ترسلها.
8- أصوات غريبة أثناء المكالمات.
9- نشاط غريب في الحسابات المرتبطة بالهاتف.
10- إيقاف تشغيل الهاتف أو إعادة تشغيله تلقائيًا دون سبب.

ماذا تفعل إذا كنت تعتقد أن هاتفك مخترق؟

1- احذف أي تطبيق مشبوه من قائمة التطبيقات.
2- افحص هاتفك ببرنامج مضاد للفيروسات مثل Malwarebytes أو Bitdefender.
3- غير كلمات المرور لحساباتك المهمة.
4- قم بإعادة ضبط المصنع إذا استمر الاختراق، ولكن تأكد من أخذ نسخة احتياطية للبيانات المهمة أولًا.

الابتزاز الإلكتروني

يعرف الابتزاز الإلكتروني على انه عملية تهديد بنشر صور او فيديو او معلومات شخصية وحساسة للمبتز ومعظم الطلبات تتلخص في التالي!

1. دفع مبالغ مادية.
2. القيام بأعمال غير مشروعة.
3. القيام بأعمال منافية للأخلاق.
4. الافصاح عن معلومات سرية مؤسساتية او سياسية.

كيف يتم عملية الابتزاز؟

تبدأ العملية عن طريق إقامة صداقة مع الشخص المستهدف،

ثم الانتقال إلى مرحلة التواصل عن طريق برامج المحادثات المرئية او مواقع التواصل الاجتماعي، ليقوم بعد ذلك المخترق باستدراج الضحية، ليقوم بأمور مخلة بالشرف الضحية وتسجيل محادثة التي تحتوي على محتوى مسيء وفاضح للضحية.

كيفية تتجنب الوقوع في فخ المبتزين؟

أ.تجنب طلب صداقات أو قبول طلب صداقات من قبل أشخاص غير معروفين.

ب.عدم الرد والتجاوب على أي محادثة ترد من مصدر غير معروف.

ت.تجنب مشاركة معلوماتك الشخصية وصورك مع أصدقائك في فضاء الإنترنت "أصدقاء الفيسبوك المعارف الجدد التي لا تربطك بهم اي معرفة مسبقاً".

ث.ارفض طلبات إقامة محادثات الفيديو مع أي شخص، ما لم تكن تربطك به صلة وثيقة.

ج.لا تنجذب للصور الجميلة والمغرية، وتأكد من شخصية المرسل.

ح.قم بتزويد جهازك الإلكتروني ببرامج مكافحة الفيروسات، وغيرها من برامج الحماية.

خ.لا تقم بالموافقة على طلبات التحميل لأي مادة ترد إليك من مصدر غير معروف.

المراجع:

- المعلومات الواردة بتقدير حجم الجرائم المعلوماتية عالميًا وعربيًا في تقرير The Norton Cybercrime Report 2011 الصادر عن شركة سيمانتك العالمية المتخصصة في أمن المعلومات حول أوضاع جرائم المعلومات في عام 2011، والذي حمل عنوان «صورة إجمالية لأوضاع أمن المعلومات حول العالم».

- أمن المعلومات والحماية الرقمية جمال محمد غيطاس – باحث ورئيس تحرير مجلة «لغة العصر» الصادرة عن المؤسسة الأهرام، محرر تكنولوجيا المعلومات بصحيفة الأهرام.

- كتاب «أمن المعلومات بلغة ميسرة» لمحمد بن عبدالله القحطاني وخالد بن سليمان الغثبر.

- كتاب «أمن المعلومات باللغة العربية» للدكتور ذيب القحطاني.

- كتاب «السيبرانية هاجس العصر» د. منى الأشقر جبور.

المعيار القانوني/ القضائي للهكترة
(تمييز الهاكر ونشاطه عن غيره من الاعمال؟)

ترجمة الحكم في قضية PETERSEN / بيترسي امام القضاء الأمريكي 1996
محكمة الاستئناف للولايات المتحدة الامريكية/ الدائرة التاسعة

United States v. Justin Tanner Petersen,

98 F.3d 9) 502th Cir. 1996)

Court of Appeals for the Ninth Circuit

Filed: October 22nd, 1996

Precedential Status: Precedential

Citations: 98 F.3d 502

Docket Number: 50037-96

98 F.3d 502

65 USLW 96 ,2367 Caal. Daily Op. Serv. 7770,

96 Daily Journal D.A.R. 12,819

UNITED STATES of America, Plaintiff-Appellee,

v.

Justin Tanner PETERSEN, Defendant-Appellant.

Nos. 50038-96 ,50040-96 ,50037-96 and 50039-96.

United States Court of Appeals,

Ninth Circuit.

Argued and Submitted June 1996 ,4.

Decided Oct. 1996 ,22.

Jay L. Lichtman, Los Angeles, CA, for defendant-appellant.

David J. Schindler, George S. Cardona, Assistant United States Attorneys, Los Angeles, CA, for plaintiff-appellee.

Appeals from the United States District Court for the Central District of California, Stephen V. Wilson, District Judge, Presiding. D.C. Nos. CR-00956-91-SVW, CR-91--00995SVW, CR-00575-92-SVW and CR-00214-95-SVW.

Before: FLETCHER, BEEZER, and KLEINFELD, Circuit Judges.

FLETCHER, Circuit Judge:

يستأنف المتهم Justin Tanner Petersen الحكم الصادر ضده بالعقوبة بعد اقراره بالذنب plea of guilty في تهم الاحتيال بالحاسوب، وحيازة سيارة مسروقة تم نقلها عبر خطوط الولاية، والتآمر لارتكاب الاحتيال بالحاسوب computer fraud والاحتيال السلكي wire fraud، واعتراض الاتصالات السلكية والإلكترونية interception of wire and electronic communications في أربع قضايا منفصلة تم دمجها للحكم. ويطعن Petersen في التعديل التصاعدي (1) لمحكمة المقاطعة المكون من مستويين لاستخدام مهارة خاصة special skill تستند إلى مهاراته في الحاسوب. (2) تعديل تصاعدي على مستويين لعرقلة سير العدالة؛ (3) الفشل في خفض مستوى الجريمة على أساس أن إحدى عمليات الاحتيال كانت مجرد محاولة؛ و (4) الأمر برد مبلغ 40,000 دولار. لدينا اختصاص قضائي بموجب المادة 1291 من قانون الولايات المتحدة رقم 28 ونؤكد ذلك.

قاضي المقاطعة: FLETCHER

في 20 يوليو 1992، أقر Petersen بأنه مذنب في ثلاث قضايا جنائية. وفي الوثيقة CR SVW-00995-91، أقر بأنه مذنب بتوجيه تهمة واحدة من ثماني تهم للاحتيال الحاسوبي في انتهاك للمادة 1030(أ)(2) من القسم 18 من تقنين الولايات المتحدة U.S.C. وتضمنت لائحة الاتهام indictment بأنه تمكن بين 11 فبراير 1991 و21 أبريل 1991 من الوصول غير المصرح به إلى حواسيب شركة TRW Information Services، وهي وكالة للإبلاغ عن الائتمان الاستهلاكي consumer credit reporting agency. وأظهرت الأدلة عند إصدار الحكم أن Petersen، الذي كان آنذاك في تكساس، شارك في الاحتيال على بطاقات الائتمان عن طريق اختيار أسماء من دليل الهاتف و"هكترة hacking" خدمات الإبلاغ الائتماني للحصول على معلومات استخدمها لطلب بطاقات ائتمان احتيالية. ثم وجه اتهامات على بطاقات الائتمان الاحتيالية.

وفي الوثيقة SVW-00956-91-CR، أقر Petersen بأنه مذنب pled guilty بتهمة واحدة من لائحة اتهام واحدة لحيازة سيارة مسروقة عبرت حدود الولاية في انتهاك للمادة 18 من قانون الولايات المتحدة 2313. وأظهرت الأدلة عند إصدار الحكم أنه في 12 يناير 1991 أو نحو ذلك، رد Petersen، الذي كان آنذاك في كاليفورنيا، على إعلان في صحيفة محلية يعرض سيارة بورش 1986 للبيع. أخذ Petersen السيارة لاختبار القيادة وانطلق بالسيارة. نقل لوحات الترخيص license plates من سيارة مسجلة له إلى سيارة بورش المسروقة وانتقل إلى تكساس.

وفي الوثيقة SVW-00575-92 CR، أقر Petersen بأنه مذنب pled guilty في جميع تهم المعلومات المكونة من أربع تهم. اتهم البند الأول Petersen بالتآمر للوصول غير المصرح به إلى نظام كمبيوتر فيدرالي للمصلحة لتنفيذ مخطط للاحتيال واعتراض الاتصالات السلكية والإلكترونية في

انتهاك للقسم 18 من تقنين الولايات المتحدة المواد 371 و1030 (أ) (4) و2511. اتهم البند الثاني Petersen باعتراض الاتصالات السلكية والشفوية والإلكترونية في انتهاك للمادة 2511 من الباب 18 من تقنين الولايات المتحدة. اتهمت التهمتان الثالثة والرابعة Petersen بالوصول غير المصرح به إلى نظام كمبيوتر فيدرالي في انتهاك للمادة 1030 (أ) (4) من الباب 18 من تقنين الولايات المتحدة.

وفيما يتعلق بالتهمة الأخيرة، أظهرت الأدلة عند إصدار الحكم أنه في 28 سبتمبر 1989، تمكن Petersen من الوصول غير المصرح به إلى Pacific Bell لتسهيل اعتراض ومصادرة الخطوط الهاتفية لمحطة الإذاعة KPWR FM. اكتشف حلفاء confederates المدعو Petersen وهما Kevin Lee Poulsen و Ronald Mark Austin برنامج حاسوب يمكن التلاعب به manipulated "للتلاعب/ للعبث rig" بالمسابقات الترويجية للمحطة الإذاعية من خلال السيطرة على خطوط الهاتف المؤدية إلى محطة الراديو للتأكد من أنهم كانوا المتصل الصحيح للفوز بجوائز مختلفة. حيث تم نصح Petersen بهذا المخطط، واستخدم Petersen المعلومات للاتصال بالمحطة الإذاعية و "الفوز" بجائزة نقدية بقيمة 10000 دولار. و"فاز" Poulsen وAustin بسيارتين على الأقل من نوع Porsche، وجائزة نقدية بقيمة 20000 دولار، وجائزة نقدية بقيمة 10000 دولار، ورحلتين إلى هاواي.

وألقي القبض على Petersen في دالاس Dallas بولاية تكساس Texas في يونيو 1991 أو نحو ذلك، ووافق على استجوابه بشأن أنشطته الإجرامية criminal activities. وأبرم اتفاق إقرار بالذنب plea agreement يتطلب تعاونه ومساعدته في إنفاذ القانون ونقل إلى المنطقة الوسطى من كاليفورنيا. وهناك أطلق سراحه بكفالة من أجل مساعدة مكتب التحقيقات الفيدرالي. بعد أن أقر Petersen بأنه مذنب في التهم المذكورة أعلاه، استمر الحكم بالنص عدة مرات من أجل السماح بتعاون Petersen. وشارك Petersen في مساعدة واسعة النطاق للحكومة أثناء الإفراج عنه بكفالة. استأجر له مكتب التحقيقات الفيدرالي شقة مع أجهزة حاسوب وخطوط هاتف وأجهزة الاستدعاء pagers. من بين أمور أخرى، ساعد Petersen في مصادرة seize على حاسوب Poulsen، مما أدى إلى أدلة استخدمت لإدانة Poulsen، وساعد في جمع الأدلة ضد Austin، الذي حوكم وأدين في نهاية المطاف ultimately.

وفي أكتوبر 1993، تلقى مكتب التحقيقات الفيدرالي معلومات تشير إلى أن Petersen قد شارك في نشاط إجرامي إضافي أثناء الإفراج عنه بكفالة on bail. واجتمعت جهة الاتهام وهي الولايات المتحدة مع Petersen ومحاميه لمواجهتهم بهذه المزاعم. واعترف Petersen بارتكاب أعمال إضافية من الاحتيال على بطاقات الائتمان أثناء الإفراج عنه بكفالة. خلال عطلة، هرب Petersen. وصدر أمر قضائي بالقبض عليه.

وفي 24 يناير/كانون الثاني 1994، مثل المحامي أمام محكمة المقاطعة. وظل بيترسن هاربا. وحذفت المحكمة تاريخ النطق بالحكم من الجدول الزمني في انتظار القبض على بيترسن أو استسلامه الذاتي self-surrender.

بينما كان Petersen هاربا fugitive، اخترق أجهزة الحاسوب الخاصة ب Heller Financial وحصل على الرموز اللازمة لتنفيذ تحويل مصرفي من Heller إلى حساب مصرفي آخر. في 17 أغسطس 1994، واشاع Petersen تهديدين بوجود قنبلة في مبنى Heller كإلهاء. وأثناء إخلاء المبنى، قام بتنفيذ تحويل مصرفي بقيمة 150000 دولار من Heller عبر بنك ميلون Mellon Bank إلى حساب في بنك الاتحاد Union Bank. في اليوم التالي اكتشف هيلر التحويل وتمكن من الاستيلاء على مبلغ 150,000 دولار قبل إزالته من بنك الاتحاد.

وفي 29 أغسطس 1994، تم القبض على بيترسن. وفي 27 مارس 1995، أقر بأنه مذنب في كلتا التهمتين استنادا إلى الجرائم التي ارتكبها أثناء الإفراج عنه بكفالة. الوثيقة CR 95-00214-SVW. حيث اتهم وفق البند الأول بالتآمر لارتكاب الاحتيال الحاسوبي والاحتيال السلكي في انتهاك للقسم 18 من تقنين الولايات المتحدة المواد 371 و 1030 (أ) (4) و 1343. واتهم وفق البند الثاني Petersen بحيازة خمسة عشر جهازا أو أكثر من أجهزة الوصول غير المصرح بها (أي كلمات مرور الحاسوب) التي سرقت وتم الحصول عليها بقصد الاحتيال في انتهاك للمادة 1029 (أ) من الباب 18 من تقنين الولايات المتحدة.

