حماية الاقتصاد الرّقمي بين السّياسة الجنائية والمواطنة الرّقمية

د. ناني نبيلة
جامعة البليدة2
البليدة، الجزائر
profnabilanani@gmail.co

أ.ناني لحسن
جامعة إبن خلدون
تيارت، الجزائر
lahcenenani@gmail.co

الملخص:

بكل إيجابياتها وسلبيّاتها تفرض الرّقمنة اليوم لغتها حتميةً حضاريةً لا خيارا إيديولوجيًّا، والاقتصاد الرّقمي بالرغم من حداثته كمفهوم وكممارسة إلا أن البراعة فيه، وبالتّسارع المناسب، مطلبٌ حضاري لكلّ أمّة طموحة، علما أنّ الحداثة على قدر ما تعطيه للاقتصاد الرّقمي من مزايا على حساب الاقتصاد الكلاسيكي، على قدر ما تضعه في موقف الضّعيف أمام مخاوف متوقّعة وغير متوقّعة من المساس بأمنه، خصوصا وأن الفجوة الرّقمية لا زالت شاسعة بين دولة وأخرى من جهة، وبين فئات نفس المجتمع في البلد الواحد من جهة أخرى. ومع صعوبة مسايرة الانفجار المعرفي والتكنولوجي لهذا العصر، فإن بعض أصحاب المعرفة الرّقميّة يُصَعِّدون في استغلال معارفهم للمساس بأمن المنظومات الاقتصادية على المستوى المحلي و/أو الدولي كلما زادت المعارف وتدنّت القيم. من هذا المنطلق نعرض لكم في ورقتنا البحثية هذه توليفةً من التدابير التي تساهم في حماية الاقتصاد الرّقمي، والتي توصّلنا إليها في إطار مسيرة من البحوث "النفسُقانونية" والتي تجمع بين الحلول النفسية والقانونية لمشكلات المجتمعات الرّقمية.

الكلمات المفتاحية: المواطنة الرّقمية، الاقتصاد الرّقمي، السياسة الجنائية، الفجوة الرّقمية.

Abstract:

The present research aims to determine to which extent the variable of the mother's job influences the development of sexual profiling of roles in both boys and girls between 6 and 9 years of age using sex roles.

The test consists of a classification of 12 items representing a group of activities for adults, and a group of games for young people in the form of drawings submitted to the examinees to classify them as males, females, and for both sexes. To treat the information statistically, K^2 test

was used to examine if there existed significant differences with respect to sex and age variables, and the mother's age. As a result, we found no differences except in the age variable and in a few items.

مقدمة:

في الوقت الذي تخترع فيه الأمم المتقدمة بدائل جديدة متجددة للحياة، فإن الأمم الخاملة تكتفي بنصب حلقات النقاش لتجيب عن السؤال: هل نسمح باستدخال هذا الجديد؟ وقبل أن تخلُص إلى الجواب تجد أن واقعها تجاوزها، وتُرغَم على أن تُعيد ترتيب طاولة النقاش لتجيب عن سؤال آخر وهو: حسنا....كيف نتعامل مع هذا الجديد؟ وتظل الأمم الواعية تتقدّم، بينما الأمم الخاملة "تُناقش"!

إن أمما كهذه، يغيب عنها أنه ليس النقاش هو المطلوب دائما، وأن الوقت الذي تستغرقه في النقاش إنما يُضاف لرصيد تخلّفها ما دامت لم تحرص على استثماره في تقدّمها. إننا نعيش عصرا تتسارع فيه دواليب "التغيير الكوني" المحتوم، والجديد الذي نخشاه علينا أن نستبقه إستشرافًا وتحسّبًا، لا أن نقتله مجادلةً ونقاشًا.

إن واحدة من أحدث محرّكات التغيير الراهنة هي "الرّقمنة"[1]، والتي فرضت نفسها حتمية في مختلف مناحي الحياة الإنسانية وأملت متطلباتها بالنتيجة، وكونه يتصدر قائمة القطاعات الأشد تفاعليّة مع المحيط، فإن القطاع الاقتصادي كان سبّاقا في مسار الرقمنة، ذاك المسار الذي بقدر ما يرتفع بمستويات الاقتصاد بقدر ما يضعه أمام تحديات "الخطر الرقمي"[2] التي تهدد أمنه واستمراريته.

في مقالنا هذا، وبعد أن نبيّن حتمية "الاقتصاد الرقمي"[3] ومحاذيره، سنعرض بين أيديكم نتاج دراستنا النفسُقانونية والماثل في توليفةً من التدابير الاستباقية ثم الردعيّة لحمايته من أشكال الجُرم الرقمي.

[1] **Digitization.**
[2] **Digital risk.**
[3] **Digital economy.**

1. التأطير المرجعي للمشكلة:

لأسباب علمية وابستيمولوجية لا يتسع المقام لذكرها هاهنا، نتبنى المقاربة المنظوميّة[4] في تناولنا موضوع حماية الاقتصاد الرقمي، وذلك وفقا للتقنية التي طورناها خلال سنوات من البحث في التحليل المنظومي[5] (L. Bouabdellah and al. 2012)، فنسوق لكم نواتج تحليلاتنا وفقا للتراتب الآتي:

1-1- **رسم حدود المنظومة:** منظوميا تُعرّف كل منظومة بمكوناتها، تفاعلاتها وغايتها، ومنه نعرّف الاقتصاد الرقمي، كما يلي: "هو كليّة تكنولوجيات المعلومات والاتصال المتكاملة في بنيتها والمتساندة في وظائفها بغاية تحقيق الرفاه الإقتصادي".

