

## حماية الخصوصية الالكترونية للمستهلك في التشريع المغمربي



**بدر الدين الالءوءى:** طالب باء بسلء الءءءواء  
كلية العلوم القانونية والاقتصادية والاجتماعية بمكناس

### ملءءة:

إن السؤل الءوءرى الءى ءطرءه الءوم ءءنولوجيا المعلوماء الءءءة على رءال القانون ىءمءل بالأساس فى ءءءءء مءاطر الءصوصية الءى ءسببها للإنسان، فىإلاء الإءار الزمكاني للعالم ونقله إلى آءر افءراضى، فإن هءه الءءنولوجيا ءعرضه من ناحية للعىش فى وهم الشفافىة، وباءراء أبسط ءركاءه وسكناءه فى الآلاء، فإنها ءءل منه من ناحية أخرى عرضة لاءءهاء الءصوصىة<sup>1</sup>.

وبعء الءءء عن الءصوصىة بصفة عامة<sup>2</sup>، والءءمس فى الءءوة إلى ءءصىنها، ومعااءة الأصواء الءى ءسءهءنها من الأمور القءىمة، فقء "بءأ الوعى بءظورة الءاسب على ءرمة الءىاة الءاصة فى الءول الغربىة منذ ما ىزىء عن أربعىن سنة، ءىء ءعالت صىءاء ءما هءه الءىاة لمواءه مءاطر المءالءة الآلىة للبىاءاء الاسمىة لاسىما فى فرنسا"<sup>3</sup>، على أن ملامء المءاطر المءءءة لهذا الكىان لم ءبرز بشكل ءلى إلا مع عصر الألفىة الءالءة بما ءمله من ءغىراء ءءرىة، فقء أصبءء الءءنولوجيا الرقمىة طاعىة على مءءلف أوءه ءىاءنا الءومىة واكءسءء ءمىع المءالاء، كما ءعءء اسءعمالها ءاصة فى مىءان الءءارة.

إن هءا الءكامل والءفاعل الءى ءصل بىن الاءءرنء والءءارة ءءن لءقبه اقءرب فىها العالم من بعضه بعضا، من ءلال ما أءاءه من فرص رىط مباءر بىن المءاوله ومءءلف المستهلكىن<sup>4</sup>، مما ىسر من مهمة القىام بعملىاء الءسوق

1- آلان سوبىو، ءرءمة عاءل عبء الناصر، الإنسان القانونى، بءء فى وظىفة القانون الأءروبولوجىة، الطبعة الأولى، المنظمه العربىة للءرءمة، لبنان، سءنبر 2012، ص 235.

2- الءق فى الءصوصىة بصفة عامة ىنصب على مقوماء وعناصر الشءصىة فى مءءلف مظاهرها الطبىعىة والمعنوىة، الفرءىة والاجتماعىة، بءىء ءعبىر عما للشءص من سلطاء مءءلفة على هءه المقوماء وعلى ءلك العناصر بقصد ءنمىة شءصىة المرء. أما ءصوصىة المعلوماء فقء عرفها ( Alan Weston) بأءها "ءق الأفراد فى ءءءء مءى وكىف وإلى أى مءى ءصل المعلوماء المءعلقة بءم للآءرىن"، أما ءعرىف مىلر فقء ءاء أكءر شمولىة بءىء قال بأنه ىءىل على "قءرة الأفراد على الءءكم بءورة المعلوماء الءى ءءلق بءم. للمزىء ءول هءا الشآن ىنظر بن سعىء صبرىنة، ءماىة الءق فى ءرمة الءىاة الءاصة فى عهد الءءنولوجيا "الإعلام والاءءال"، أطروءة لنىل شءاءة الءءءواء فى العلوم القانونىة، كلية الءقوق والعلوم السىاسىة، ءامعة الءاء لءضىر، باءنة، 2014-2015، ص 123.

3- ولىء العاكوم، مفهوم وظاهرة الإءرام المءلوماتى، بءء مؤءمر القانون والكومبىوئر والاءءرنء، المءلء الأولى، الطبعة الءالءة، 2004، ص 16.  
4-Sisira NETI, Social Media and Its Role In Marketing, International Journal Of Enterprise Computing and Business Systems, Vol 1, July 2011, p 1.