وتم توحيد consolidated القضايا الأربع للنطق بالحكم. في 27 نوفمبر 1995، حكمت محكمة المقاطعة على Petersen بفترة سجن إجمالية قدرها 41 شهرا، ولمدة ثلاث سنوات من الإفراج تحت الإشراف، ورد مبلغ 40,000 دولار تقريبا. واستند الحكم إلى مستوى جريمة معدل من 18 شهرا وتاريخ إجرامي من الفئة الثالثة مما أدى إلى مجموعة مبادئ توجيهية تتراوح بين 33 و 41 شهرا.

تم حساب مستوى الجريمة المعدل على النحو التالي: مستوى الجريمة الأساسي بموجب U.S.S.G. § 2F1,1 (الاحتيال Fraud والخداع Deceit; التزوير Forgery; الجرائم التي تنطوي على أدوات معدلة أو مزيفة Offenses Involving Altered or Counterfeit Instruments) [6 نقاط]؛ خسارة أكثر من 200,000 دولار بموجب الفقرة 2F1,1(b)(1) [8 نقاط]؛ أكثر من الحد الأدنى للتخطيط بموجب الفقرة 1,1,2(ب)(2) من المادة 2F1 [نقطتين]؛ استخدام مهارة خاصة special skill بموجب الفقرة 3B1,3 [نقطتان]؛ عرقلة سير العدالة obstruction of justice بموجب المادة 3C1,1 [نقطتان]؛ ارتكاب جريمة أثناء الإفراج عنه بكفالة committing offense while on bail بموجب المادة 2J1,7 [3 نقاط]؛ قبول المسؤولية acceptance of responsibility بموجب الفقرة 3E1,1(أ) [ناقص 3 نقاط]؛ والمساعدة الكبيرة في المغادرة substantial assistance downward departure بموجب الفقرة 5K1,1 [ناقص نقطتين].

هذا ولقد تم مراجعة النتائج الوقائعية التي توصلت إليها محكمة المقاطعة عند إصدار الحكم بحثا عن خطأ واضح. الولايات المتحدة ضد الولايات المتحدة ( ) فوينتيس - مندوزا، 56 3d.F 1113, 1116 (9th Cir.)، شهادة مرفوضة، --- ----, الولايات المتحدة 116 S.Ct. 326, 133 2d.L.Ed 227 (1995)؛ (18) مدونة قوانين الولايات المتحدة § 3742 (ه). ويستعرض تطبيق محكمة المقاطعة للمبادئ التوجيهية لإصدار الأحكام على الوقائع بحثا عن إساءة استخدام السلطة التقديرية abuse of discretion. وتفسير محكمة المقاطعة للمبادئ التوجيهية، كمسألة قانونية،... لا يحق له الإذعان، على الرغم من أن "تحول صغير إلى ما إذا كنا نصنف مراجعة هذه المسألة بالذات إساءة استخدام السلطة التقديرية أو من جديد، من أجل ان تسيء محكمة المقاطعة بحكم تعريفها استخدام سلطتها التقديرية عندما ترتكب خطأ قانونيا".

حيث تقرر في احكام عدة ((تقرر أن خروج محكمة محلية عن المبادئ التوجيهية يعاد النظر فيه بسبب إساءة استخدام السلطة التقديرية)) وأيضا تقرر ((تقرر محكمة الاستئناف... الاحترام الواجب لتطبيق محكمة المقاطعة للمبادئ التوجيهية على الوقائع").

A وصف المهارة الخاصة Special Skill Adjustment

فرضت محكمة المقاطعة تعديلا تصاعديا من مستويين بموجب المادة 3B1,3 من تقنين الولايات المتحدة من أجل "استخدام مهارة خاصة USE of a special Skill". وعلى الرغم من أن Petersen لم يتلق تدريبا رسميا في مجال أجهزة الحاسوب، إلا أن محكمة المقاطعة district court استنتجت reasoned أنه "من الواضح أن لديه معرفة استثنائية بكيفية عمل أجهزة الحاسوب وكيفية تخزين المعلومات how information is stored، وكيفية استرداد المعلومات how information is retrieved، وكيف يمكن الحفاظ على أمن هذه الأنظمة أو غزوها" وأنه "حتى لو لم يتمكن من إنشاء برامج، يمكنه بالتأكيد العمل في النهاية الأمنية لأعمال الحاسوب". واستنادا إلى هذه النتائج، قررت محكمة المقاطعة أن قدرات Petersen الحاسوبية تشكل مهارة خاصة بالمعنى المقصود في الفقرة § 3B1,3.

ينص القسم 3B1,3 على أنه يجوز لمحكمة المقاطعة تعزيز مستوى جريمة المتهم إذا "أساء استخدام منصب ثقة عامة أو خاصة، أو استخدم مهارة خاصة special skill، بطريقة سهلت بشكل كبير ارتكاب الجريمة أو إخفائها." U.S.S.G. § 3B1,3. وتعرف عبارة "مهارة خاصة special skill " بأنها "مهارة لا يمتلكها أفراد من عامة الجمهور وتتطلب عادة قدرا كبيرا من التعليم أو التدريب أو الترخيص. ومن الأمثلة على ذلك الطيارون والمحامون والأطباء والمحاسبون والكيميائيون وخبراء الهدم". وينطبق التعديل على الأشخاص الذين يسيئون استخدام مناصبهم محل الثقة أو مهاراتهم الخاصة لتسهيل ارتكاب جريمة أو إخفائها إلى حد كبير. وينظر إلى هؤلاء الأشخاص عموما على أنهم أكثر عرضة للاذناب culpable".

لقد فسرنا الفقرة 3B1,3 على أنها تتطلب من المتهم استخدام "مهارة مشروعة موجودة مسبقا لا يمتلكها عامة الناس" في ارتكاب الجريمة أو إخفائها. "إن استخدام المبدأ التوجيهي لكلمة 'ميسرة facilitated' يعني ضمنا أن تعزيزا لاستخدام مهارة خاصة بموجب المادة 3 باء-1-3 ينبغي أن ينطبق إذا كانت المهارة الخاصة تجعل من الأسهل بكثير على المدعى عليه ارتكاب الجريمة أو إخفائها". حيث رفضنا تطبيق الفقرة 3B1,3 "لمجرد أن الجريمة كان من الصعب ارتكابها أو تتطلب مهارة خاصة لإكمالها". ونحن نستنتج أن محكمة المقاطعة لم تخطئ في تحديد أن قدرات Petersen الحاسوبية تدعم تعزيز المهارات الخاصة. وكما وجدت محكمة المقاطعة، فإن Petersen ماهر في الوصول إلى أنظمة الحاسوب والتلاعب بها. هذه المهارات ذات مستوى عال ولا يمتلكها أفراد من عامة الناس.

وعلى الرغم من أن المبادئ التوجيهية تنص على أن المهارات الخاصة "عادة usually" تتطلب قدرا كبيرا من التعليم أو التدريب أو الترخيص، فإن الفقرة 3B1,3 من تقنين الولايات المتحدة تعلق على ذلك. (الملاحظة 2)، وهذا التعليم أو التدريب أو الترخيص ليس شرطا مسبقا مطلقا لتعديل المهارات الخاصة. وعلى الرغم من افتقار Petersen إلى التدريب الرسمي أو الترخيص، إلا أن مهاراته الحاسوبية المتطورة يمكن مساواتها بشكل معقول بالمهارات التي يمتلكها الطيارون والمحامون والكيميائيون وخبراء الهدم لأغراض الفقرة 3B1,3.

ومن الواضح أن Petersen "استخدم used" مهاراته في الحاسوب في ارتكاب الجرائم التي أقر بأنه مذنب بها. من خلال تمكينه من اقتحام أنظمة الحاسوب المتطورة sophisticated computer systems، ووضع أجهزة التنصت place wire taps على الهواتف، وتحويل مبالغ كبيرة transfer large sums من المال بين البنوك، فإن مهارات Petersen الحاسوبية "سهلت facilitated" قدرته على ارتكاب سلسلة من الجرائم.

والسؤال الأقرب هو ما إذا كانت قدرات Petersen الحاسوبية تشكل مهارات "مشروعة legitimate" بالمعنى المقصود في الفقرة 3B1,3. في حين أن محكمة المقاطعة district court خلصت بشكل صحيح properly إلى أن مهارات Petersen في اختراق الحاسوب يمكن نقلها إلى الاستخدام المشروع legitimate use في المستقبل، مثل العمل في النهاية الأمنية لصناعة الحاسوب work in the security end of the computer industry، فإن هذا لا يعني بالضرورة أن Petersen يحوز possessed مهارة مشروعة موجودة مسبقا preexisting legitimate skill.

إن تفسير مذكرة المعلومات الأساسية بأن الأشخاص الذين يسيئون استخدام مهاراتهم الخاصة يخضعون لتعديل تصاعدي حيث ينظر إليهم عموما على أنهم أكثر ذنبا more culpable يشير إلى نية تطبيق التعديل على شخص مثل مبرمج حاسوب ناجح ومتمرس

يتحول إلى الجريمة، على سبيل المثال، لص قد يكون قادرا على نقل معرفته بأنظمة الإنذار إلى عمل مشروع كخبير أمني في المستقبل. ("لا يوجد في التعليق ما يشير إلى أن الفقرة 3B1,3 تنطبق على المجرم الذي... يعظم حيل تجارته ويصبح بارعا في ارتكاب جريمة لا يعرف عامة الناس كيف يرتكبونها").

لم تكن معرفة Petersen بالحاسوب التي تعلمها بنفسه نتيجة "استثمار مجتمعي خاص وتشجيع مما يسمح للشخص باكتساب المهارات التي يتم الاحتفاظ بها بعد ذلك في نوع من الثقة لنا جميعا". ولكن يمكن أيضا اكتساب مهارة خاصة دون استثمار اجتماعي، وهي مهارة تمكن المرء من إيذاء الآخرين بشكل أكثر فعالية من الشخص الذي لا يمتلك هذه المهارة، لذلك قد تكون هناك حاجة إلى رادع أكبر لتثبيط استخدامها في سوء المعاملة. أيضا، يبدو أن Petersen استخدم مهاراته في الحاسوب في العمل لصالح وكالة تحقيق خاصة في الثمانينات من القرن العشرين واعترف محامي الدفاع بأن موكله قد نصح الشركات أثناء الإفراج عنه بكفالة حول كيفية "جعل نظام الكمبيوتر الخاص بهم آمنا من المتسللين الآخرين". حث Petersen المحكمة، ووافقت المحكمة، على عدم منع Petersen من استخدام أجهزة الحاسوب في سياق عمله في المستقبل. هذا يشير إلى أن Petersen كان بإمكانه استخدام مهاراته في الحاسوب لنشاط قانوني مفيد اجتماعيا. وبدلا من ذلك، أساء استخدام معرفته بالتكنولوجيا وقدرته على الوصول إلى أنظمة الحاسوب والتلاعب بها، مما مكنه من ارتكاب جرائم خطيرة.

ان Petersen هو شخص ماهر في الوصول إلى أنظمة الحاسوب والتلاعب بها. هذه المهارة لا يتقاسمها أفراد من عامة الناس؛ سهلت المهارة تنفيذه لسلسلة من الجرائم؛ كانت موجودة قبل تنفيذه للجرائم. وهي قابلة للترجمة translatable (وقد ترجمت) إلى استخدام مشروع. وبناء على ذلك، لم تخطئ محكمة المقاطعة في تعديل مستوى جريمة Petersen بموجب الفقرة 3B1,3 لاستخدام مهارة خاصة.

. **عرقلة العدالة** Obstruction of Justice

فرضت محكمة المقاطعة تعديلا تصاعديا من مستويين لعرقلة العدالة بموجب المادة C1,1 من تقنين التنفيذ للولايات المتحدة. ووجدت المحكمة أن Petersen هرب أثناء الإفراج عنه بكفالة، وكان يعلم أنه كان من المفترض أن يعود للحكم، وفشل عمدا في العودة، وبالتالي تم تأخير إصدار الحكم. واستنادا إلى هذه النتائج، قررت المحكمة أن Petersen عرقل العدالة. حيث ينص القسم 3C1,1 على زيادة من مستويين في مستوى الجريمة المطبق "إذا عرقل المتهم عمدا أو أعاق أو حاول عرقلة أو إعاقة إقامة العدل أثناء التحقيق أو المقاضاة أو الحكم على الجريمة الفورية." ومن الأمثلة على نوع السلوك الذي ينطبق عليه التعزيز "الهروب أو محاولة الهروب من الاحتجاز قبل المحاكمة أو إصدار الحكم؛ والهروب من الاحتجاز قبل المحاكمة أو إصدار الحكم؛ والهروب من

الاحتجاز قبل المحاكمة أو عدم المثول عمدا، على النحو الذي أمر به، لاتخاذ إجراء قضائي". أحد الأمثلة على نوع السلوك الذي لا يبرر تطبيق التعزيز هو "تجنب الاعتقال أو الهروب منه avoiding or fleeing from arrest".