1-2- **تعريف غاية المنظومة:** "الرفاه الإقتصادي" هو تلك الحالة التي تعطي الفرد إمكانية تطوير ذاته ومحيطه[6] بالتزامُن. ويزداد الرفاه الإقتصادي كلما ازداد ثابت التناسب الطردي بين رفاهية الفرد ورفاهية المحيط[7].

1-3- **التحليل البنائي لمنظومة الاقتصاد الرقمي:** تتكون منظومة الاقتصاد الرقمي من ثلاث لبنات أساسيّة وهي:

- **الأصول:** منها الفكرية ومنها والمادية، فأصول الاقتصاد الرقمي في أهم أشكالها هي أصول فكرية تتمثل في المعرفة والمعلومة، بينما الأصول الماديّة مثل السيولة، الهياكل والمُنشآت فهي أصول داعمة، وقد تنضوي تكنولوجيات الاعلام والاتصال تحت بند الأصول عندما تكون محلا للاستثمار.
- **الرقمنة:** تمثل تكنولوجيات الاعلام والاتصال اللبنة الأساسية في الاقتصاد الرقمي وهي في شكليها (السوفت/ الهارد) تمثل الوسيلة لكل مناشطه.

---

[4] Systemic approach.

[5] Systemic analysis.

[6] المحيط هنا نعني به أقصى نقطة يمكن أن يصلها تأثير الاقتصاد الرقمي.

[7] هذا التعريف توصلنا إليه بعد دراسة مفاهيميّة في مفهوم الرفاه الإقتصادي لا يتسع المقام هنا لسردها.

- **التشريع:** النصوص التشريعيّة ترافق النشاط الاقتصادي مهما كان حجمه ونوعه منذ أن يلوح فكرة في الخاطر إلى أن يتجسّد على أرض الواقع وتظل تلك النصوص تتعهده بالرقابة والحماية.

4-1- **التحليل التفاعلي لمنظومة الاقتصاد الرقمي:** يتم التحليل التفاعلي على مستويين، على المستوى الداخلي حيث ندرس أشكال التفاعلات الداخلية للبُنى فيما بينها التي يُفتَرَضُ أنها تُؤدي بالنتيجة وظائفها لتحقيق الغاية النهائية للمنظومة، ثم على المستوى الخارجي حيث ندرس أشكال تفاعل المنظومة ككل مع محيطها والتي يُفترض أنها تحقق غايات المنظومة والمحيط في آن واحد.

1-4-1- **التحليل التفاعلي الداخلي لمنظومة الاقتصاد الرقمي:** ينطلق التحليل التفاعلي الداخلي من مُصالبة مكونات المنظومة كما يأتي:

	الأصول	الرقمنة	التشريع
الأصول		1	2
الرقمنة	$\bar{1}$		3
التشريع	$\bar{2}$	$\bar{3}$	

وانطلاقا من هذه المصفوفة يمكننا رصد التفاعلات الداخلية لمنظومة الاقتصاد الرقمي كالآتي:

✍ **التفاعل ($1\text{-}\bar{1}$): (أصول ↔ رقمنة):** في الوقت الذي تعطينا فيه الأصول إمكانية الحصول على أحدث تكنولوجيات المعلومات والاتصال فإن الرّقمنة بدورها تعطينا إمكانية تعظيم العائد من إستثمار الأصول.

✍ **التفاعل ($2\text{-}\bar{2}$): (الأصول ↔ التشريع):** بينما كمّ وكيف الأصول يعطينا الأساس لتحديد النصوص التشريعية المنظِّمة لنشاطنا الاقتصادي فإن التشريع يعطي شرعيّة الوجود والنشاط للأصول، ويوفّر لها الحماية اللازمة.

✍ **التفاعل (3-3): (التشريع ↔ الرقمنة)**: بينما التشريع يعطي شرعية الوجود والنشاط لتكنولوجيات الرقمنة المتوفرة لدينا ويوفّر لها الحماية اللازمة، فإن طبيعة الرّقمنة هي التي تفرض علينا النصوص التشريعيّة الواجب تطبيقها في مجالي التنظيم والحماية.

إن التفاعلات السابق تحليلها تتمظهر في نتائجها بواحد من الأشكال الثلاث الآتية:

أولا: الحالة الإيجابية: هنا تتوجه بُنى المنظومة من خلال تفاعلاتها نحو تحقيق غاية المنظومة شدة واتجاها.

ثانيا: الحالة السلبيّة: هنا لا تتوجه بُنى المنظومة نحو تحقيق غاية المنظومة من خلال تفاعلاتها لكنها لا تتوجه نحو عرقلتها أيضا، فهي تفاعلات محايدة في محرّكاتها إذ لا تُحرّكها مقاصد لا مؤيّدة ولا مُعارضة لغاية المنظومة، لكنها في ذات الوقت تفاعلات سلبيّة في حركاتها لأنها تستنزف موارد المنظومة ولا تؤدي الدور الذي أنشِأت لأجله.

ثالثا: الحالة العدائية: هنا تتوجه البنيات عبر وظائفها نحو ضرب غاية المنظومة مباشرة.

1-4-2- **التحليل التفاعلي الخارجي لمنظومة الاقتصاد الرقمي:** يُعني التحليل التفاعلي الخارجي بالتفاعلات الواقعة بين المنظومة ومحيطها

أولا: الحالة الإيجابية: هنا تتوجه منظومة الاقتصاد الرقمي بأكملها، ومن خلال تفاعلها مع محيطها نحو تحقيق غاياته شدةً واتجاهًا بصفتها واحدة من بُناه.