الكترونيا، وعرض المنتجات على نطاق واسع، "إلا أن الجانب المشرق لهذا التفاعل رافقه جانب آخر متسم بالأنانية والظلمة، والاعتداء غير المشروع على قيم ومصالح مادية ومعنوية، خاصة فيما يتعلق بالخطر الكبير الذي أصبح يترتب بالحياة الخاصة للمستهلكين، ويهدد بانتهاك حرمتها وتعرية أسرارها"<sup>1</sup>، فولج الأفراد المكثف للأسواق الإلكترونية جعل المقومات الكاشفة لهويتهم تكتسي طابعا شفافا، لأن التواصل في الغالب يتم من خلال تقنية إرسال وتبادل الملفات عن بعد، وبالتالي كشف الهوية الكاملة للمستهلك<sup>2</sup>.

ولعل ما أفرز المشكلة بشكل أكبر، ذلك التنافس العنيف الذي خلقته سمات هذه البيئة الإلكترونية، والذي أوجب على المقاولات اعتماد إستراتيجيات تسويقية موجهة، حتى تتصدى لأزماتها التصريفية، وفي هذا نجد بأن الانترنت قد أضاف أدوات ووسائل جديدة للمقاولات تزيد من فرص نجاح عملياتها التسويقية، و" تعتبر عملية الحفاظ على سجلات رقمية للزوار ومسك ملفاتهم، إلى جانب إجراء التحاليل المتعلقة بنتائج عمليات التسويق المفتاح الرئيسي المعتمد لنجاح هذه العملية"<sup>3</sup>.

فمن خلال هذه المعطيات تستطيع المقاولات إجراء العديد من الدراسات التي تستهدف دراسة سلوك الزبناء والمستهلكين، من أجل معرفة المنتجات والخدمات التي يفضلونها، وذلك بعد ترصد وتقفي آثارهم، ومن ثم التنبؤ بقراراتهم الشرائية، حتى أضحي من الممكن الحديث على ما يمكن تسميته "بظاهرة الشعوذة الإلكترونية".

وهو ما أثبت معه العديد من المخاطر التي تهدد خصوصية الفئات السالفة، خاصة في ظل هاجس الربح الذي يحث المسوقين الإلكترونيين على ضرورة تبني إستراتيجية تسويق الكتروني تعتمد على التكنولوجيا الرقمية، للبحث عن المنتجات والخدمات المستهلكة والمطلوبة، وإيمانهم العميق بأن عدم خوضهم في عالم الانترنت سيعرضهم لفقدان فرص ذهبية، وفي أسوأ الظروف يمكن أن يتخلفوا عن ركب العديد من المنافسين الذين ما فتئوا يتقدمون عبر هوة رقمية متزايدة الاتساع<sup>4</sup>.

ولما كان القانون ظاهرة اجتماعية تفاعلية، يفترض أن تظل قادرة على تنظيم مختلف العلاقات بما يحدث فيها من تطور، بحيث لا يجوز أن يحدث تطور في ميدان من الميادين ويظل القانون بعيدا عنه، وإلا حدث فصل بين القانون والمجتمع، فصل يكون به القانون مجرد إرث قديم، ولأن مجتمعنا عرف تطورات سريعة ومتلاحقة كان للتقدم التقني والعلمي نصيب في إحداثها، فقد كان حتما على القانون أن يساير تلك التطورات لوضعها في إطار وقالب مناسب<sup>5</sup>، من هنا، كان السعي لمواءمة التشريع وسباق التطور العلمي على نحو يروم إرساء الاطمئنان في العالم المعلوماتي، حيث