في جلسة استماع عقدت في 18 أكتوبر 1993، واصلت محكمة المقاطعة الحكم على Petersen حتى 24 يناير 1994. وعندما استفسرت المحكمة المحلية عن ذلك، ذكر محامي Petersen أن موكله وافق على (وبالتالي كان على علم) بالاستمرارية. ومع ذلك، فشل Petersen في حضور جلسة النطق بالحكم في 24 يناير 1994. ومثل محامي الولايات المتحدة أن Petersen كان على اتصال به وعرف أنه يجب أن يمثل. وفي ظل هذه الظروف، خلصت محكمة المقاطعة على نحو سليم إلى أن Petersen "لم يحضر عمدا، كما أمر، لإجراء قضائي" بالمعنى المقصود في الفقرة 3C1,1.

كما أن فرار بيترسن Petersen's absconding أثناء الإفراج عنه بكفالة بعد إدانته conviction وقبل الحكم عليه يدعم أيضا عرقلة تعزيز العدالة. وفي حين أن مجرد الهروب أثناء التحقيق في جريمة ما لا يبرر التعزيز، فقد أيدت هذه المحكمة التعزيز حيث تم بالفعل اعتقال المتهم بسبب الجريمة، وقيل له إنه مشتبه به في قضية جنائية، و"كان يعلم أنه كان من المتوقع أن يسلم نفسه طواعية".

ولم يكن Petersen قد اعتقل فحسب، بل أدين أيضا في الوقت الذي فر فيه. ففي قضية سابقة قررت المحكمة (التي ترى أن هروب المتهمة أثناء وجودها بكفالة بعد إدانتها وقبل الحكم عليها كان سببا كافيا للاستنتاج بأنها عرقلت العدالة). وطوال الأشهر العشرة التي كان فيها Petersen هاربا، كان على اتصال بضباط إنفاذ القانون الذين أبلغوه بأن مذكرة توقيف صدرت بحقه.

وخلصت محكمة المقاطعة بشكل صحيح إلى أن هروب Petersen بين الإدانة والحكم وعدم المثول أمام جلسة استماع مقررة للحكم يبرر إجراء تعديل تصاعدي على مستويين لعرقلة سير العدالة.

محاولة/ تخفيض التآمر Attempt/Conspiracy Reduction

يطعن Petersen في رفض محكمة المقاطعة خفض مستوى جريمته وفقا للمادة 2X1,1 من تقنين الولايات المتحدة U.S.S.G. § 2X1,1.. وفي القضية رقم CR 95-00214، أقر بيترسن بأنه مذنب بالتآمر لارتكاب احتيال حاسوبي وسلكي فيما يتعلق بمخطط لتحويل الأموال من Heller Financial إلى مؤسسة مالية أخرى. ويدعي أن تنفيذ مخطط الاحتيال defraud على Heller Financial لم يكن سوى solely محاولة أو مؤامرة، مما منحه تخوله تخفيضا reduction بمقدار ثلاث نقاط في مستوى جريمته بموجب المادة 2X1,1. وخلصت المحكمة الجزئية إلى أن "هذه قضية اكتملت فيها الجريمة بشكل كبير". ووجدت المحكمة أن "كل شيء قد تم" وأن استلام بيترسن للأموال المحولة من هيلر "قد تم أعاقته من قبل طرف ثالث". وبناء على ذلك، رفضت المحكمة تخفيض مستوى الجريمة the court declined to reduce the offense level.

وتنص المادة 2X1,1(b)، في الجزء ذي الصلة، على ما يلي: إذا كانت هناك محاولة [أو مؤامرة]، تنخفض بمقدار ثلاثة مستويات، ما لم يكمل المتهم جميع الأعمال التي يعتقد أنها ضرورية لإستكمال الجريمة الموضوعية substantive offense بنجاح أو تثبت الظروف أن المتهم [أو المتآمرين] كان على وشك إكمال جميع هذه الأعمال لولا القبض عليه أو انقطاعه من قبل حدث مماثل خارج عن سيطرة المدعى عليه [أو المتآمرين].

وتنص مذكرة المعلومات الأساسية للفقرة Background Note to § 2X1,1 **على ما يلي:**

وفي معظم الاتهامات القضائية المتعلقة بالمؤامرات أو المحاولات، تكون الجريمة الموضوعية substantive offense قد اكتملت إلى حد كبير أو توقفت أو منعت على وشك الانتهاء بشفاعة سلطات إنفاذ القانون أو الضحية victim. في مثل هذه الحالات، لا يوجد ما يبرر تخفيض مستوى الجريمة. ومع ذلك، في بعض الأحيان، يحدث الاعتقال قبل وقت طويل من إكمال المتهم أو أي متآمر مشارك له الأفعال اللازمة للجريمة الموضوعية. وفي ظل هذه الظروف، ينص على تخفيض قدره 3 مستويات بموجب الفقرة 2X1,1(b)(1) أو (2).

قام Petersen بالتنصت على خط هاتف Telenet وحصل على كلمات المرور اللازمة لتنفيذ التحويل المصرفي. ثم نفذ تحويلا مصرفيا بقيمة 150,000 دولار من Heller Financial إلى بنك الاتحاد. وتم الكشف عن المخطط من قبل Heller Financial في اليوم التالي. أبلغ هيلر بنك الاتحاد وتمكن من الاستيلاء على مبلغ 150000 دولار قبل أن يتمكن Petersen أو شركاءه coconspirators من سحبه withdrawn.

ونظرا لأن Petersen كان قد نفذ بالفعل التحويل البنكي الاحتيالي fraudulent wire transfer، فإننا نتفق مع محكمة المقاطعة على أن "الجريمة الموضوعية قد اكتملت بشكل كبير the substantive offense was substantially completed." U.S.S.G. § 2X1,1 تعليق. (backgr'd). وبقدر ما كان لا يزال يتعين القيام بخطوات، فإن الاحتيال "توقف أو منع على وشك الانتهاء بشفاعة intercession... الضحية" وهي Heller Financial. وبناء على ذلك، رفضت محكمة المقاطعة على نحو دقيق تخفيض مستوى الجريمة. (لم يكن يحق للمتهم الحصول على تخفيض بموجب المادة 2X1,1 حيث "كان لديه أجهزة وصول غير مصرح بها وكان على وشك استخدامها لتوجيه التهم والحصول على المال... هناك أمران فقط أوقفاه: اعتقاله، وحقيقة أن المحطات الطرفية لم تكن متصلة بأحد البنوك").

D. الاستعادة/ الرد/ الاسترداد Restitution

وكجزء من الحكم الصادر بحق Petersen، فرضت محكمة المقاطعة تعويضا بموجب قانون حماية الضحايا والشهود the Victim and Witness Protection Act, 18 U.S.C. § 3663، بمبلغ 40,000

دولار لبعض الكيانات والأشخاص المتضررين. في وقت إصدار الحكم، لم يكن لدى Petersen أي أصول أو دخل وكان لديه ديون غير مضمونة بقيمة 19,100 دولار. ومع ذلك، وجدت محكمة المقاطعة أن Petersen كان يتمتع بمهارات كمبيوتر قوية، وكان "واضحا articulate... طماع gutsy وذكي smart وواسع الحيلة resourceful ومبدع creative" و "ربما يمكن أن يكون شخصا ناجحا pretty successful ومنتجا جدا productive person" في المستقبل. Petersen شاب وقد أظهر قدرة على كسب المال في الماضي كمروج للحفلات الموسيقية concert promoter ومهندس صوت sound engineer ويعمل في شركة تحقيق خاصة private investigation company.

وبناء على إلحاح Petersen، سمحت محكمة المقاطعة له بالحصول على وظيفة مستقبلية تتعلق باستخدام أجهزة الحاسوب، شريطة أن يحصل على إذن من ضابط المراقبة probation officer الخاص به. وأشار بيترسن إلى أنه يعتقد أنه يستطيع البحث عن عمل كمستشار لأمن الحاسوب. ويجوز للمحكمة المحلية أن تأمر المتهم المعوز بدفع التعويض شريطة أن تكون هناك أدلة كافية في السجل تثبت أنه ستكون لديه قدرة مستقبلية على الرد restitution.

وعلى الرغم من أن Petersen قد يواجه بعض الصعوبات في الحصول على عمل بسبب إدانته بجناية، إلا أن هناك بالتأكيد احتمالا معقولا بأنه سيكون قادرا على دفع تعويض pay restitution بمبلغ 40000 دولار. انظر Ramilo, 986 F.2d at 337 (إلغاء فرض الرد بمبلغ 454,841,97 دولار، المستحق بعد ثلاث سنوات من انهاء المتهم لعقوبة السجن، لأنه لا توجد إمكانية واقعية لأن يدفع المتهم مثل هذا المبلغ). ونظرا لوجود "بعض الأدلة، فانه قد يكون المتهم قادرا على دفع المبلغ المحدد عند الحاجة إلى القيام بذلك" لم تسيء محكمة المقاطعة استخدام سلطتها التقديرية abuse its discretion في إقرار الرد ش

ومع ذلك، يؤكد Petersen أنه كجزء من اتفاقات الإقرار بالذنب plea agreements التي أبرمها، كان مطلوبا منه التنازل عن أرباحه المستقبلية للحكومة، مما قوض قدرته على دفع التعويضات. لا نرى شيئا في اتفاق الإقرار بالذنب يشير إلى أن Petersen وافق على تسليم دخله المستقبلي للحكومة. بل على العكس من ذلك، ينص اتفاق الإقرار بالذنب على أنه "عند التوقيع على هذه الاتفاقية، فإنك توافق [بيترسن] على دفع تعويض عن الخسارة الكاملة الناجمة عن أنشطتك، بمبلغ تحدده المحكمة وقت إصدار الحكم".

وأخيرا، يدعي Petersen أنه لا ينبغي أن يضطر إلى دفع 10000 دولار لمحطة إذاعة KPWR-FM كجزء من أمر الاسترداد. ويدعي أنه نظرا لأن المحطة الإذاعية كانت ستدفع لبعض المتصلين الآخرين 10000 دولار كجائزة لو لم يتلاعب بالنظام rigged the system، فإن المحطة لم تتكبد أية خسارة suffered no loss. ولأن الفائز البديل غير معروف، فلا يوجد أحد يدفع له التعويض. ترد النيابة العامة بشكل غير صحيح بأن Petersen فشل في إثارة هذه المسألة أدناه. أثار Petersen

هذه المسألة في مذكرة الحكم التي أصدرها لمحكمة المقاطعة. ومع ذلك، فإن الحجة لا أساس لها من الصحة. ولا يعفى المتهم من إعادة "جائزة" تم الحصول عليها عن طريق الاحتيال من محطة إذاعية لأن شخصا آخر كان سيحصل على الجائزة. لا تزال المحطة الإذاعية تعاني من خسارة من خلال دفع 10000 دولار تحت ذرائع كاذبة. "الرد الجنائي Criminal restitution هو وسيلة لتحقيق الأهداف الجزائية penal objectives مثل الردع deterrence أو إعادة التأهيل rehabilitation أو القصاص retribution " وكذلك التعويض compensation.

نخلص إلى أن محكمة المقاطعة لم تخطئ في فرض تعديلات تصاعدية upward adjustments لاستخدام مهارة خاصة بموجب الفقرة § 3B1,3 وعرقلة العدالة obstruction of justice بموجب المادة § 3C1,1، في رفض خفض مستوى الجريمة بموجب الفقرة § 2X1,1 للمحاولة / التآمر attempt/conspiracy، أو في الأمر بالرد ordering restitution.

تم التأكيد

AFFIRMED.

-

العدوان على الملكية الفكرية تحقير للبحث العلمي

مبدأ في القضاء الأمريكي

قضية منصة التواصل الاجتماعي

تيك توك TIKTOK

بشأن طلبات إصدار أمر قضائي / زجري في انتظار المراجعة
أمام محكمة الاستئناف الأمريكية لدائرة مقاطعة كولومبيا
17 يناير 2025

المحكمة العليا للولايات المتحدة

قضية تيك توك
بشأن طلبات إصدار أمر قضائي / زجري في انتظار المراجعة
أمام محكمة الاستئناف الأمريكية لدائرة مقاطعة كولومبيا
17 يناير 2025

SUPREME COURT OF THE UNITED STATES

Nos. 656–24 and 657–24

TIKTOK INC., ET AL., PETITIONERS 656–24 v. MERRICK B. GARLAND, ATTORNEY GENERAL

BRIAN FIREBAUGH, ET AL., PETITIONERS 657–24 v. MERRICK B. GARLAND, ATTORNEY GENERAL

ON APPLICATIONS FOR INJUNCTION PENDING REVIEW TO THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

[January 2025 ,17]

المحكمة PER CURIAM.

اعتبارا من 19 يناير، سيجعل قانون حماية الأمريكيين من التطبيقات الخاضعة للرقابة الأجنبية Foreign Adversary Controlled Applications Act من غير القانوني للشركات في الولايات المتحدة تقديم خدمات لتوزيع أو صيانة أو تحديث منصة التواصل الاجتماعي TikTok، ما لم يتم فصل تشغيل المنصة في اللايات المتحدة عن السيطرة الصينية. الملتمسون Petitioners هم كيانان تشغيليان لـ.. TikTok ومجموعة من مستخدمي TikTok في الولايات المتحدة. ونحن نعتبر ما إذا كان القانون، كما هو مطبق على الملتمسين، ينتهك التعديل الأول First Amendment.

ومن خلال القيام بذلك، ندرك أن القضايا المعروضة علينا تتضمن تقنيات جديدة ذات قدرات تحويلية transformative capabilities. هذا السياق الجديد الصعب ينصح بالحذر من جانبنا. كما نصح القاضي فرانكفورتر Justice Frankfurter قبل 80 عاما عند النظر في تطبيق القواعد القانونية المعمول بها على «المشاكل الجديدة تماما totally new problems» التي أثارتها الطائرة والراديو، يجب أن نحرص على عدم «إحراج المستقبل embarrass the future». حيث يتم زيادة هذا الحذر في هذه الحالات، بالنظر إلى الوقت المعجل المسموح به للنظر فيه. ويجب فهم تحليلنا على أنه مركز بشكل ضيق narrowly focused في ضوء هذه الظروف.