ثانيا: الحالة السلبيّة: هنا لا تتوجه المنظومة نحو تحقيق غايات محيطها من خلال تفاعلها معه لكنها لا تتوجه نحو عرقلتها أيضا، فهي تفاعلات محايدة في محرّكاتها إذ لا تُحرّكها مقاصد لا مؤيّدة ولا مُعارضة لغاية المحيط، لكنها في ذات الوقت

تفاعلات سلبيّة في حركاتها لأنها تستنزف موارد المحيط ولا تؤدي الدور الذي أنشِأت لأجله.

ثالثا: الحالة العدائية: هنا تتوجه المنظومة عبر وظائفها نحو ضرب غايات المحيط مباشرة.

1-5- **تحليل المخرجات (Outputs):** تتفاعل مدخلات منظومة الاقتصاد الرقمي عبر سيرورة داخلية فتعطي نتائج آنية في شكل المخرجات التالية:

- **السلع:** وتختلف بإختلاف موقع تكنولوجيا الاعلام والاتصال ضمن منظومة الاقتصاد، فإن كانت من ضمن الأصول، كان المنتج رقمي بحت، سواء مصنع (جاهز للاستعمال) أو نصف مصنع (جاهز ليكون عنصر لتصنيع منتج آخر)، أما إن كانت مجرد وسيلة، فإنها تسهل الحصول على المنتج بنجاعة أكبر وتكلفة أقل .
- **الخدمات:** وتختلف هي الاخرى بإختلاف موقع تكنولوجيا الاعلام والاتصال، فقد تكون هذه التكنلوجيا موضوعا للخدمات وموجهة مباشرة للجمهور، كأنظمة الفحص والحماية للاجهزة أو خدمة البريد الالكتروني أو استضافة المواقع، وقد تكون تكنولوجيا الاعلام والاتصال أداة مسهلة لخدمة موجودة مسبقا، كالعمليات البنكية.

1-6- **تحليل العوائد (Outcomes):** يتحكّم كم وكيف المخرجات في مستوى العوائد التي تُقاس بدرجة قربها أو بعدها من غاية المشروع الاقتصادي والمتمثلة في تحقيق الرفاه الاقتصادي الذي تشير أغلب الكتابات عنه أنه يتحدد من خلال مؤشرات الصحة، التعليم، الانفاق والأمن لدى الفرد.

1-7- تحليل الأثر (Impact) : تستمد منظومة الاقتصاد الرقمي مدخلاتها من محيطها، كما تستمد مبررات وجودها، استمراريتها وريادتها من نفعيّتها له والتي

تتجلّى في الأثر الممتد لعوائدها عليه، فالمنظومة الاقتصادية التي تحقّق الرفاه الاقتصادي المنشود، تساهم بالنتيجة في تحقيق الرّفاه الإنساني في المحيط الذي تتموقع فيه، لكن في حالة عجز الاقتصاد الرقمي عن تحقيق غايته فإنّه لن يكون له الأثر الإيجابي على محيطه وبالتالي يفقد أسباب وجوده واستمراره.

1-8- خلاصة التحليل: من تحليلاتنا المنظومية السابقة توصّلنا إلى أن الرقمنة بقدر ما تعطينا السرعة والاحتراف، بقدر ما تفتح الثغرات على أمن المنظومة التي تتبنّاها، خصوصا بالنظر إلى **الفجوة الرقمية** القائمة بين المجتمعات وبين طبقات المجتمع الواحد، وفيما يأتي نعرض أكثر نقاط ضعف منظومة الاقتصاد الرقمي التي تتوزع عبر المحطّات التالية:

أولا: على المستوى البنائي: إن عدم قدرة المؤسسة الاقتصادية على امتلاك أحدث تكنولوجيات المعلوماتية والاتصال، سواء لأسباب ماديّة أو بشريّة، يجعلها عرضة لأشكال الخطر الرقمي من طرف أولئك الذين يمتلكونها، سواء كانوا أفرادا أومؤسسات، وهنا لا نجد إلا "قيم المنافسة الشريفة" على مستوى المؤسسات و"السلوك الرقمي السّوي" على مستوى الأفراد يليها "إستصدار تشريعات إحترازية وأخرى رادعة" كضمانات لحماية بنية المؤسسة.

ثانيا: على مستوى التفاعلات الداخلية: تتوقّف مُخرجات المؤسسة الاقتصادية الرقمية على نواتج التفاعلات القائمة داخليا بين مدخلاتها، وأشكال النواتج المُقلقة هنا تظهر حينما تكون الموارد الرقمية غير مناسبة لبلوغ أهداف المؤسسة، أوعندما لا تتمتع النصوص التشريعية بالمرونة الكافية لاستدخال أحدث التكنولوجيات وتنظيم استخدامها وفق أهداف المؤسسة، كما أن العنصر البشري غير المؤهّل، أو غير المؤمن بأهداف مؤسسته سيأخذ مسارا مُعاكسا لها.