- 1- طارق عثمان، الحماية الجنائية للحياة الخاصة عبر الانترنت (دراسة مقارنة)، رسالة لنيل شهادة الماستر في القانون الجنائي، جامعة محمد خير، كلية الحقوق والعلوم السياسية (قسم الحقوق)، بسكرة، 2006-2007، ص 4.
- 2- وهنا يظهر الفرق مقارنة مع التجارة التقليدية التي تسمح للزبون في غالب الأحيان بأن يحتفظ بهويته مجهولة، وذلك عبر حضوره الشخصي لأداء الثمن مقابل السلعة أو الخدمة، دون الإدلاء ببطاقة هوية، للمزيد حول هذا الشأن ينظر العربي جنان، الأنظمة المعلوماتية والانترنت بين التنظيم القانوني وأحكام لمسؤولية (النظرية والتأصيل)، أطروحة لنيل شهادة الدكتوراه في الحقوق، جامعة القاضي عياض، كلية العلوم القانونية والاقتصادية والاجتماعية، مراكش، 2009-2010، ص 249.
- 3- خضر مصباح الطيطي، التجارة الإلكترونية والأعمال الإلكترونية من منظور تقني وتجاري وإداري، دون ذكر الطبعة، دار الخادم، عمان، 2008، ص 75.
- 4- داميان رايان وكالفين جونز، التسويق الرقمي، إستراتيجية لجذب الجيل الرقمي، الطبعة الأولى، دار نخضة مصر للنشر، يناير 2014، ص 19.
- 5- خاصة وأن الأمر ارتباطا بمطعمي دستوري هو خصوصية المعطيات المتعلقة بالأفراد حيث نص الفصل 24 من دستور المملكة: "لكل شخص الحق في حماية حياته الخاصة"، كما أن الرأي العام والحكومات خاصة في الدول الغربية قد انزعج من الممارسات الأخلاقية التي مست هذه الخصوصية ودافعا باتجاه احتوائها تشريعيا.

تم تكريس الحق في الخصوصية في ثلة من الإعلانات والمواثيق الدولية<sup>1</sup>، وعلى الصعيد الوطني أصدر المشرع ترسانة مهمة من القوانين في سياق انفتاحه على المعطيات الجديدة للمجتمع الرقمي<sup>2</sup>.

من خلال ما سبق يتضح أن الإشكالية التي تطرح نفسها تتحدد في ماهية أبرز السبل القانونية التي وضعها المشرع المغربي لحماية الخصوصية الإلكترونية للمستهلك من مختلف المخاطر المترتبة بها في عصر التجارة الإلكترونية؟ للإحاطة بهذه الإشكالية، وسعياً نحو ضبط الموضوع أكثر، ستقتصر عناصر الإجابة على تناول الحماية التي وفرتها المشرع الوطني للخصوصية الإلكترونية للمستهلك من مختلف المخاطر التي خلفتها التجارة الإلكترونية (ثانياً)، لكن قبل ذلك لابد من بيان أبرز هذه المخاطر (أولاً).

## أولاً : المخاطر المهددة للخصوصية الإلكترونية للمستهلك

ترتكز المقاولات في حملاتها التسويقية إلى حد كبير على مدى توافر المعلومات المتعلقة بالمتغيرات البيئية المحيطة بها-أي بالمقولة-، لاسيما تلك المتعلقة بتحليل الطلب من خلال دراسة خصائص وسلوك المستهلكين<sup>3</sup>، وفي هذا نجد بأنها لم تتوار عن القيام بالعديد من الخطوات التي يمكن أن تمس بخصوصية المستهلك الذي يترك عقب كل استخدام له لشبكة الانترنت آثار ودلالات تستغل من قبل هذه المقاولات في الدراسات التي تقوم بها (ب). ولا يتوقف الأمر عند هذا الحد، بل إن الخصوصية التي يفترض أن يتمتع بها المستهلك تكون في معظم الأحيان أيضاً عرضة لعديد من الزيارات العدائية والاختراقات (أ).

### أ : انتهاك حرمة الحياة الخاصة للمستهلك الإلكتروني عبر الزيارات العدائية

لقد أصبح هذا العنوان بديهية من البديهيات، للاقتناع السائد بأن الانترنت أضحت بما لا يدع مجالاً للشك مرادفاً لانتهاك الخصوصية، خاصة وأن هذا العصر هو عصر الإجرام الإلكتروني الذي يتم عبر الاختراق المعلوماتي لحدود نظام من النظم السائدة في هذا الفضاء. فقد أضحت صناعة المعلومات تشهد من آن لآخر عمليات اقتحام عديدة، أو ما يمكن أن نطلق عليه مسمى "الزيارات العدائية"، وقد أدخلت هذه الممارسات العالم في أشكال جديدة من الصراعات الإلكترونية الشرسة التي تتم بواسطة محترفين ولم تعد قاصرة على هواة الاقتحام والتسلل<sup>4</sup>.