تيك توك TikTok عبارة عن منصة تواصل اجتماعي social media platform تتيح للمستخدمين إنشاء مقاطع فيديو قصيرة متراكبة بالصوت والنص ونشرها وعرضها ومشاركتها والتفاعل معها. ومنذ إطلاقها في عام 2017، جمعت المنصة أكثر من 170 مليون مستخدم في الولايات المتحدة وأكثر من مليار مستخدم في جميع أنحاء العالم. هؤلاء المستخدمون هم منشئو محتوى prolific content creators ومشاهدون viewers غزير الإنتاج. وفي عام 2023، قام مستخدمو TikTok الأمريكيون بتحميل أكثر من 5,5 مليار مقطع فيديو، والتي تمت مشاهدتها بدورها أكثر من 13 تريليون مرة حول العالم.

حيث يؤدي فتح تطبيق TikTok إلى جلب المستخدم إلى صفحة «من أجلك For You» - موجز محتوى مخصص مصمم خصيصا لاهتمامات المستخدم. يقوم TikTok بإنشاء الخلاصة باستخدام خوارزمية algorithm خاصة توصي بمقاطع الفيديو للمستخدم بناء على تفاعلات المستخدم مع النظام الأساسي. كل تفاعل يجريه المستخدم على TikTok - مشاهدة مقطع فيديو، ومتابعة حساب، وترك تعليق- يمكن نظام التوصية من تخصيص موجز محتوى مخصص بشكل أكبر.

هذا، ويتم تشكيل موجز محتوى مستخدم TikTok أيضا من خلال قرارات الإشراف على المحتوى والتصفية. يستخدم TikTok معالجات آلية وبشرية automated and human processes لإزالة المحتوى الذي ينتهك إرشادات مجتمع المنصة. حيث يروج Tik-Tok أيضا لمحتوى معين أو يخفضه من رتبته لتعزيز أهداف أعماله وأهدافه الأخرى.

هذا، ويتم تشغيل TikTok في الولايات المتحدة بواسطة شركة TikTok Inc. وهي شركة أمريكية incorporated تأسست ومقرها في كاليفورنيا. الشركة الأم النهائية لشركة TikTok Inc. هي

ByteDance Ltd. وهي شركة مملوكة للقطاع الخاص لديها عمليات في الصين. تمتلك ByteDance Ltd. خوارزمية TikTok المملوكة، والتي تم تطويرها وصيانتها في الصين، كما أن الشركة مسؤولة أيضا عن تطوير أجزاء من كود المصدر source code الذي يدير منصة TikTok. تخضع شركة ByteDance Ltd. للقوانين الصينية التي تتطلب منها «المساعدة أو التعاون assist or cooperate» مع «العمل الاستخباراتي intelligence work» للحكومة الصينية وضمان أن الحكومة الصينية لديها «سلطة الوصول إلى البيانات الخاصة والتحكم فيها» التي تحتفظ بها الشركة.

في السنوات الأخيرة، اتخذ مسؤولو الحكومة الأمريكية إجراءات متكررة لمعالجة هواجس الأمن القومي national security concerns التي تعيد تعزيز العلاقة بين الصين وتيك توك.

وفي أغسطس 2020، أصدر الرئيس ترامب أمرا تنفيذيا تقرر فيه أن «انتشار التطبيقات المتنقلة في الولايات المتحدة التي طورتها وتملكها شركات في [الصين] لا يزال يهدد الأمن القومي والسياسة الخارجية والاقتصاد للولايات المتحدة.». حيث قرر الرئيس ترامب أن TikTok أثارة مخاوف خاصة، مشيرا إلى أن المنصة «تلتقط تلقائيا مساحات شاسعة من المعلومات من مستخدميها» وهي عرضة للاستخدام لتعزيز مصالح الحكومة الصينية. ولقد استند الرئيس إلى سلطته بموجب قانون الصلاحيات الاقتصادية الدولية في حالات الطوارئ (IEEPA)، 50 U. S. C. §1701 وما يليها، وقانون الطوارئ الوطنية، 50 U. S. C. §1601 وما يليها، لحظر بعض «المعاملات transactions» التي تشمل Byte Dance Ltd. أو الشركات التابعة لها، على النحو الذي حددته وزارة التجارة. حيث نشر الوزير قائمة بالمعاملات المحظورة list of prohibited transactions في سبتمبر 2020. ولكن المحاكم الفيدرالية فرضت الحظر قبل أن تدخل حيز التنفيذ the pro-hibitions before they took effect، ووجدت أنها تجاوزت سلطة السلطة التنفيذية بموجب IEEPA.

وبعد أيام فقط من إصدار أمره التنفيذي الأولي initial Executive Order، أمر الرئيس ترامب Pres¬ident Trump شركة ByteDance Ltd. بتصفية جميع المصالح والحقوق في أية ممتلكات «تستخدم لتمكين أو دعم تشغيل ByteDance لتطبيق TikTok في الولايات المتحدة»، إلى جانب «أي بيانات تم الحصول عليها أو مشتقة من» مستخدمي TikTok في الولايات المتحدة ورفعت شركة TikTok دعوى قضائية في دائرة العاصمة، وأعلنت دستورية الأمر. في فبراير 2021، حيث جعلت دائرة العاصمة القضية معلقة للسماح لإدارة بايدن Biden administration بمراجعة المسألة وتمكين الأطراف من التفاوض على علاج عدم تصفية الاستثمارات من شأنه أن يعالج أوضاع الأمن القومي للحكومة.

وطوال عامي 2021 و2022، تفاوضت شركة Byte Dance Ltd. مع مسؤولي الفرع التنفيذي لتطوير اتفاقية أمان وطنية national secu¬rity agreement من شأنها حل هذه المخاوف. ومع ذلك، قرر مسؤولو الفرع التنفيذي في النهاية أن الاتفاقية المقترحة لشركة Byte Dance Ltd. لم تخفف بشكل كاف من المخاطر التي تشكلها الأمن القومي للولايات المتحدة. 2 التطبيق 686. حيث توقفت

المفاوضات، ولم يتوصل الطرفان إلى الاتفاق أبدا.

وعلى هذه الخلفية، سن الكونجرس قانون حماية الأمريكيين من التطبيقات التي يسيطر عليها الخصوم الأجانب. حيث يحظر القانون على أي كيان تقديم خدمات معينة «لتوزيع أو صيانة أو تحديث» «تطبيق خصم أجنبي foreign adversary con-trolled application» في الولايات المتحدة. حيث تخضع الكيانات التي تنتهك هذا الحظر لإجراءات إنفاذ مدنية civil enforcement actions وعقوبات مالية باهظة hefty monetary penalties.

حيث ينص القانون على وسيلتين يمكن من خلالهما تعيين الطلب على أنه «تطبيق خاضع لسيطرة الخصم الأجنبي». أولا، ومن ثم يحدد القانون صراحة أي تطبيق «يتم تشغيله، بشكل مباشر أو غير مباشر»، من قبل «ByteDance Ltd.» أو «TikTok» أو أية شركة تابعة أو خلف لها.

ثانيا، يضع القانون إطارا عاما للتعيين لأي تطبيق:

(1) تديره «شركة مشمولة» «يسيطر عليها خصم أجنبي»،

(2) يحدده الرئيس ليمثل تهديدا كبيرا للأمن القومي للولايات المتحدة ،

وبعد عملية الإخطار العام والإبلاغ. بعبارات عامة، يعرف القانون «الشركة المشمولة covered com¬pany» لتشمل الشركة التي تدير تطبيقا يمكن المستخدمين من إنشاء المحتوى ومشاركته وعرضه ولديه أكثر من 1,000,000 مستخدم نشط شهريا.

ويستثني القانون من هذا التعريف الشركة التي تدير تطبيقا «هدفه الأساسي هو السماح لنا بنشر مراجعات المنتجات أو مراجعات الأعمال أو معلومات السفر والمراجعات».

وتدخل محظورات القانون حيز التنفيذ بعد 270 يوما من تصنيف الطلب على أنه تطبيق خاضع لسيطرة الخصم الأجنبي. نظرا لأن القانون نفسه يحدد التطبيقات التي تديرها «ByteDance، Ltd.» و«TikTok»، فإن المحظورات المتعلقة بهذه التطبيقات تدخل حيز التنفيذ بعد 270 يوما من سن القانون - 19 يناير 2025.

هذا، ويعفي القانون التطبيق الذي يتحكم فيه الخصم الأجنبي من المحظورات إذا خضع الطلب لـ.. «التجريد المؤهل qualified divestiture» وهو الذي يقرر الرئيس أنه سيؤدي إلى عدم سيطرة الخصم الأجنبي على الطلب «بعد الآن». أيضا يجب على الرئيس أن يقرر أن تصفية الاستثمارات «تمنع إنشاء أو الحفاظ على أية علاقة تشغيلية بين عمليات الولايات المتحدة لـ.. [التطبيق] وأية دول تابعة سابقا يسيطر عليها خصم أجنبي، بما في ذلك أي تعاون فيما يتعلق بتشغيل خوارزمية توصية المحتوى أو اتفاقية فيما يتعلق بمشاركة البيانات.». ويسمح القانون للرئيس بمنح تمديد لمرة واحدة لمدة لا تزيد عن 90 يوما فيما يتعلق بتاريخ سريان المحظورات البالغ 270 يوما إذا قدم الرئيس شهادات معينة للكونغرس فيما يتعلق بالتقدم نحو تصفية مؤهلة.

ولقد قدمت شركة ByteDance Ltd. وTikTok Inc. - جنبا إلى جنب مع مجموعتين من مستخدمي TikTok والمبدعين creators (مقدمي الالتماسات creator petitioners) - دعاوى

صغيرة للمراجعة في دائرة العاصمة، متحدية الاساس الدستوري للقانون. كما هو ملائم هنا، وجادل الملتمسون بأن المحظورات التي يفرضها القانون، وتعيين التطبيق الذي يتحكم فيه الخصم الأجنبي الخاص بـ.. TikTok، ومتطلبات البحث تنتهك التعديل الأول، ودرست دائرة العاصمة العرائض ورفضتها، معتبرة أن القانون لا ينتهك حقوق التعديل الأول لمقدمي العرائض. وبعد أن خلصت المحكمة لأول مرة إلى أن القانون يخضع لتدقيق مشدد بموجب التعديل الأول، افترضت المحكمة دون أن تقرر أن التدقيق الصارم، وليس التدقيق الداخلي مطبقinterme¬diate scrutiny applied.

حيث رأت المحكمة أن القانون يفي بهذا المعيار، ووجدت أن مبررات الأمن القومي للحكومة - مواجهة جهود جمع البيانات ومعالجة المحتوى السري في الصين- كانت مقنعة compelling، وأن القانون مصمم بشكل ضيق لتعزيز تلك المصالح. ولقد وافق رئيس القضاة سرينيفاسان Chief Judge Srinivasan جزئيا على ما في الحكم حيث كان القانون خاضعا للتدقيق الوسيط inter¬mediate scrutiny، وكان دستوريا constitutional بموجب هذا المعيار، لقد منحنا اذنا مبدئيا certiorari لتقرير ما إذا كان القانون، كما هو مطبق على مقدمي العرائض، ينتهك التعديل الأول.

ومن البداية، ننظر فيما إذا كانت الأحكام المطعون فيها تخضع لتدقيق التعديل الأول. حيث يمكن للقوانين التي تنظم السلوك التعبيري expressive conduct بشكل مباشر، ولكن ليس بالضرورة، أن تؤدي إلى مثل هذه المراجعة. ولقد طبقنا أيضا تدقيق التعديل الأول في «الحالات التي تنطوي على تنظيم حكومي للسلوك الذي يحتوي على عنصر تعبيري»، وعلى «بعض القوانين التي، على الرغم من أنها موجهة إلى النشاط ذي المكون غير التعبيري، تفرض عبئا غير متناسب على أولئك الذين **يشاركون في أنشطة التعديل الأول المحمية**».

ليس من الواضح ما إذا كان القانون نفسه ينظم بشكل مباشر النشاط التعبيري المحمي، أو السلوك الذي يحتوي على مكون تعبيري. وفي الواقع، لا ينظم القانون المبدعين على الإطلاق. حيث انه ينظم بشكل مباشر ByteDance Ltd. و TikTok Inc. فقط من خلال متطلبات التجريد. ولم يحدد الملتمسون، من جانبهم، أية قضية تعاملت فيها هذه المحكمة مع لائحة مراقبة الشركات على أنها تنظيم مباشر للنشاط التعبيري أو السلوك شبه التعبيري. ونحن نتردد في فتح هذا الطريق الجديد في هذه القضية الفريدة.

وعلى أي حال، فإن حجج الملتمسين petitioners' arguments تقترب بشكل وثيق من الادعاء بأن المحظورات التي يفرضها القانون، والتعيين الخاص specific designation بـ.. TikTok، ومتطلبات التجريد «تفرض عبئا غير مؤيد على» أنشطة التعديل الأول الخاصة بهم. ويؤكد مقدمو الالتماسات - ولا تعترض الحكومة - أنه نظرا لأنه من غير المجدي تجاريا تصفية TikTok خلال الإطار الزمني البالغ 270 يوما للقانون، فإن القانون يحظر TikTok فعليا في الولايات المتحدة. حيث يجادل مقدمو العرائض بأن مثل هذا الحظر سيثقل كاهل أنشطة التعديل الأول المختلفة، بما في ذلك الإشراف على المحتوى، وإنشاء المحتوى، والوصول إلى وسيط متميز للضغط، والارتباط بمتحدث آخر أو محرر ed¬itor مفضل، وتلقي المعلومات والأفكار.