ثالثا: على مستوى التفاعلات الخارجية: إنّ منظومة الاقتصاد الرقمي تستقبل فيما تستقبله من محيطها عددا من المخاطر والتهديدات التي قد تسبب لها الضرر الجزئي أو الانهيار الكلّي، وقد تُستغَلّ الرقمنة ذاتها في ضرب أهداف المؤسسة، بينما يعجز الإطار التشريعي الوطني أو الدولي سائر المفعول على حمايتها. وهنا تظهر أهميّة النهوض بالمجتمعات إلى مستوى المواطنة العالمية حيث تقف الأخلاق مانعا داخليا لمن يفكّر في ممارسة الجُرم الرقمي، ثم تظهر أهمية تطوير آليات السياسات الجنائية التي تقف رادعا خارجيا لمن تحرر من المانع الداخلي.

مما سبق يتّضح أن توليفة (المنع والردع) تضمّ تحت غطائها أغلب آليات الحماية الممكنة للاقتصاد الرقمي. في الأسطر القادمة سنعرض مدخلين متكاملين من أجل مواجهة الخطر الرقمي سواء إستباقا أوردعا، يتمثل المدخل الأوّل في توظيف قيم المواطنة من أجل تربية جيل متمدّن حضاري يزدري السلوكات المنحرفة ويعي عواقب الجُرم الرقمي على وطنه ومحيطه العالمي قبل وقوعه، أما المدخل الثاني فهو المدخل القانوني الذي يسطّر الإجراءات الاحترازية والردعية لمجازاة مرتكب الجُرم الرقمي بعد وقوعه.

2. مداخل المواطنة الرقمية في حماية الاقتصاد الرقمي:

إن مختلف التعريفات اللغوية لم تحدد معايير المواطنة المُثلى، فيما ظل يتطوّر هذا المفهوم اصطلاحا بتطور القوانين والحياة السياسية خصوصا، لذلك فهو مفهوم قانوني سياسي بالدرجة الأولى، وبالرغم من أن المواطنة تحددها القوانين والتشريعات السائدة في المجتمع، لكن قناعات المواطن تبقى محتفظة بتأثيرها وفي أحيان كثيرة نجد أن المواطن يجتهد في تصيُّد ثغرات القانون أكثر مما يجتهد في فهم القانون نفسه، فكل مواطن يمارس مُواطنته على شاكلة قناعاته ما دام خارج طائلة

الردع والتجريم، والحلقة الأبرز هنا هم الشباب، ففي كثير من المجتمعات هم فئة شديدة الذكاء غزيرة الطاقة كثيرة الابداع قليلة الفرص. فئة تحلم بالتغيير فتصطدم بالواقع لتنقسم إلى صنفين، الأول مُحبَط مُنسحب، والثاني ناقمٌ متمرّد.

وبعد ظهور "الثورة الرقميّة" مُقتحِمة كل مناحي الحياة الإنسانية، وجد صنف الناقمين المتمرّدين في العالم الرقمي ملاذا لهم، أين لا حدود ولا قيود، فأينما وصل نشاطهم الرقمي فذلك وطنه، وكلّ ما طالته حيلهم الرقميّة فذلك حق لهم في الوقت الذي ظهرت حركة المجتمعات الرسميّة بطيئة في الاستجابة للوضع الجديد[8]. ومن هنا ظهرت الحاجة إلى البحث في مداخل "المواطنة الرقمية" لحماية عالمنا الواقعي من المآسي القادمة عليه من العالم الافتراضي. تلك القيم تتوزع على تسعة محاور أساسية بحسب كل من "Mike Ribble, Gerald bailey"[9] صاحبَيْ أهم مؤلّف في مجال المواطنة الرقمية لحد الآن. وفيما يلي سنبيّن مداخل المواطنة الرقمية في حماية منظومة الاقتصاد الرقمي ومساعدتها على تعظيم عوائدها ثم تحقيق أفضل الأثر على محيطها وفقا لتلك المحاور:

- **محور الثقافة الرقمية:** تعتبر الفجوة الرقمية من كبرى تحديات الاقتصاد الرقمي، لذلك فإن "محو الأميّة الرّقمية" من أولى الخطوات في تنشأة المواطن الرقمي الصالح، حيث نُمكّنه من معرفة مختلف أشكال تكنولوجيات المعلوماتية والاتصال الموجودة وندرّبه على كيفية استخدامها بالشكل الصحيح، حتى لا

8 في دراسة سابقة لنا أجريناها سنة (2013) بعنوان تقييم محتوى كتب التعليم الجزائري في ضوء متطلبات تربية المواطنة (دراسة تحليل محتوى في كتب التربية المدنية)، وجدنا أن قيم المواطنة بمفهومها التقليدي الضيّق حاضرة في المرتبة الأولى من حيث الكثافة، بينما قيم المواطنة العالمية ضئيلة نسب حضورها (الانفتاح على الثقافات الأخرى≅ 00.04%- النزاهة ≅00.04%) لأن وصلت درجة الصفر فيما تعلق بقيم احترام الأديان ونبذ العنصرية.

9 Mike Ribble, Gerald bailey (2015): Digital Citizenship in Schools, Third Edition, International Society for Technology in Education (ISTE), Washington.

يُسيء استخدامها من جهة، ثم حتى لا يكون ضحيّة لمن يسيئون استخدامها من جهة أخرى.

- **محور الوصول الرقمي:** المواطنة الرقمية الفارهة تتطلب تكافؤ فرص أفراد المجتمع في الوصول إليها، بغض النظر عن مستوياتهم التعليمية أو الماديّة، وهنا على الدولة أن تحرص على إتاحة الوصول الرقمي الآمن لكافة مواطنيها بأحسن شكل، على أوسع نطاق وبأقل التكاليف الماديّة والتعقيدات البيروقراطية، و ديمقراطية الوصول الرقمي هي من أهم آليات القضاء على الأميّة الرقمية في المجتمعات التي تطمح إلى التقدم.