أما عن الصور التي تتخذها عملية الاختراق المعلوماتي لحرمة الحياة الخاصة للمستهلك الإلكتروني فهي متعددة، كما هو الشأن بالنسبة لجريمة الإطلاع على الرسائل الشخصية الموجهة عبر وإلى البريد الإلكتروني أو إتلافها، التجسس،

1- نصت المادة 12 من الإعلان العالمي لحقوق الإنسان الذي أقرته الجمعية العامة لمنظمة الأمم المتحدة سنة 1948 على أنه "لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة أو في شؤون أسرته أو مسكنه أو مراسلاته"، ونصت الاتفاقية الدولية للحقوق المدنية والسياسية لسنة 1966 في مادتها 17 على أنه "لا يجوز التدخل بشكل تعسفي أو غير قانوني بخصوصيات أحد أو بعائلته أو بيته أو مراسلاته".

2- ABDELKARIM GHALI, La protection juridique de l'échange électronique des données au Maroc à l'épreuve, revue Marocain d'administration locale et de développement, 93, juillet-Aout 2010, P : 86.

3- رشيدة بن الشيخ الفقون، دور نظام المعلومات التسويقية في اتخاذ القرار التسويقي، رسالة لنيل شهادة الماستر في علوم التسيير (اختصاص تسيير المؤسسات)، جامعة منتوري، كلية العلوم الاقتصادية وعلوم التسيير، قسنطينة، 2005-2006، ص 196.

4- محمد سمير أحمد، التسويق الإلكتروني، دون ذكر الطبعة، دار المسيرة للنشر والتوزيع، 2009، ص 286.

أأخذ صورة للمستهلكين الالكترونيين، استغلال ما حصل من أأأأأ خاصة وسرية أو صور أو رسائل عبر البريد بقصد النشر أو إأأار الغير بها<sup>1</sup>، هي في حقيقة الأمر صور كثيرة سنأأول رصد بعضها.

### أ انتأال الشخصية :

"يقصد بانتأال الشخصية قيام أأأ الأأيار باستخدام شخصية طرف أأر للاستفادة من سمعته مثلاً أو ماله أو صلاحياته، وتتأذ هذه الجريمة على الانترنت إأأى الوجهين التاليين: انتأال شخصية الفرد وانتأال شخصية المواقع"<sup>2</sup>.

أما انتأال شخصية الفرد فتتم في الغالب عبر استغلال أأأ المترصدين لبيانات شخص ما على شبكة الانترنت من أأل الحصول على بطاقات بنكية أأمانية مثلاً، ذلك أن البيانات السالفة الذكر تمكنهم من التأمدم بطلبات لاستأأار البطاقة البنكية عبر الانترنت خاصة من ألال الهيئات التي لا تتأذ إأأراء أمنية صارمة عبر الشبكة.

في أأن أن انتأال شخصية المواقع فيأد الاختراق أأأاعي أأز صورها، إذ يأسء "أأطر أنواع الاختراقات، أأ يتأكر أأأ القراصنة في شخصية طرف يمثل مؤسسة مالية أو صاحب بطاقات بنكية يمكنه من ألالها أأصيل أموال من التأار والمستهلكين على أأ سواء"<sup>3</sup>، عبر أأويلهم أأو الموقع أأأال، ثم طلب الرموز السرية منهم<sup>4</sup>.

ويتأقق هذا الفعل الإأرامي من ألال العمل على إنشاء مواقع وهمية على شبكة الانترنت على أرار مواقع الشركات والمؤسسات التجارية الأصلية الموجودة على الشبكة، أأ يظهر هذا الموقع وكأنه الموقع الأصلي الذي يقدم الخدمة، ولكي ينشأ هذا الموقع يقوم القراصنة بالحصول على كافة بيانات الموقع الأصلي من ألال الشبكة، ومن ثم إنشاء الموقع الوهمي، من ألال أأديل البيانات السابقة التي تم الحصول عليها بطريق غير مشروء أأ لا يظهر بأن هنالك ازدواأا في المواقع، فيأدو الموقع الأصلي وكأنه الموقع الوحيد.

### أ اقتناص الرسائل الالكترونية (البريد الالكتروني)<sup>5</sup>:

لأد اتفق رجال القانون على أأأأار البريد الالكتروني عبارة عن معلومة إسمية، خاصة وأنه يشتمل على بلد الشخص وأأيانا اسمه الصحيح إلى أأب معلومات أأرى. والملاحظ بهذا الشأن أنه رغم كون البريد الالكتروني يؤمن إأارة وتبادل الرسائل بأقل تكلفة، إلا أن إمكانية اعتراضه أأول دون الوثوق به، إذ يمكن اعتراض الرسائل التي يتم أأميلها طرفيا عبر الشبكة، وكشف مضمونها من ألالها الموزع وعبر برامج معينة قادرة على قراءة هذه الرسائل التي يجب أن تمر من ألال الموزع ليتم أأميلها إلى الطرف الآخر، مما يفتأ أأال أمام إمكانية قراءتها.