لقد اعترفنا بعدد من هذه المصالح المؤكدة في التعديل الأول. ومن المؤكد أن الحظر الفعلي على منصة وسائط اجتماعية تضم 170 مليون مستخدم أمريكي يثقل كاهل النشاط التعبيري لهؤلاء المستخدمين بطريقة غير بسيطة non-trivial way.

في الوقت نفسه، فإن القانون الذي يستهدف سيطرة خصم أجنبي على منصة اتصالات يختلف من نواح كثيرة من نوعه عن لوائح الفعل غير التعبيري التي أخضعناها لتدقيق التعديل الأول. قد تؤثر هذه الاختلافات - تركيز القانون على حكومة أجنبية، وعلاقة العداء التي حددها الكونجرس بين تلك الحكومة الأجنبية والولايات المتحدة، والخطوات السببية بين اللوائح والعبء المزعوم على الكلام المحمي- على ما إذا كان التدقيق في التعديل الأول ينطبق.

لم تحدد هذه المحكمة إطارا واضحا لإزالة ما إذا كان تنظيم النشاط غير التعبيري الذي يثقل كاهل المشاركين في النشاط التجريبي بشكل غير متناسب يؤدي إلى مراجعة متزايدة. ولسنا بحاجة إلى القيام بذلك هنا. اذ نفترض دون أن نقرر أن الرؤى المؤيدة المطعون فيها تندرج ضمن هذه الفئة وتخضع لتدقيق التعديل الأول.

«في قلب التعديل الأول يكمن المبدأ القائل بأن كل شخص يجب أن يقرر بنفسه الأفكار والمعتقدات التي تستحق التعبير والنظر والالتزام.». والإجراء الحكومي الذي يقمع التعبير بسبب رسالته «يتعارض مع هذا الحق الأساسي». و«القوانين القائمة على المحتوى – تلك التي تستهدف الكلام بناء على محتواه التواصلي – يفترض أنها غير دستورية ولا يمكن تبريرها إلا إذا أثبتت الحكومة أنها مصممة بشكل ضيق لخدمة مصالح الدولة الملحة». والقوانين المحايدة للمحتوى، وفي الواقع، «تخضع لمستوى متوسط من التدقيق لأنها في معظم الحالات تشكل خطرا أقل جوهرية لاستبعاد أفكار أو وجهات نظر معينة من الحوار العام». وبموجب هذا المعيار، سنحافظ على قانون محايد للمحتوى «إذا كان يدعم مصالح حكومية مهمة لا علاقة لها بقمع حرية التعبير ولا يثقل كاهل الكلام أكثر من اللازم لتعزيز تلك المشاركات».

ولقد حددنا شكلين من أشكال تنظيم الكلام المستند إلى المحتوى:

أولا، القانون هو المحتوى القائم على وجهه إذا كان «يتوافق مع خطاب معين بسبب الموضوع الذي تمت مناقشته أو الفكرة أو الرسالة المعبر عنها».

ثانيا، ومع ذلك، يتم التعامل مع القانون المحايد ظاهريا للمحتوى على أنه تنظيم للكلام القائم على المحتوى إذا كان «لا يمكن تبريره» دون الرجوع إلى محتوى الخطاب المنظم» أو «تم تبنيه من قبل الحكومة» بسبب عدم الموافقة على الرسالة التي ينقلها الخطاب». كما هو مطبق على الملتمسين، فإن الأحكام المطعون فيها محايدة من حيث المحتوى ويتم تبريرها بأساس منطقي محايد للمحتوى.

ان الأحكام المطعون فيها محايدة من حيث المحتوى. حيث إنهم يفرضون حضورا خاص بـ.. TikTok بسبب سيطرة خصم أجنبي على المنصة ويجعلون التجريد شرطا أساسيا لاستمرار تشغيل المنصة في الولايات المتحدة. حيث إنهم لا يستهدفون خطابا معينا بناء على محتواه، أو تنظيم أساس الكلام على وظيفته أو غرضه، على النقيض من ذلك.

ويجادل الملتمسون بأن القانون يستند إلى محتواه لأنه يستبعد من تعريف «الشركة المغطاة covered com¬pany» أي شركة تدير تطبيقا «هدفه الأساسي هو السماح للمستخدمين بنشر مراجعات المنتجات أو مراجعات الأعمال أو معلومات السفر والمراجعات». ولسنا بحاجة إلى أن نقرر ما إذا كان هذا الاستبعاد قائما على المحتوى. السؤال المطروح أمام المحكمة هو ما إذا كان القانون ينتهك التعديل الأول كما هو مطبق على الملتمسين. للإجابة على هذا السؤال، ننظر إلى أحكام القانون التي تؤدي إلى حظر TikTok الفعلي الذي يجادل الملتمسون بأنه يثقل كاهل حقوقهم في التعديل الأول. ومع ذلك، فإن الاستبعاد لبعض نماذج المراجعة ينطبق فقط على الإطار العام لتعيين التطبيقات التي تسيطر عليها «الشركات المغطاة»، وليس على التعيين الخاص بـ TikTok. وعلى هذا النحو، فإن الاستبعاد exclusion لا يقع في نطاق الطعن المطبق الذي قدمه الملتمسون.

تدعم الحكومة أيضا الأحكام المطعون فيها بمبرر محايد للمحتوى: منع الصين من جمع كميات هائلة من البيانات الحساسة من 170 مليون مستخدم أمريكي. وهذا الأساس المنطقي هو بالتأكيد لا أدري للرضا agnostic. إنه لا يشير إلى محتوى الكلام على TikTok ولا يعكس الخلاف مع الرسالة التي ينقلها هذا الكلام. نظرا لأن تبرير جمع البيانات يعكس «غرضا لا علاقة له بمحتوى التعبير»، فهو محايد المحتوى.

علاوة على ذلك، فإن الفروق الخاصة ب TikTok في القانون لا تؤدي إلى تدقيق صارم. ولهذا السبب، «غالبا ما تمثل التعديلات التي تميز بين وسائل الإعلام، أو بين المتحدثين المختلفين ضمن وسيط واحد، مخاوف خطيرة بشأن التعديل الأول». ولكن في حين أن «القوانين التي تفضل بعض المتحدثين على الآخرين تتطلب تدقيقا صارما عندما يعكس تفضيل المتحدث للهيئة التشريعية تفضيلا للمحتوى» فإن مثل هذا التدقيق «غير مبرر عندما تكون المعاملة التفاضلية «مبررة من خلال بعض الخصائص الخاصة ل « المتحدث المعين الذي يتم تنظيمه.

للأسباب التي أوضحناها، فإن طلب التجريد بغرض منع خصم أجنبي من التنازل عن البيانات الحساسة لـ.. 170 مليون مستخدم أمريكي TikTok ليس «وسيلة خفية لممارسة تفضيل المحتوى». وتنظم المحظورات والتعيين الخاص بـ.. TikTok ومتطلبات التجريد TikTok بناء على اهتمام جمع البيانات المحايدة بالمحتوى. ويتمتع TikTok بخصائص خاصة - قدرة الخصم الأجنبي على الاستفادة من سيطرته على المنصة لجمع كميات هائلة من البيانات الشخصية من 170 مليون مستخدم أمريكي- تبرر هذه المعاملة التفاضلية. حيث «لا يفترض أن الفروق القصوى من هذا النوع غير صالحة بموجب التعديل الأول.».

بينما نجد أن المعاملة التفاضلية differential treatment كانت مبررة هنا، فإننا نؤكد على الضيق المتأصل في حيازتنا. يعد جمع البيانات وتحليلها ممارسة شائعة في هذا العصر الرقمي digital age. لوكن حجم TikTok وقابليته للسيطرة على الخصم من الأجانب، جنبا إلى جنب مع المساحات الشاسعة من البيانات الحساسة التي تجمعها المنصة، تبرر المعاملة المختلفة لمعالجة مخاوف الحكومة الوطنية. إن القانون الذي يستهدف أي متحدث آخر يستلزم بالضرورة تحقيقا

متميزا وجلسات منفصلة. وعلى هذا الفهم، لا يمكننا قبول دعوة الملتمسين للتدقيق الصارم. ليس أكثر من التدقيق الوسيط في محله.

وكما ينطبق القانون على مقدمي العرائض، فإنه يفي بالتدقيق الوسيط scrutiny intermediate. وتعزز الأحكام المطعون فيها مصلحة حكومية هامة لا علاقة لها بقمع حرية التعبير، ولا تثقل كاهلا أكثر بكثير مما هو ضروري لتعزيز هذه المصلحة.

فقد تم تصميم المحظورات ومتطلبات التجريد في القانون لمنع الصين - وهي مدفع أجنبي معين - من الاستفادة من سيطرتها على ByteDance Ltd. لالتقاط البيانات الشخصية لمستخدمي TikTok في الولايات المتحدة. هذا الدليل مؤهل كمصلحة حكومية مهمة في التدقيق الوسيط. ولا يجادل مقدمو العرائض في أن الحكومة لديها مصلحة مهمة وراسخة في منع الصين من جمع البيانات الشخصية لعشرات الملايين من مستخدمي TikTok الأمريكيين. ولا يمكنهم ذلك. اذ تجمع المنصة معلومات شخصية exten¬sive personal information موسعة من مستخدميها وعنهم.

وعلى سبيل المثال، إذا سمح المستخدم لـ.. TikTok بالوصول إلى قائمة جهات اتصال هاتف المستخدم للتواصل مع الآخرين على المنصة، فيمكن لـ.. TikTok الوصول إلى «أي بيانات مخزنة في قائمة جهات اتصال المستخدم»، بما في ذلك الأسماء ومعلومات الاتصال وصور جهات الاتصال والمسميات الوظيفية والملاحظات.

وتخشى الحكومة أن الوصول إلى مثل هذه المعلومات التفصيلية حول المستخدمين الأمريكيين قد يمكن «الصين من تتبع مواقع الموظفين والمقاولين الفيدراليين، وإنشاء ملفات للمعلومات الشخصية للابتزاز، وإجراء تجسس الشركات». ويتيح القانون الصيني للصين مطالبة الشركات بتسليم البيانات إلى الحكومة» مما يجعل الشركات التي تتخذ من ذلك مقرا لها أداة تجسس» للصين.

وبدلا من الاعتراض بشكل هادف على نطاق البيانات التي يجمعها TikTok أو الغايات التي يمكن استخدامها من أجلها، يعارض المبتدئون الاحتمالية، مؤكدين أنه «من غير المحتمل» أن الصين «تجبر TikTok على تسليم بيانات المستخدم لأغراض جمع المعلومات الاستخباراتية، نظرا لأن الصين لديها وسائل أكثر فعالية وكفاءة للحصول على المعلومات ذات الصلة». وعند مراجعة دستورية القانون، على أي حال، «يجب أن نعطي احتراما كبيرا لأحكام الكونجرس المتوقعة». و»غالبا ما يطلب صنع السياسات السليمة من المشرعين التنبؤ بالأحداث المستقبلية وتوقع التأثير المحتمل لهذه الأحداث بناء على الاستدلالات والاستنتاجات التي قد لا يتوفر لها الدعم التجريبي الكامل.». وهنا، لا توجد مخاوف الحكومة المتعلقة بجمع البيانات المتعلقة ب TikTok بمعزل عن غيرها. حيث يعكس السجل أن الصين «انخرطت في جهود مكثفة وطويلة لسنوات لتجميع مجموعات البيانات المنظمة، ولا سيما على الأشخاص الأمريكيين، لدعم عملياتها الاستخباراتية ومكافحة الاتصالات».

حتى لو لم تستفد الصين بعد من علاقتها مع ByteDance Ltd. للوصول إلى بيانات مستخدمي TikTok في الولايات المتحدة، فإن العرائض لا تقدم أي أساس لاستنتاج أن إنهاء الحكومة للصين قد تفعل ذلك ليس على الأقل «استنتاجا يمكن أن يستند إلى أدلة جوهرية». ونحن ندرك أن هذا القانون ينشأ في سياق «تنشأ فيه قيود تتعلق بالأمن القومي والسياسة الخارجية فيما يتعلق بالجهود المبذولة لمواجهة التهديدات المتطورة في منطقة يصعب فيها الحصول على المعلومات ويصعب تقييم تأثير سلوك معين». وبالتالي فإننا نعطي «الحكم المستنير» للحكومة احتراما كبيرا هنا. المرجع نفسه.

يجادل مقدمو العرائض كذلك بأن القانون غير شامل فيما يتعلق بمخاوف الحكومة المتعلقة بحماية البيانات data protection، مما يثير الشكوك حول ما إذا كانت الحكومة تسعى بالفعل إلى تحقيق هذه المصالح. وعلى وجه الخصوص، يجادل الملتمسون بأن تركيز القانون على التطبيقات ذات المحتوى الذي ينشئه المستخدم ويشاركه المستخدم، إلى جانب استبعاده لبعض نماذج المراجعة، يعفي من تطبيقات التنظيم التي «يمكن أن تكون قابلة مثل TikTok لجمع بيانات الأمريكيين». لكن «التعديل الأول لا يفرض أي وضع مستقل في ظل قيود الشمولية»، والحكومة «لا تحتاج إلى معالجة جميع جوانب المشكلة بضربة واحدة». علاوة على ذلك، كما خلصنا بالفعل، كان لدى الحكومة سبب وجيه لتمييز Tik-Tok بمعاملة خاصة. وفي هذا السجل، كان للكونغرس ما يبرره في معالجة مخاوف الأمن القومي المتعلقة ب TikTok بشكل خاص.