- **محور قواعد السلوك الرقمي:** بما أن العالم الرقمي "وطن" ومن يستخدم الرقمنة يعتبر "مواطنا رقميّا" فيه، فإن للعيش في هذا الوطن أخلاق وآداب لا بد للمواطن أن يتحلى بها حتى يكون مُحترما ويحفظ للآخر حُرمته، ومن معايير السلوك الرقمي الصحيح نذكر على سبيل المثال احترام خصوصية النفس والغير، الالتزام بآداب الحوار، احترام حقوق التأليف والنشر، التأكّد من صحة المعلومات قبل نشرها، وفي هذا السياق ظهر حديثا "علم النفس الرقمي" الذي يمكنّنا من علاج السلوكات الرقمية غير السويّة على مستوى العالم الافتراضي، حيث يلتقي المُعالِج وطالب العلاج كمواطنين رقميين في وطنهما الرقمي، ورغم حداثة هذا التخصص إلا أنه بدأ يجني ثماره الطيبة في مجال تهذيب السلوك الرقمي.

- **محور الصحة و الرفاهية الرقمية:** المواطنة الرقميّة كما تُعنى بحماية المنظومات الرقمية من تهديدات العنصر البشري، فهي تُعني أيضا بحماية العنصر البشري من مخاطر "الحياة الرقميّة"، وذلك من خلا تدريبه على

استخدام التكنولوجيات المتطورة بالشكل المعقول المسؤول حفاظا على وقته وصحّته، وتوعيته بآثارها السلبية على صحته وعلاقاته الاجتماعية.

- **محور التجارة الرقمية:** كما تهتم المواطنة الرقمية بحماية الاقتصاد الرقمي، فهي تهتم أيضا تهتم بحماية المستهلك الرقمي أثناء عمليات البيع والشراء من خلال تعريفه بأساليب التأكد من: صحة العرض التجاري، سلامة المحتوى المعروض وقانونيته، سلامة الأرضية الرقمية محل الدعوة للتعاقد. ثم تدريبه على التعامل مع المواقع التجارية الموثوقة وعدم الاندفاع وراء العروض الاشهارية.

- **محور الاتصال الرقمي:** الاتصال الرقمي حق مكفول قانونا لكل مواطن، إذ له الحق في تلقي وإرسال المعلومات بمختلف أشكالها في حدود ما يسمح به القانون ووفق ما تحدده الحقوق والمسؤوليات في هذا المجال، ويتحقق هذا الاتصال عبر وسائل وأجهزة الاتصال الرقمي، مواقع وتطبيقات الاتصال، المسموعة، المرئية والمقروءة، ولا يمكن منعها، حضرها أو حجبها إلا بموجب نصوص قانونية. كما أنه يمنع اعتراض المراسلات، تسجيلها ومراقبتها إلا بموجب إذن صادر من الجهات المخوّلة بذلك قانونا وغالبا ما تكون السلطة القضائية (مكلفة بحماية الحريات). لكن بالمقابل علينا أن ننشر الوعي بضرورة الاستخدام الواعي والمسؤول لتقنيات الاتصال الرقمي، تفرض تحمل المسؤولية الاخلاقية والقانونية الكاملة لما قد يرتبه مضمون الاتصال، وإذا كان المستفيد من الخدمة قاصرا، أو تابعا لجهة معينة، فيجب أن يلتزم بقواعد الاتصال المفروضة من قبل الجهة متولية الرقابة.

- **محور الحقوق والمسؤوليات الرقمية:** توفر الرقمنة جملة من المزايا والحريات لمستخدمي تكنولوجيا المعلوماتية، لكن علينا أن نربي الوعي لدى

مواطنينا بضرورة معرفة حقوقهم ومسؤولياتهم المترتبة على استخدامها، سواء في النصوص القانونية المحلية الخاصة بالدولة مكان الاتصال، أو تلك الخاصة بالدولة مستضيفة للموقع محل النفاذ، وكذا البنود المتعلقة بسياسة الاستعمال لكل موقع. فمعايير السلوك السوي في استعمال تكنولوجيا المعلوماتية تفرض علينا احترام حقوق الملكية الفكرية، مع إمكانية نشر الآراء والمنتجات الفكرية والعلمية الشخصية بمقابل أو بدونه.

- **محور الأمن الرقمي**: علينا أن ننمي لدى مواطنينا حسّ اليقظة الأمنية الرقمية، بهدف ضمان سلامة برامجهم، أجهزتهم ومعلوماتهم الشخصية، وذلك من خلال التأكيد على ضرورة استعمال النسخ الأصلية والمضمونة من البرامج والاجهزة كخطوة أولى، ثم الاستعانة ببرامج الحماية من الفيروسات، الاختراق، التجسس وغيرها من عمليات الاعتداء الرقمية المباشرة أوغير المباشرة التي غالبا ما يكون للضحية يد فيها من خلال الافصاح عن معلوماته الشخصية للغير، نشرها للجمهور أو منحها بعد إغوائه عبر الرسائل والحملات الاشهارية الوهمية.

- **محور القانون الرقمي:** علينا أن ننشر بين مواطنينا القدر الكافي من الوعي بالقانون الرقمي، إذ يتضمّن الحقوق الرقمية وتنظيم المجال لضمان عدم تداخل المصالح، وحمايتها من كل اعتداء، فمن خلال النصوص القانونية يتم ضبط أغلب مختلف محاور المواطنة الرقمية، وأية مخالفة لذلك تترتب عليها عقوبات وفق النصوص الاجرائية والموضوعية المحددة في هذا المجال بهدف ضمان الأمن والاستقرار في العالم الرقمي.