1- راجع عبد الرحمان بن أألال، جريمة الانتأاك الالكتروني أأمة الحياة الخاصة (أأاسة مقارنة)، أألة الفقه والقانون، أبريل 2014، العدد 18، ص 96.

2- سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية، رسالة لنيل شهادة الماستر في الحقوق، أأامة محمد أأضر، كلية الحقوق والعلوم السياسية، بسكرة، 2013-2014، ص 28.

3- صليأة أأجي، الآليات القانونية لتأريس الأمن المعلوماتي، أألة العلوم الجنائية، 2015، العدد الثاني، ص 11.

4- كأثرين فيو، التسويق الإلكتروني، ترجمة ودية راشء، الطبعة الأولى، مؤسسة محمد بن راشء آل كنوم، 2008، ص 137.

5 - البريد الالكتروني هو عنوان صندوق البريد الذي عن طريقه يتم إرسال الرسائل البريدية الإلكترونية باستخدام شبكة الانترنت، ذلك أن كل شخص مستأدم هذه الشبكة يكون له إن أراد عنوانا بريديا، يتم أأول إليه بكلمة مرور لا يعلمها إلا الشخص صاحب صندوق البريد نفسه، للمزيد أأل هذا الشأن ينظر محمد سالم أأأير، تأثير العنوان الإلكتروني على علامة الخدمة، رسالة لنيل شهادة الماستر في القانون الخاص، أأامة أأسن الأول، كلية العلوم القانونية والاقتصادية والاجتماعية، سطات، 2009-2010، ص 38.

والمشكلة أن عملية التطفل هذه إلى جانب كونها أضحت تباشر من قبل محترفين كما سلف وأشرنا، فإنها كذلك يمكن أن تتم من قبل موظفين أو بأمر من الإدارة لدى الموزع، وفي غالبية الدول تكون هذه الرقابة مفروضة من لدن أجهزة رسمية للتجسس بدعوى حماية الأمن والنظام العام<sup>1</sup>.

### ◀ الغش المعلوماتي :

تعددت تسميات وتعريفات الغش المعلوماتي، حيث نجد من الفقه من استخدم تسمية "الاحتيال المعلوماتي"، في حين استخدم آخرون تسمية "غش الحاسوب"، ولكن التعريفات تلتقي جميعها حول وصف هذا الجرم بأنه سلوك احتيالي أو خداعي مرتبط باستخدام الكمبيوتر، يهدف مرتكبه إلى تحقيق فائدة أو مصلحة مالية<sup>2</sup>، كما عرفه الأستاذ رضوان بن خضراء بكونه ذلك "الخداع الذي يعمد من ورائه الشخص للحصول من الغير، بدون حق، على فائدة أو مزية"<sup>3</sup>، فالغش المعلوماتي من خلال هذه التعاريف عبارة عن مفهوم واسع، حيث تنضوي تحته العديد من الجرائم، من قبيل السرقة، النصب، اختلاس مال الغير، وهي أفعال غالبا ما تتم بواسطة الحاسوب وعن بعد. ولعل أبرز مظهر من مظاهر الغش المعلوماتي نجد جرائم السطو على بطاقات الائتمان والتحويل الإلكتروني غير المشروع للأموال<sup>4</sup>، كيف لا وجريمة الغش المعلوماتي قد نشأت مع شيوع أنظمة تحويل الأموال بطريقة الكترونية، حيث تزايدت بشكل ملحوظ قيمة الأموال المتداولة بهذه الطريقة، مما جعلها تصبح موضوعا لجرائم التحويل الإلكتروني غير المشروع<sup>5</sup>.

### ◀ السلب بالقوة الإلكترونية:

تظهر بجلاء صورة هذا الفعل اللامشروع في استخدام الحاسوب من أجل التلاعب بالمعلومات، وذلك بإدخال بيانات زائفة من جانب المتحاييل واختلاق معاملات أو فواتير ينبغي تسديد ثمنها، أما المستهلك فلن يتمكن من إثبات كونه غير مدين بالأداء لوجود فواتير معلوماتية، وهكذا يستغل المتحاييل طرق الدفع الآلية للحصول على أموال غير شرعية على حساب هذا المستهلك<sup>6</sup>.