كما هو مطبق على مقدمي العرائض، تم تصميم القانون بما فيه الكفاية لمعالجة مصلحة الحكومة في منع خصم مباشر من جمع مساحات شاسعة من البيانات الحساسة حول 170 مليون شخص أمريكي يستخدمون TikTok. للبقاء على قيد الحياة من التدقيق المتوسط، «لا يجب أن تكون اللائحة أقل وسيلة تقييد للكلام لتعزيز مصالح الحكومة». بدلا من ذلك، فإن المعيار «مستوفي» طالما أن اللائحة تعزز مصلحة حكومية كبيرة يمكن تحقيقها بشكل أقل فعالية في غياب اللائحة «ولا «يتحدث بشكل مرهق أكثر مما هو ضروري» لتعزيز هذه المصلحة.

تفي الأحكام المطعون فيها بهذا المعيار. من الواضح أن الرؤى المقترحة تخدم الحكومة في جمع البيانات بشكل مباشر «بطريقة مباشرة وفعالة». وتفسر المحظورات حقيقة أنه في غياب تصفية مؤهلة، فإن عملية TikTok في الولايات المتحدة تورط في عمليات جمع البيانات الحكومية، في حين أن المتطلبات التي تجعل التجريد «مؤهلا qualified» تضمن معالجة هذه المخاوف قبل أن تستأنف TikTok عملياتها في الولايات المتحدة. علاوة على ذلك، لا المحظورات ولا شرط التجريد «أوسع بكثير من اللازم لتحقيق» هدف الأمن القومي هذا. بدلا من حظر TikTok تماما، يفرض Actim حظرا مشروطا. تمنع المحظورات الصين من جمع البيانات من مستخدمي TikTok الأمريكيين ما لم يقطع تصفية مؤهلة سيطرة الصين.

ويستعرض مقدمو العرائض سلسلة من البدائل - طلبات الإفصاح، وقيود مشاركة البيانات، واتفاقية الأمن الوطنية المقترحة، وشرط التعيين العام - التي يؤكدون أنها ستعالج مصلحة الحكومة في جمع البيانات بنفس القدر من حظر TikTok المشروط. هذه البدائل لا تغير تحليل الخياطة لدينا.

تتجاهل البدائل alternatives المقترحة من قبل مقدمي الالتماسات «العرض» الذي نمنحه للحكومة لتصميم حلول تنظيمية لمعالجة المصالح المحايدة للمحتوى content-neutral interests. للأسباب التي أوضحناها، فإن الأحكام المطعون فيها «ليست أوسع بكثير من اللازم not substan¬tially broader than necessary» لمعالجة مخاوف الحكومة المتعلقة بجمع البيانات. ولا تتحول صلاحية الأحكام المطعون فيها إلى ما إذا كنا نتفق مع استنتاج الحكومة بأن المسار التنظيمي الذي اختارته هو الأفضل أو «الأنسب». حين يتم استيفاء هذه المتطلبات هنا.

بالإضافة إلى مخاوف جمع البيانات التي تم تناولها أعلاه، تؤكد الحكومة اهتمامها بمنع خصم أجنبي من السيطرة على خوارزمية التوصية التي تدير منصة اتصالات أمريكية مستخدمة على نطاق واسع، ومن القدرة على ممارسة هذه السيطرة لتغيير المحتوى على المنصة في رجل لا يمكن اكتشافه. فإن هذا الأساس المنطقي هو تبرير قائم على المحتوى «يلوث» مصلحة الحكومة في جمع البيانات ويؤدي إلى تدقيق صارم strict scrutiny.

لم يشر مقدمو العرائض إلى أية قضية قامت فيها هذه المحكمة بتقييم المستوى المناسب من التدقيق في التعديل الأول لقانون صادر عن الكونغرس مبرر على أساس محايد المحتوى الاولي content-neutral والمستند الى المحتوى content-based. ومع ذلك، فإنهم يؤكدون أن الأحكام المطعون فيها تخضع للتدقيق الصارم – وتفشل – لأن الكونجرس لم يكن ليمرر الأحكام في غياب الأساس المنطقي لسيطرة العدو الأجنبي. ولسنا بحاجة إلى تحديد الموقف المناسب لقضايا المبررات المختلطة mixed-justification cases أو تحديد ما إذا كان تبرير السيطرة على الخصم الأجنبي للحكومة محايدا للمحتوى. حتى بافتراض أن الأساس المنطقي يتحول إلى المحتوى، فإن حجة الملتمسين تفشل في ظل التحليل المضاد للواقع الذي يقترحونه: السجل المعروض علينا يدعم بشكل كاف الاستنتاج القائل بأن الكونجرس كان سيمرر الأحكام الصعبة بناء على تبرير جمع البيانات وحده data collection justification.

بادئ ذي بدء، يركز تقرير مجلس النواب House Report بشكل كبير على مخاوف الحكومة المتعلقة بجمع البيانات، مشيرا إلى «توسع» TikTok في جمع بيانات data collection، و «صعوبة تحديد فئات البيانات بدقة tight interlinkages» التي تجمعها المنصة، والروابط الوثيقة بين TikTok والحكومة الصينية، وقدرة الحكومة الصينية على «إكراه» الشركات في الصين على «توفير البيانات وفي الواقع، لا يبدو أن أي مشرع عارض مخاطر الأمن القومي المرتبطة بممارسات جمع البيانات في TikTok، ولا شيء في السجل التشريعي يشير إلى أن جمع البيانات كان شيئا سوى مصدر قلق كبير للكونغرس. نحن قلقون بشكل خاص من تحليل دوافع الكونجرس في هذا السجل فيما يتعلق بقانون تم تمريره بدعم مذهل من الحزبين.

ويؤكد مقدمو الالتماسات أن نص القانون نفسه يقوض هذا الاستنتاج. على وجه الخصوص، يجادلون بأن الأساس المنطقي لجمع البيانات من قبل الحكومة لا يمكن أن يبرر شرط أن يمنع التجريد المؤهل «أي علاقة اختيارية» تسمح «بالتعاون مع إعادة النظر في تشغيل توصية المحتوى أو اتفاق فيما يتعلق بمشاركة البيانات». نحن نختلف. أوضحت الحكومة أن ByteDance Ltd. تستخدم البيانات التي تجمعها لتدريب خوارزمية توصية TikTok، والتي تم تطويرها وصيانتها في الصين. وفقا للحكومة، رفضت شركة ByteDance Ltd. سابقا الموافقة على التوقف عن جمع بيانات المستخدم الأمريكية أو إرسال تلك البيانات إلى الصين لتدريب الخوارزمية. فقد لاحظت الحكومة كذلك الصعوبات المرتبطة بمراقبة مشاركة البيانات بين ByteDance Ltd. وTikTok Inc. وفي ظل هذه الظروف، نجد أن تبرير الحكومة لجمع البيانات data collection justification كافيا لمواصلة الأحكام المطعون فيها.

ليس هناك شك في أنه بالنسبة لأكثر من 170 مليون أمريكي، يوفر TikTok منفذا مميزا وواسعا للتعبير ووسائل المشاركة ومصدر الاتصال. لكن الكونجرس قرر أن سحب الاستثمارات أمر ضروري لمعالجة التزامات الأمن القومي المدعومة جيدا فيما يتعلق بممارسات جمع البيانات في TikTok وعلاقتها مع خصم أجنبي. للأسباب المذكورة أعلاه، نستنتج أن الأحكام المطعون فيها لا تنتهك حقوق الالتماسات في التعديل الأول.

تم تأكيد حكم محكمة الاستئناف الأمريكية لدائرة مقاطعة كولومبيا.

It is so ordered. لذلك إنه أمر بذلك.

أ.د. عمر إبراهيم احسين
استاذ القانون الخاص
بكلية القانون جامعة طرابلس

في رحلة استثنائية تبدأ من قرية تامزاوة بمنطقة الشاطئ بجنوب ليبيا، وصولاً إلى قاعات ومدرجات الجامعة طالبا وأستاذا، وصياغة مشروعات القوانين واللوائح ومنها مايتعلق بتنظيم عمل المصارف، يحكي الأستاذ الدكتور عمر حسين أستاذ القانون الخاص والقمة والقامة العلمية التي خطت تاريخا مشرفا بأحرف من ذهب عبر سيرة علمية وحياتية حافلة بالإنجازات. إذ كرَّس حياته لتطوير التعليم القانوني وساهم في صياغة تشريعات رائدة أبرزها قانون المصارف الليبي رقم 1 لسنة 2005، الذي كان رئيسًا للجنة إعداده الذي وضع لبنات التحول الرقمي في القطاع المصرفي. في هذا الحوار نستعرض مسيرته من النشأة إلى ريادة الرقمية ونكشف عن رؤيته لتحديات التعليم القانوني ومستقبل التشريع في ليبيا.

- لتكن البدايات مدخلا لهذا الحوار فمن هوالأستاذ الدكتور عمر ابراهيم حسين ؟ وكيف تدرجت تعليميا وصرت أستاذا جامعيا ؟

- ولدت في قرية تامزاوة الشاطئ بجنوب ليبيا في عام 1959، دون ذكر اليوم والشهر لعدم التوثيق الدقيق في القرية يومئذ ؛ لأسباب موضوعية تتعلق بضعف التعليم، وتربيت في كنف المرحوم والدي الذي كان يمتهن الرعي في جبل الحساونة قبل أن تبدأ الدولة تشغيل أبنائها، لكن بعد اكتشاف النفط صارت الدولة تستوعب الأيدي العاملة من بينها والدي الذي اشتغل عاملا بأجر يومي في براك الشاطئ ، التي هي مركز متصرفية الشاطئ، وكان عمله بداية في مشروع زراعي يطلق عليه « عين التنمية»، مع عدد كبير من سكان الشاطئ بعضهم أقاربه منهم المرحوم عمي الغناي الهادي محمد.

تعلمت في مدرسة تامزاوة الابتدائية التي كان يدرس فيها ابناء قرى مجاورة ايضا، صاروا اعلاما في تخصصاتهم مثل المرحوم د إبراهيم ابوخزام ود الحبيب اوداعة الحسناوي وداحمد اعويدات ود عقيل حسين وم حمودة الاسود، اطال الله عمرهم جميعا ، درست الإعدادية في مدرسة براك الإعدادية التي كانت الوحيدة في منطقة الشاطئ وتحصلت على الثانوية من مدرسة سبها الثانوية، التي كانت أيضا الوحيدة في كل جنوب ليبيا، بعدها درست القانون في كلية القانون جامعة قاريونس التي تحصلت منها على الاجازة الجامعية الأولى عام 1982 بتقدير جيد جدا ، ولما كنت من ضمن اوائل دفعتي اختارتني الكلية معيدا في قسم المعاملات والقوانين الاقتصادية « القانون الخاص»، ولأن الدولة أوقفت الإيفاد للخارج فحرصت الكلية على ان تؤهل

معيديها في الداخل فالتحقت بالدفعة الثانية لدبلوم القانون الخاص ، الذي كان يطلق عليه يومئذ. « دبلوم المعاملات والقوانين الاقتصادية « وزميلي في هذا الدبلوم المرحومين د المستشار سعد العسيلي، والمحامي مصطفى العالم ، وبعد اجتياز المرحلة التمهيدية دافعت عن رسالتي للماجستير بعنوان. « جماعية المسؤولية المدنية « بتقدير جيد جدا في شهر سبتمبر 1988، تم تعييني عضو هيأة تدريس في الكلية، بعدها بدأت رحلة طويلة في التعليم الجامعي تخللها الدفاع عن اطروحة الدكتوراة في كلية الحقوق جامعة بيروت العربية، التي تشرف علميا عليها جامعة الإسكندرية ، ولم يكن ذلك أمرا سهلا لأنه بعد ايقاف ايفادي للدكتوراة في المغرب تم تكليفي مشرفا طلابيا على الطلبة الليبين الدارسين في لبنان وسوريا والاردن، مع ذلك استطعت الدفاع عن اطروحتي للدكتوراة في عام 1998 ؛ اجيزت بتقدير جيد جدا من لجنة رفيعة المستوى د مصطفى الجمال من مصر – د. نبيل ابراهيم سعد رئيس قسم القانون المدني في كلية الحقوق جامعة بيروت العربية ومن لبنان د.عبدالسلام شعيب ومن سوريا د الياس حداد ومن ليبيا د الكوني اعبودة، عدت مباشرة إلى كلية القانون بطرابلس لأنني كنت انتقلت اليها من جامعة قاريونس قبل انتهاء ايفادي للخارج ، ولم تمض شهورا حتى تم تكليفي عميدا لكلية القانون الذي استمر على مدى ست سنوات، فتدرجت فيها من محاضر حتى اعلى درجة في سلم سلك التدريس الجامعي.

- في ضوء تجربتكم بالتعليم الجامعي القانوني والادارة التعليمية، كيف تنظرون إلى التعليم القانوني بشكل عام والتعليم في القانون الخاص على وجه أخص؟ وما التحديات التي تواجه الباحثين فيه ؟

- أزعم مروري بتجربة ثرية في الإدارة التعليمية على مستوى التعليم العالي والتعليم الجامعي، في كلية القانون الام جامعة بنغازي او على مستوى وزارة» امانة « التعليم العالي او في جامعة طرابلس وغيرها من مؤسسات التعليم العالي في المنطقة الغربية، اظن ان تعليمنا العالي يعاني مشكلات كثيرة بعضها يشاركه فيها التعليم على المستوى العربي والعالمي وبعضها ينفرد بها، لكن التعليم القانوني الذي نعرفه اكثر من غيره ؛ صار بعد مروره بتجربة امتدت سبعين عاما في حاجة إلى التطوير في نواح عدة، اهمها تجاوز غياب ارتباطه بالتطبيق العملي للقانون في الواقع القضائي خاصة ، لأن احكام القضاء هي القانون الحي، علاوة على اغراق الطالب في تفاصيل كثيرة تحول دون تكوين الطالب تكوينا عاليا في الأساسيات والمبادئ الكبرى، والأهم التحدي الرقمي الذي صار ضروريا في العمل القضائي خاصة والقانوني عامة، فهو يغيب غيابا واضحا عن التعليم القانوني ، ولعل مشكلة مشاكل التعليم القانوني تتمثل في انتشاره بشكل غير مدروس ؛ ولم يقف ذلك عند المرحلة الجامعية الأولى، بل امتد حتى الى الدراسات العليا ؛ التي صارت في كل مكان دون النظر الى متتطلبات الجودة ومعاييرها.