3. الحماية الجنائية للاقتصاد الرقمي:

يعادل الإقتصاد الرقمي ثلث اقتصاد دولة الصين الشعبية، وفق ما أعلن عليه خلال المؤتمر العالمي الرابع للإنترنت في مدينة ووزن الصينية المنظم من قبل

الأكاديمية الصينية لدراسات الانترنت، حيث بلغ الاقتصاد الرقمي الصيني (3,4 ترليون دولار) في 2014، ومن المتوقع أن ينمو سوق أمن قاعدة البيانات دوليا من 2.95 مليار دولار أمريكي في عام 2017 إلى 7.01 مليار دولار أمريكي بحلول عام 2022، بمعدل نمو سنوي مركب يبلغ 18.9٪ خلال فترة التوقعات (Sam Park and al. 2014) ، وهو ما يدعو الإستثمار في المجال الرقمي، وفي إحصائيات نشرتها مجموعة المشاريع الاستراتيجية،[10] فإن تطور الاستثمار في مجال الامن الرقمي يحتل الصدارة بنسبة 63٪ لسنة 2018.

إن تطور الدول والمؤسسات يعتمد في الوقت الراهن أساسا على إنشاء بنية تحتية رقمية، هذا الإنشاء لا يكفي، بل يجب حمايته من خلال نظام أمني، اقتصادي، وقانوني متكامل، فالدول حاليا ملزمة بتأطير وتنظيم الصيرفة الرقمية والبنوك الافتراضية وكل ما تعلق بالإقتصاد الرقمي من خلال ما لها من صلاحيات في إصدار القوانين داخليا، وفرض سيادتها على هذا المجال دوليا، أما المؤسسات الاقتصادية فبإمكانها المساهمة في الحماية من خلال الاستعمال السليم والحذر لتكنلوجيا المعلوماتية، أو من خلال انشاء شركات اقتصادية متخصصة في المجال الرقمي تستجيب للمعايير الدولية والأطر القانونية الخاصة.

إن الإعتداء الرقمي لا يقتصر على المؤسسات الإقتصادية الخاصة بل قد يمتد الى المؤسسات السيادية ومثاله ما حدث سنة 2012 لعملاق الطاقة في منطقة الشرق الاوسط، وتحديدا شركة Aramco **(Robert Mandel.2014)** من اختراق وعبث ببرامجها وأجهزتها، وتختلف أشكال الإعتداء الرقمي، فقد يكون اعتداء مباشر على نظام الي لمعالجة المعطيات او اعتداء على منشئات باستعمال المعلوماتية، كما قد يكون من خلال توفير الخدمات و المنتجات غير الشرعية، أو توفير الخدمات

[10] Enterprise Strategy Group: http://www.esg-global.com/

والمنتجات القانونية بطريقة غير شرعية، ونجد أن أدق تعريف للجريمة المتصلة بتكنولوجيا المعلوماتية هوما قدمه د. مارتن والذي اصطلح على هذا النوع من الجرائم مصطلح الجريمة ذات التقنية العالية، فعرفها على انها تلك الجريمة التي تغطي جميع الأفعال غير المشروعة للإهتمام بتكنولوجيا المعلومات والإتصالات من حيث الأجهزة والبرمجيات**(Chawki Mohamed.2006)**.

وعليه وللحيلولة دون وقوع هذا الصنف من الجرائم من الأفضل اتخاذ جميع الاحتياطات اللازمة، باعتماد أحدث الوسائل التقنية والبرامج، ثم اتباع الإجراءات الإحترازية، أما في حال وقوع الإعتداء أو السلوك الإجرامي فيجب التدخل بالأساليب الناجعة والكفيلة بتوقيف الجاني وتحديد أسباب فشل نظام الحامية وتطويره. ونقصد بالإجراءات الإحترازية، مجموع الإجراءات التي تسبق السلوك الإجرامي والتي تهدف أساسا إما لمنع وقوعه وهنا تسمى بالإجراءات الاحترازية الوقائية، أو أنها تهدف إلى الحفاظ على النظام وكذا الأدلة في لحظة التعرض للإعتداء وتسمى هنا بالإجراءات الإحترازية التحفظية، ويمكن ذكر أهم هاته الإجراءات في ما يلي:

- **تكوين وتطوير المستخدمين والشركاء:** ويستهدف هذا البند العنصر البشري بإعتباره العنصر الأساسي في الإقتصاد الرقمي، وبغية بناء استراتيجية وقائية فعالة في مواجهة الإجرام الرقمي يجب التركيز على نقطتين أساسيتين خلال أي عملية تكوين أو تطوير لمهارات العنصر البشري **(الأمانة العامة لمؤتمر الامم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية. 2014)**، أولهما بناء قاعدة معرفية مفصلة حول الرقمنة والإقتصاد الرقمي، على الأقل ضمن مجال تخصص المؤسسة، وثانيهما توضيح العوامل الإجرامية المسهلة والأنماط السائدة في مجال الاجرام الرقمي.

- **الحماية للأجهزة والبرامج:** يعتقد العديد أن الدخول غير المصرح للأنظمة والشبكات يكون عن طريق القرصنة او اختراق الشبكات، لكن أغلب الإحصائيات العالمية تؤكد أن ذلك يتم من خلال حسابات موجودة فعليا، تم الاستحواذ عليها نتيجة سرقة بيانات اسم المستخدم وكلمة المرور أو ما يسمى بسرقة الهوية، ويعتمد المجرم في ذلك على اسلوب "التصيد"[11]، أو أسلوب "الهندسة الإجتماعية"[12]، هاته الاساليب تستهدف المستخدمين مباشرة وكذلك الشركات، ومن خلال الحساب محل السرقة يصبح بإمكان الجاني الوصول الى المعلومات الخاصة بالشركة وربما إدخال تعديلات عليها، لذا يجب اعتماد كلمات سر معقدة، خاصة لكل حساب، والعمل على تغييرها دوريا، إضافة الى اعتماد أنظمة التشفير في التواصل الرقمي خصوصا المعلومات الهامة، كما يمكن استخدام أنظمة إخفاء البيانات، وهي أنظمة تختلف عن التشفير، ويقصد بها تضمين المعلومات السرية ضمن أخرى غير سرية، ولا يمكن كشفها إلا عن طريق استعمال نفس أداة التضمين، هذا فيما يخص الحفاظ على سرية وسلامة المعطيات، أما إذا أردنا التحقق من هوية الموظف أو الشريك أو الجهة المنشئة للمستند الرقمي فيجب تفعيل أنظمة التوقيع الالكتروني بمختلف أشكالها، ويجب في كل الحلات استخدام أنظمة الجدار الناري، لمنع نفاذ الجهات غير المرخص لها.

- **وضع خطط أمنية رقمية وأنظمة آلية إحتياطية:** وليس المقصود هنا هو الاعتماد على البرامج وأنظمة الشبكات العالمية، إنما المقصود هو إنشاء نظام أمني داخلي خاص بالمؤسسة، يعتمد أساسا على العنصر البشري المؤهل ويؤخذ بعين الاعتبار شبكة الربط الداخلية وكذا الخارجية، حيث يقوم على الفحص الدوري والمستمر لتكاملية وسلامة المحتوى، واستمرارية الخدمة الرقمية، وفي حال

[11] **Phishing**

[12] **Social Engineering**

اكتشاف اي اعتداء أو خرق لأنظمة الحماية، فإنه يعمل على عزل الوحدة محل الإعتداء مع الحفاظ على السير العادي للنظام ككل داخل المؤسسة، أما في حال عدم التمكن من حصر محل الإعتداء أو عدم اكتشافه في الوقت المناسب، فيمكن اللجوء الى أنظمة احتياطية توفر الحد الأدنى من الخدمة.

- **التوثيق لجميع العمليات الرقمية بطريقة تمكن من المراجعة و الإسترداد:** ويكون ذلك من خلال إنشاء وتفعيل السجلات الرقمية الخاصة بنظام التشغيل وقواعد البيانات وكذا أدوات الحماية الرقمية، غالبا ما تحدد هذه السجلات الجهة المستخدمة، تاريخ ومكان وجهاز النفاذ، طبيعة العملية – انشاء، حذف، تعديل – وكل ما يتعلق بأي عملية او اعتداء على البنية الرقمية للمؤسسة، هذه السجلات يجب أن تحفظ على الأقل لمدة سنة نظرا لدورها البالغ الأهمية في حال وقوع أي اعتداء أو في حال التحقيق في احتمال وقوع اعتداء لم يكتشف في حينه، فهي أداة فعالة ضمن التحليل الجنائي الرقمي[13]، كما أنها تعتبر دليل رقمي[14] يستخدم في التحقيقات القانونية.

- **إنشاء ارشيف رقمي معزول ومحمي:** في عملية دورية، تحال المعطيات والسجلات الرقمية غير المستعملة على الأرشيف، ليتم حفظها لأطول مدة ممكنة، بعيدا عن البيئة الرقمية المفتوحة، وبالتالي لا تكون محلا للتعديل أو الحذف أو التلف، تعتبر هي الأخرى دليل رقمي يستعمل في التحقيقات القضائية ما اذا تم حفظها وفق الطرق التي تضمن سلامتها.

- **حفظ الأدلة طبقا للقوانين الإجرائية والموضوعية:** إن التوثيق للعمليات الرقمية، وحفظ المعلومات والسجلات والأدلة سوآءا بشكل مؤقت أو في شكل نهائي (أرشيف) لا يكفي لتكوين دليل كامل أمام الجهات القضائية، بل يجب

[13] Digital Forensics.

[14] Digital Evidence.

توافر ضمانات كافية تؤكد سلامة المعطيات، ويختلف الحد الأدنى لهذه الضمانات من دولة إلى أخرى، تشمل هذه الضمانات سلامة الدعامة الحاملة للدليل الرقمي وكذا الدليل الرقمي ذاته من أي تعديل أو تحريف، وهو مجال في تطور مستمر بسبب ارتباطه بالعالم الرقمي الإفتراضي يطلق عليه اسم الطب الشرعي الرقمي[15].

- **اللجوء الى التأمين من مخاطر التكنلوجيا الرقمية:** بينما تدرس دول إعتماد تكنولوجيا المعلوماتية كوسيلة مسهلة لعملها الكلاسيكي، تسعى أخرى الى الترويج إلى منتج جديد، يهدف إلى الحماية من مخاطر العالم الإفتراضي وسمي أيضا بالتأمين من مخاطر الرقمنة[16]، يهدف الى تغطية مجمل التكاليف المترتبة بسبب الأضرار الناتجة عن سوء استعمال المعلوماتية، ومثاله ما تم إنشاؤه من قبل مجموعة من المبدعين ببريطانيا تحت اسم (Digital Risks)، وبالتالي فإن التأمين عن المخاطر المعلوماتية فرصة جديدة ومجال استثماري خصب بالنسبة لشركات التأمين، لاسيما في ضل توسع التجارة الإلكترونية.