اما التعليم القانوني في القانون الخاص فعلاوة على حاجته للتطوير في المسائل التي يحتاجها التعليم العالي بشكل عام فهو في حاجة إلى النظر إليه بعين فاحصة ؛ خاصة على مستوى الدراسات العليا التي يجب أن تدخل تجربة جديدة تنسجم مع حاجة المجتمع للتخصصات في الشركات التجارية والقانون المصرفي وقطاع الأعمال والتجارة الدولية والقانون الرقمي.

تواجه الباحثين في الدراسات العليا بالقانون الخاص تحديات كثيرة، بعضها تشترك فيها فروع آخرى وبعضها ينفرد بها، فعلاوة على ضعف المكتبات وتراجع تزويدها بأحدث ما انتجه العقل العلمي الإنساني ؛ بل خلوها من رسائل واطروحات الدكتوراة حتى المجازة في ليبيا ؛ يعيش التعليم العالي في القانون الخاص مشكلات عدة اهمها ؛ عدم امتلاك الطالب لغة اجنبية تمكنه من متابعة الاطروحات والرسائل الجامعية والأبحاث التي تُكتب بغير العربية، علاوة على عدم متابعة الأحكام القضائية والتحكيمية الوطنية والدولية في المنازعات المدنية والتجارية الوطنيةوالدولية.

ينقص التعليم القانوني في القانون الخاص غياب تخصص الطالب في فرع منه سواء في الدراسة الجامعية او على مستوى الدراسات العليا ، فلا نجد في الدراسة الجامعية من يتخصص في الجانب القضائي او في المهن القانونية الأخرى، بعد دراسة المبادئ الكلية في فروع ألقانون عامة، كما لا نجد هذا التخصص الدقيق على مستوى الدراسات العليا ايضا ؛ حيث يدرس الطالب المواد العامة في القانون الخاص دراسة معمقة في موضوع يختاره الاستاذ ؛ في القانون المدني والمرافعات والتجاري والعمل في بعض الكليات ويختار الطالب مادتين اختياريتين في التحكيم التجاري او قانون الضمان الاجتماعي او غيرهما، دون ان يتخصص في القانون المدني او التجاري او إجراءات التقاضي والتحكيم او القانون الاجتماعي بفرعيه العمل والضمان الاجتماعي ، ولا يتخصص الباحث الا عندما يكتب الماجستير او الدكتوراة.

- كنتم رئيسا للجنة قانون المصارف رقم 1 / 2005 فما المبادئ التى انطلق منها هذا القانون ؟

- جاء هذا القانون بعد سياسة تشريعية طويلة في القانون المصرفي، منذ صدور اول قانون للنقد الليبي رقم 4لسنة 1951ثم القانون رقم 3لسنة 1955 بإنشاء البنك الوطني الليبي الذي تغير اسمه الى مصرف ليبيا بموجب القانون رقم 4لسنة 1963 بشأن البنوك وكان آخرها القانون رقم 1 لسنة 1993 بشأن المصارف والنقد والائتمان وتعديلاته ، الذي اطلق تسمية مصرف ليبيا المركزي واعتمدها القانون الساريالذي حاول تجاوز ما اعترض قانون1993 من مشاكل عملية وغياب مسائل مصرفية ضرورية ؛ اهمها على الاطلاق استقلالية المصرف المركزي، وتولت صياغة القانون رقم 1لسنة 2005 لجنة رفيعة المستوى من قانونيين ومصرفيين ذوي خبرة منهم زميلنا المرحوم د مصطفى ادبارة ، الذي كان مقررا للجنة وابدع بلغته القوية في سبك صياغة القانون واستاذ الاقتصاد البارز في جامعة بنغازي د محمد ابوسنينة ، الذي كان مديرا لإدارة الرقابة على المصارف والنقد في المصرف المركزي وقتئذ، والاستاذ علي اشنيبيش مدير إدارة البحوث في المصرف المركزي

صاغت اللجنة القانون بما يليق بالمصرف المركزي بأعتباره السلطة النقدية الأعلى و يلبي حاجة المصارف الليبية ويضمن تطويرها فتم تقسيمه منهجيا الى ثلاثة ابواب، تلبي حاجة القطاع المصرفي، جعلت لجنة الصياغة الباب الأول للمصرف المركزي المواد 1-64 وتم تخصيص الباب الثاني إلى المصارف التجارية المواد 65-100 اما الباب الثالث فخصصته اللجنة إلى العقوبات المواد 101 -119 .وتم تعديله لاحقا بإضافة فصل للصيرفة الاسلامية بموجب القانون رقم 6لسنة2012.

ضبط القانون في الباب الأول دور المصرف المركزي بأعتباره سلطة نقدية مستقلة ؛ يختص بمزاولة وظائف

عدة ، تدور حول اصدار النقد الليبي وإدارة احتياطات الدولة وتنظيم السياسة النقدية والائتمانية والمصرفية وتحقيق أهداف السياسة الاقتصادية تجاه استقرار المستوى العام للأسعار وسلامة النظام المصرفي وإدارة السيولة النقدية وتنظيم سوق الصرف الاجنبي و الاهم منح القانون المصرف المركزي صفة مستشار الدولة بالسياسة الاقتصادية العامة ، وقد ترجمت المواد من السادسة إلى الرابعة والستين وظائف المصرف المركزي.

اما الأداة التى تعمل على تطبيق السياسة النقدية المرسومة في مجلس إدارة مصرف ليبيا المركزي فهي المصارف التجارية ، فخصص لها القانون الباب الثاني الذي توزع على ثلاثة فصول فكان أولها خاصا بتاسيس المصارف والاشراف عليها المواد 65 -72 وبين الفصل الثاني واجبات المصارف المواد 73-92 وجعل القانون الفصل الثالث إلى الأحكام العامة المواد،93 - 100.

استعان القانون بالجزاء الجنائي لتأكيد طابعه الآمر فكانت المواد 101 - 119 ، تخللتها عقوبات يوقعها مجلس ادارة المصرف المركزي، على المصارف التجارية إذا خالفت تعاليماته والسياسة النقدية التي يرسمها، ويعمل محافظ المصرف ونائبه على ضمان تطبيقها وبينت المادة 101 ثانيا ما يختص به مجلس إدارة المصرف المركزي بتوقيع عقوبات مالية حددتها المواد102، 104، 106، 107، 111،108.

- ما أبرز المسائل التي استحدثها قانون المصارف رقم 1 لسنة 2005 ؟

- اظن تستغرق الاجابة على هذا السؤال الحوار كله ، لكن نذكر ما نراه هاما وجديدا فقط ونحصره فيما يلي

1- حرص القانون على تأكيد استقلالية المصرف المركزي، حيث صارت تبعيته إلى السلطة التشريعية في المادة 2 (مؤتمر الشعب العام سابقا)، الذي حل محله البرلمان ويدار المصرف بموجب المادة 14 بمجلس إدارة يكون المحافظ رئيسا له نائب المحافظ نائبا للرئيس علاوة على وكيل وزارة المالية وأربعة من ذوي المؤهلات العالية في القانون او الشؤون المالية او المصرفية او الاقتصادية.

يختار البرلمان بموجب المادة 17 (مؤتمر الشعب العام سابقا) المحافظ ونائبيه لمدة خمس سنوات وبجوز اعادتهما وتعين إدارة البرلمان بالتشاور مع المحافظ الأعضاء الخمسة عدا وكيل وزارة المالية، نقارن فقط وضع المصرف المركزي في قانون 1993وقانون2005 لنعرف مدى تبعية المصرف المركزي لوزارة المالية في القانونين، حيث استقل المصرف المركزي استقلالا تاما عن وزارة المالية في قانون 2005فلم يعد لها دور في رسم السياسة النقدية التي يستقل بها مجلس ادارة النصرف المركزي دون غيره.

2- استحدث قانون المصارف رقم 2005/1 وضعا لم يكن موجودا في قانون المصارف السابق لعام 1993 وهو ما نصت عليه م65 (يكون مصرفا تجاريا كل شركة)، وكشفت المادة 67 شكل هذه الشركة لأنها اشترطت ان تتخذ (شكل شركة مساهمة)، بما تمثله من نظام قانوني راسخ، (يساهم فيه الأشخاص الطبيعيون والاعتباريون العامة والخاصة)، وتلك دعوة إلى دور اكبر للقطاع الخاص إلى الاستثمار في الحقل المصرفي وهو ما اراد قانون المصارف ترسيخه، وشهدنا بعد صدور هذا القانون ، حجم مشاركة القطاع الخاص في تأسيس المصارف مقارنة بقانون 1993.

3- اجاز القانون في المادة41 لكل شخص طبيعي او معنوي الاحتفاظ بما يملكه او يحوزه او يؤول إليه من نقد

اجنبي، وله إجراء اي عملية من عملياته، بما في ذلك التحويل للخارج ، كما اجازت المادة43 للمصارف التجارية فتح حسابات بالنقد الاجنبي للأشخاص الطبيعين والمعنويين وتتم تغديتها بواسطة ودائع بالعملة الأجنبية او مبالغ محولة من الخارج اومن حساب محلي بالنقد الأجنبي.

4- اجاز القانون للمصرف المركزي في المادة 46 بأذن من مجلس إدارته مزاولة الصرافة والخدمات المالية وفق الضوابط التي يضعها مجلس الإدارة، وذلك توجه جديد يفتح آفاقا جديدة للعمل .

5- اجازت المادة 53 للمصارف التجارية منح عملائها ائتمان بالنقد الأجنبي وفق ضوابط يحددها مجلس إدارة المصرف المركزي.

6- منح القانون لمحافظ المصرف حق اتخاذ جملة من الاجراءات، اذا اتضح له ان اي مصرف تجاري يعاني مشاكل مالية، بما في ذلك دعوة الجمعية العمومية للانعقاد لاتخاذ اي اجراء مناسب، وله أيضا وقف مجلس إدارة هذا المصرف بل منحه القانون مكنة تعيين لجنة إدارة مؤقتة لتصحح أوضاع المصرف ، كما منح المحافظ دمج المصرف في مصرف آخر بشرط موافقة الجمعية العمومية للمصرف المدموج فيه.

7- فتحت صياغة القانون المرنة إمام المصرف المركزي السماح للمصارف التجارية بالصيرفة الإسلامية ، حيث نصت المادة65 ثانيا فقرة 12يعتبر من الأعمال المصرفية التي يمارسها المصرف التجاري « اي أعمال آخرى تتعلق بالنشاط المصرفي يوافق مصرف ليبيا المركزي على ممارستها»، وفعلا قرر مجلس ادارة المصرف المركزي ادخال الصيرفة الإسلامية اعمالا لهذا التفسير الذي ابديته في اجتماع للمجلس، بعد ان طلب من إدارة الرقابة على المصارف والنقد اعداد دراسة حول الامر التي اعتمده المجلس في عام 2008 وعمم منشورا على المصارف لمباشرة الصيرفة الإسلامية من بين انشطته، كان ذلك قبل تعديل القانون بموجب القانون رقم 46 لسنة 2012 بسنوات ؛معتبرا الصيرفة الاسلامية من بين ما تقدمه المصارف التجارية الليبية.

8- اجاز القانون لمصرف ليبيا المركزي في، المادة67 ثالثا لأول مرة منذ تأميم المصارف الأجنبية، الأذن بتاسيس مصارف برأس مال اجنبي واجازت ذات المادة للمصارف الأجنبية المساهمة في مصارف ليبية وفق الشروط التي يضعها مجلس إدارة المصرف المركزي.

9- اجازت المادة 72 لأول مرة للأشخاص الطبيعيين والمعنويين امتلاك أسهم في المصارف المملوكة للدولة، تشجيعا للقطاع الخاص، واجازت هذه المادة لكل مصرف تجاري ان يضع ما يقتضيه واقع الحال من دخول للعاملين فيه بقرار يصدره مجلس ادارته، وذلك يشجع المصارف على استقطاب الخبرات والقدرات المصرفية.

10- وضعت المادة 79 شروطا قاسية على مجلس إدارة كل مصرف تجاه منح اي ائتمان ؛ الا اذا تأكد من الجدارة الائتمانية وصحة المعلومات والبيانات المقدمة وآليات الرقابة على استخدام الا ئتمان، وحرص على ان يكون في الهيكل التنظيمي لكل مصرف وحدة للامتثال.

11- لضمان حق كل مصرف تجاري في استرداد ما قدمه من إئتمان ، الزمه القانون في م80 ان ينشئ نظاما للتسجيل الفوري والمستمر لمراكز زبائنه المتحصلين على تسهيلات ائتمانية وربطه بقاعدة المعلومات المُجمعة بمصرف ليبيا المركزي.

12- حرص القانون في المادة86 على منح المساهمين الذين يملكون ربع الاسهم ان يطلبوا من مصرف ليبيا المركزي التفتيش على أعمال المصرف.

13 - اجاز القانون في المادة87 لضمان المتانة المالية للمصارف مكنة الاندماج في غيرها بشرط موافقة مجلس إدارة المصرف المركزي.

14 - أنشأ القانون لأول مرة في م91 صندوقا لضمان أموال المودعين للتأمين على الودائع في المصارف الليبية، تكون له شخصية اعتبارية وذمة مالية مستقلة يضم جميع المصارف التي تقبل الودائع.

15- اجاز القانون في 92 لأول مرة في ليبيا للمصارف ان تنشئ اتحادا بينها، يصدر مجلس إدارة المصرف المركزي قرارا بإنشائه ونظامه الأساسي ايضا.

16 - لم يكتف القانون بالنص على السر المصرفي في م94، بل اوردت م95 حظرا على رؤساء وأعضاء مجالس الإدارة والمديرين العامين والعاملين كافة ان يعطوا معلومات مصرفية اطلعوا عليها تخص زبائن المصرف او حساباتهم او ارصدتهم او تمكين الغير من الإطلاع عليها، ما لم يكن مصرحا بها قانونا، واردت المادة 96 استثناءات اولها اطلاع مراجعي الحسابات المكلفين من الجمعية العمومية وثانيها اطلاع مفتشي إدارة الرقابة على المصارف وثالثها كشف المصرف عن كل او بعض بيانات الزبون لإثبات حقه في نزاع قضائي ورابعها ما يتخذ من إجراءات في الصكوك الراجعة ومكافحة غسل الأموال ومكافحة الارهاب.

17 - أعطى القانون في المادة 116 لأول مرة محافظ مصرف ليبيا المركزي ان يحدد بقرار الموظفين الذين لهم صفة مأموري الضبط القضائي للجرائم التي تقع بالمخالفة لقانون المصارف.

18- اظن اهم تجديد في هذا القانون هو اعتماد الرقمية ؛ عندما اعترفت المادة97 للمستندات والتوقيعات الإلكترونية حجية في الإثبات واعتبرت هذه المادة مخرجات الحاسوب المصرفية بمثابة الدفاتر التجارية وفق القانون التجاري، وتكون للنسخ المصغرة على أقراص صلبة او مرنة او مضغوطة ذات قيمة الدفاتر التجارية وتكون لها حجية في الإثبات.

- تعتبر المادة 97 من القانون تحولًا هامًا في التشريع المصرفي الليبي، كيف تم تبني هذا التوجه الرقمي؟

- قلت سابقا تكشف المقارنة بين قانون 1993 وقانون 2005 ، مدى ما أحدثه القانون الجديد من تطوير في العمل المصرفي، وكان من بين ذلك المادة 97 التي اعطت لمخرجات الحاسوب والتوقيعات الإلكترونية حجية في الإثبات ؛ مثل الاوراق التقليدية تماما، ويعد ذلك تحولا في القانون الليبي، سجل قانون المصارف السبق وإستشراف المستقبل ؛ كان النص فاتحة التحول الرقمي في ليبيا، الذي صارت المصارف العالمية تشهده، ومصارفنا مرتبطة بعلاقات معها فليس من الحكمة او من حسن الصياغة التشريعية تجاهل هذا الواقع، خاصة أن بعض المصارف الليبية بدأت استخدام الحاسوب في معاملاتها، ووضح د محمد ابوسنينة عضو لجنة إعداد القانون بإعتباره مديرا لإدارة الرقابة على المصارف، تجربة المصارف في التحول الى المستندات الإلكترونية ، وإن التحول الرقمي قادم فلا يمكن لقانون المصارف الجديد تجاهل المستقبل، وبدا نقاش واسع حوله وتكشف صياغة المادة ذلك فكانت حاضرة قواعد الإثبات في القانونين المدني والتجاري، لكن مع ذلك يتطلب العمل المصرفي تجديدا لها، بما ينسجم مع تشهده المصارف التجارية من واقع وما ستسهده في المستقبل ، ولذلك لم يكن إمام لجنة صياغة مشروع قانون جديد للمصارف، الا ان تستجيب لما آت في

المستقبل ، وهو امر يعود إلى فن الصياغة التشريعية ؛ التي لا يجب أن تقنن الواقع فقط على اهميته، بل وضع صياغة تستوعب ما قد يأتي به المستقبل.

- كيف ترون مستقبل التشريعات المصرفية في ليبيا في ظل التحول الرقمي؟

- قلت سابقا : ان مصارفنا لم تكن في معزل عن ما تشهده المصارف العالمية من تحديث، وأظن أن المادة97 من قانون المصارف رقم 2005/1 شرعنت استخدام المستندات الإلكترونية، لأن قانون المصارف أعطاها حجية في الإثبات، وأظن الزمت هذه المادة المصارف الاهتمام بمخرجات الحاسوب والتوقيعات الإلكترونية ، لأن القانون اعتبرها دليلا في الإثبات ، ولذلك يكفي فقط تأمل واقع المصارف التجارية الليبية قبل 2005 وبعدها، لتلاحظ ما المدى الذي صارت الرقمية إليه ؟ في الواقع وتنوع المنتجات المصرفية الإلكترونية من خدمات مصرفي إلى البطاقة المصرفية التي ساهمت مساهمة كبيرة في حل مشكلة السيولة، فصارت بعد نص م97 في قانون المصارف رقم 1لسنة2005 الرقمية في العمل المصرفي اصلا والورقية استثناء. فلم تغب الرقمية اليوم في العمل المصرفي في المصارف الليبية ، ولا اظن كان ذلك ممكنا في غياب نص م97 من قانون المصارف

- يعود لكم الفضل في تبني الرقمية في قانون المصارف في ليبيا فكيف استقبل الوسط القانوني ذلك،؟ وما الواقع الرقمي في الإدارة بالدولة اليوم ؟

- يعود الفضل اولا إلى لجنة إعداد القانون التي كنت رئيسها، التي ضمت نخبة من أفضل القانونين والمصرفيين، واذكر منهم شخصين كانا فاعلاين على نحو جعل القانون يخرج بهذه الصياغة اولهما زميلنا المرحوم د مصطفى ادبارة الذي كان مديرا لإدارةالشؤون القانونيةبمصرف ليبياالمركزي فكان لقدرته العميقة في اللغة دور لا ينسى، وزميلنا في جامعة بنغازي استاذ الاقتصاد البارز د محمد ابو سنينة الذي كان مديرا لإدارةالرقابة على المصارف والنقد ، حيث وضح امام اللجنة كل ما يحتاجه العمل المصرفي من تطوير، و يعود الفضل ايضا الى مصرف ليبيا المركزي ومحافظه اولا د أحمد امنيسي ثم ا فرحات بن قدارة الذي كان نائبا للمحافظ ثم صار محافظا، فالمصرف هو الذي بادر في العقد الأول من القرن الحادي والعشرين إلى إعادة النظر في المنظومة القانونية المصرفية بما يجعل القطاع الخاص مشاركا على نحو واسع ، وتشكل المصارف التجارية العمود الفقري في الحياة الاقتصادية ، فلم تصغ هذه اللجنة قانون المصارف فقط، بل صاغت قانون مكافحة غسيل الأموال وقانون التأجير التمويلي وقانون الاستقرار الاقتصادي الذي وحده لم يصدر !!.

لا تتوقع أن يقبل العقل الجمعي ، الذي عايش زمنا طويلا الإدارة التقليدية المعتمدة على المستندات الورقية بسهولة التعامل الرقمي ، لكنه فرض نفسه على الدولة التي استخدمته على نطاق واسع في معاملاتها ووثاقها الرسمية مثل الرقم الوطني وجواز السفر وغيرهما الكثير .

- هل واجهتكم تحديات في إدخال الرقمية في قانون المصارف ؟ وكيف يمكن نجاح الرقمية في ليبيا؟

- قلت سابقا : ان الحاجة هي التي فرضت تبني الرقمية في قانون المصارف لسببين اولهما التعامل مع المصارف في الخارج التي بدات فيها الرقمية منهجا وثانيهما ان بعض المصارف بدأت تدخل الرقمية في

معاملاتها.

يحتاج نجاح الرقمية لئن تصبح منهجا ووطريقة عمل وتطويرها يحتاج أمرين اولهما اصدار تشريعات تنظمها ثم التدريب الواسع لمن لا يتعامل بنجاح معها واشتراط معرفتها لكل من يتم تعيينه في الدولة او التعاقد معه للعمل في القطاع الخاص.

- هل يستوعب القانون الليبي إدخال الرقمية اداة عمل ؟

- فرضت الرقمية نفسها على كل المجتمعات والدول ، وبدأت تصدر قوانين تدخلها ضمن منظومتها القانونية، مثل قوانين التجارة الإلكترونية وغيرها، وهذا مسلك المشرع الليبي الذي اصدر قانونا خاصا بالمعاملات الإلكترونية رقم 6 لسنة 2022، ثم صدر القرار رقم 109لسنة 2022 بتشكيل لجنة للتحول الرقمي وتفعيل الادارة الإلكترونية.

عالج قانون المعاملات الإلكترونية، رقم 6 في تسعة فصول ؛ كل ما يتعلق بالمعاملات الرقمية، منها الفصل السادس. « العمليات المصرفية «، وأظن ذلك هو مبرر صدور هذا القانون انطلاقا في ديباجته من قوانين عدة منها قانون المصارف رقم 1لسنة 2005، نظم في هذا الفصل كل العمليات المصرفية الرقمية في المواد 63- 72 كل ما يتعلق بالعمليات المصرفية الرقمية ، وما كان ليتم ذلك لولا المادة97 من قانون المصارف، التي نبهت المشرع إلى حاجة العمليات المصرفية الرقمية إلى أن تحظى بالتنظيم القانوني الواسع ، تبرر خصوصية العمل المصرفي والعمليات الرقمية فيه ؛ دعوة مصرف ليبيا المركزي ان يقدم مشروع قانون ينظم العمليات المصرفية الرقمية.

- مارستم التعليم الجامعي القانوني سنوات طويلة وشاركتم في صياغة عدة قوانين ، ما رسالتكم لصناع التشريع وطلبة القانون في الدراسة الجامعية والدراسات العليا؟

- ادعو السلطة التشريعية ان تخضع القوانين التي تسنها إلى عميق الدراسة والحوار الواسع حولها سواء من المعنيين بها مباشرة، من خلال نقاباتهم وتجمعاتهم المهنية او من خلال المؤسسات المعنية بتطبيقها او من خلال مؤسسات تعليم القانون في الجامعات واكاديمية الدراسات العليا، ذلك يدفع الطلبة فيها إلى معاصرة ولادة القانون.

كما ان الحوار المجتمعي العام يجعل القانون ملبيا لحاجة المجتمع، لأن التأثير المتبادل بين المجتمع والقانون حقيقة لا يمكن تجاهلها.

خاتمة اللقاء الصحفي

في رحلة استثنائية حافلة بالإنجازات، أثبت الأستاذ الدكتور عمر حسين أن الإصرار والمعرفة هما المفتاح الحقيقي للريادة. من أروقة الجامعة إلى ساحات التشريع، سطّر تاريخًا مشرّفًا ساهم في تطوير التعليم القانوني وتعزيز التحول الرقمي في النظام المصرفي الليبي. برؤية ثاقبة وإيمان راسخ بأهمية التحديث، قاد جهودًا بارزة تركت بصمتها في مجال القانون والاقتصاد. وما بين الماضي الذي شكل الأساس، والحاضر الذي يشهد على الإنجازات، يبقى المستقبل مفتوحًا لمزيد من العطاء والإبداع. وختامًا، لا يسعنا إلا أن نُحيي مسيرة ملهمة تُعد نموذجًا يُحتذى به للأجيال القادمة.

شروط النشر في المجلة القانونية

1. القيمة القانونية

يُشترط أن يكون العمل ذا قيمة قانونية، ويتناول مواضيع مهمة ومتطورة في الجانبين القانوني والقضائي.

2. المنهجية العلمية

يجب أن يكون البحث المُحكَّم متوافقًا مع الأصول العلمية الصحيحة والمعايير الأكاديمية المعتمدة.

3. طريقة التقديم

* يُقدَّم العمل مطبوعًا على قرص مدمج (CD) باستخدام خط عربي بحجم 14، أو يُرسل عبر البريد الإلكتروني الخاص بالمجلة.

* يجب مراعاة التدقيق اللغوي والإملائي قبل التقديم.

4. عدد الكلمات والصفحات

* يجب ألا يقل عدد كلمات البحث المُحكَّم عن 5000 كلمة، وألا يزيد عن 12,000 كلمة.

* يتراوح عدد الصفحات بين 12 إلى 30 صفحة.

5. عملية التقييم

* تخضع البحوث المُحكَّمة لتقييم الهيئة الاستشارية العلمية، وفقًا للأصول العلمية.

* تخضع الأعمال الأخرى (مثل المقالات أو التراجم) لتقييم هيئة التحرير.

6. مسؤولية الآراء

الأبحاث والمقالات والتراجم المنشورة في المجلة لا تعبّر عن رأي أو توجه المجلة، وإنما تعبّر عن آراء أصحابها فقط.

7. عدم استرجاع الأبحاث

جميع الأبحاث والمقالات والتراجم المقدمة لا تُعاد إلى أصحابها، سواء تم نشرها أم لم تُنشر.

8. السيرة الذاتية

يجب أن يُرفق مقدّم العمل نبذة موجزة عن سيرته الذاتية، تتضمن المؤهلات والخبرة العلمية.

للتواصل وإرسال الأعمال

* الهاتف: +218 93 482 5045

*البريد الإلكتروني: bawsala@cid.gov.ly

مجلة
البوصلة الرقمية

المجلة الليبية لقانون الانترنت

تصدر عن إدارة مكافحة جرائم تقنية المعلومات
جهاز المباحث الجنائية / وزارة الداخلية الليبية

العدد الأول
مارس 2025

إدارة مكافحة جرائم تقنية المعلومات
CYBER CRIMES DEPARTMENT