كل ما سبق ذكره يهدف أساسا إلى منع وقوع السلوك الإجرامي على الاقتصاد الرقمي، أما وفي حال وقوع الإعتداء فيجب اتخاذ مجموعة من الإجراءات تهدف أساسا إلى توقيف الجاني لنيل ما يستحقه من جزاء وتسمى هاته الإجراءات بالإجراءات الردعية، وعادة ما تحتفظ الدولة بحقها في المتابعة الجزائية ضد المشتبه فيهم وكذا بحقها في توقيع العقاب بعد صدور حكم الإدانة، إلا أن ذاك لا يعفي المؤسسات الإقتصادية من لعب دورها ضمن الإجراءات الردعية، بل غالبا ما تكون الإنطلاقة من هاته المؤسسات وذلك من خلال إجراء التبليغ عن الأخطار و الإعتداءات الواقعة أو المحتملة، كما أن مد يد المساعدة التقنية والفنية للجهات

[15] Scientific Working Group on Digital Evidence: www.swgde.org

[16] Insurance Digital Risks.

الأمنية والقضائية من شأنه تسريع التحقيق وبالتالي الوصول إلى الجاني قبل تلف الأدلة، وعلى الجهة محل الإعتداء تشكيل لجنة داخلية، أمنية-تقنية، تتولى مهمة مرافقة الأجهزة الأمنية والقضائية ومد يد المساعدة خلال مجريات التحقيق لاسيما في ما يتعلق بحجز المعطيات الكامل أو حجز المعطيات عن طريق منع الوصول، ويمكنها من خلال ذلك تحديد أسباب وقوع الإعتداء، وإعطاء الحلول الجذرية والناجعة له. والجدير بالذكر هنا أن السياسات الجنائية الحديثة تسعى إلى محاولة التعرف على شخصية الجاني وبحث أسباب ودوافع ارتكابه للجريمة، فقد يكون الاعتداء من باب العبث أو التحدي، مثل ما يقوم به أغلب الهاكر (أصحاب الياقات البيضاء)، فمثل هذا العنصر يجب احتوائه، وهنا نرى بأن لضحية الإعتداء الأولوية في الاستفادة من الجاني.

قائمة المراجع:

ناني لحسن (2014): **التحقيق في الجرائم المتصلة بالتكنولوجيا المعلوماتية**، دار الناشر الجامعي الجديد، تلمسان، الجزائر.

ناني لحسن (2014): **"فعالية بديل العقوبة في استثمار وجدان الهاكرز"**، مقال في طور النشر في كتاب المؤتمر الدولي العاشر حول "مكانة الوجدان في علم النفس الحديث" المنعقد يومي 29-2018/01/39 من طرف وحدة البحث في تنمية الموارد البشرية بجامعة سطيف2، الجزائر.

ناني نبيلة (2013): **تقييم محتوى كتب التعليم الجزائري في ضوء متطلبات تربية المواطنة (دراسة تحليل محتوى في كتب التربية المدنية)**، عالم التربية، العدد الرابع والأربعون، الجزء الثالث، السنة الرابعة عشر، دورية علمية محكمة تصدرها المؤسسة العربية للاستشارات العلمية وتنمية الموارد البشرية بالتعاون العلمي مع المركز القومي للبحوث التربوية والتنمية ورابطة التربية الحديثة، القاهرة.

ناني نبيلة (2014): "**المواطنة بين القومية والعالمية-مقاربة منظومية-**" ورقة بحث مقدمة في الملتقى الدولي الثامن حول "المواطنة والتنمية" المنعقد بتاريخ 14-15/ 04/ 2014 بوحدة البحث في تنمية الموارد البشرية بجامعة سطيف2، الجزائر.

1. **Lahcene Bouabdellah, Ahmed Nani, Nabila Nani, Houda Kherbache** (2012)**: Systemic analysis technology. The case of systemic analysis,** http://library.iated.org/view/BOUABDELLAH2012SYS
2. **Chawki Mohamed (2006): Essai sur la notion de cybercriminalité.** http://www.legalbiznext.com
3. **Karen Mossberger, Caroline J. Tolbert and Ramona S. McNeal** (2008)**: Digital Citizenship:** The Internet, Society, and Participation (MIT Press), Massachusetts institute of technology, London.
4. **Mike Ribble, Gerald bailey** (2015): **Digital Citizenship in Schools,** Third Edition, International Society for Technology in Education (ISTE), Washington.
5. **Robert Mandel** (2014): **Optimizing Cyber deterrence, A Comprehensive Strategy for Preventing Foreign cyberattacksm,** Georgetown University Press. Washington-USA.
6. **Sam Park, Dr. Anton Grashion, James Taylor** (2014)**: Cybersecurity in Renewable Energy Infrastructure.** The Renewables Consulting Group Ltd. Gilmoora House - London - United Kingdom. www.thinkreg.com
7. **Stephen Devlin (2017): Inequality in the Digital Society,** http://neweconomics.org/wp-content/uploads/2017/01/Inequality-in-the-Digital-Society-Workshop-Summary-v2.pdf