### ب: التجسس على المستهلك الإلكتروني والتجميع اللامشروع لمعطياته الشخصية

على اعتبار أن العالم الإلكتروني هو عالم متشابك ومعقد، فإن المستخدم يترك عقب كل استخدام له لشبكة الانترنت آثار ودلالات كثيرة تتصل به على شكل سجلات رقمية، كما هو الشأن بالنسبة للموقع الذي زاره، الأمور

1- للمزيد ينظر بن سعيد صيرينة، م.س، ص 145.

2- وليد العاكوم، مفهوم وظاهرة الإجرام المعلوماتي، مؤتمر القانون والكمبيوتر والانترنت، المجلد الأول، تنظيم جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، من 1 إلى 3 ماي 2000، الطبعة الثالثة، 2004، ص 14.

3- أورده عبد الوهاب لعيل، الحماية الجنائية للحساب البنكي من الاعتداء المعلوماتي، رسالة لنيل شهادة الماستر في العلوم الجنائية، جامعة القاضي عياض، كلية العلوم القانونية والاقتصادية والاجتماعية بمراكش، 2008-2009، ص 63.

4- تتم عملية التحويل الإلكتروني غير المشروع للأموال من خلال الحصول على كلمة السر في ملفات أنظمة الكمبيوتر الخاصة بالجاني عليه، مما يسمح للجاني بالتوغل في النظام المعلوماتي، وذلك بإحدى الطرق التالية:

-الاحتيال: حيث يوهم الجاني عليه بوجود مشروع كاذب أو يحدث الأمل لديه بحصول ربح، فيسلم المال للجاني بطريق معلوماتي أو من خلال تصرف الجاني في المال وهو يعلم أن ليست له صفة التصرف فيه

-الاحتيال باستخدام بطاقات الدفع الإلكتروني

للمزيد راجع سمية مزغيش، م س، ص 30.

5- وليد العاكوم، م س، ص 14.

6- هداية بوعزة، نظام الدفع الإلكتروني بين المزايا والمخاطر، مجلة الفقه والقانون، يوليو 2014، العدد 21، ص 137.

التي يبحث عنها، المواء التي قام بتنزيلها، المطبوع الإلكتروني الذي ملأه عند طلب منتج أو خدمة عبر أحد المواقع التجارية، دون نسيان المواقع الاجتماعية التي ييسط مصممها ويشترط على كل راغب في الانتماء إليها الإدلاء بالعديد من البيانات ذات الطابع الشخصي، وكذا العناصر التي أرسلها المعني بالخدمات والطلبات التي قام بشرائها، إلى جانب معلومات أخرى مرتبطة بمواياته وميولاته، وهي سجلات تتضمن تفاصيل خصوصيته وتعتبر بحق أكبر آلة لجمع ومعالجة ونقل البيانات الشخصية، تنقل جميع الأنشطة الحياتية من العالم المادي إلى العالم الافتراضي وتترك بصمات للفرد<sup>1</sup>.

وعليه، فقد وفرت الانترنت حقلا واسعا لتقفي الآثار في إطار ما اصطلح عليه بـ (La traçabilité)، أي الطرق التي تعنى بدراسة ما يتركه الشخص عقب إقدامه على أي فعل أو سلوك أو تصرف، ذلك أنه على إثر كل ارتباط بالانترنت، يترك الفرد وراءه، عن وعي أو عن غير وعي، آثار ومخلفات في الحاسوب أو على الخط، تسجل وتخزن بحسب الأحوال إما في ذاكرة حاسوبه أو لدى مقدم الولوج أو أي خادم آخر<sup>2</sup>.

من هنا، فإذا كانت البيانات الشخصية للمستهلكين غالبا ما يقدمونها بأنفسهم وعن طوعية، على أساس أن إجراء المبادلات التجارية من بيع وشراء وإبرام للعقود على الخط تتطلب إعطاء بعض البيانات الشخصية، أو قد يتم التوصل إليها بوسيلة أو بأخرى، فإن تهديد حرمة الحياة الخاصة يثار أكثر حين تستعمل هذه المعلومات دون موافقة المعني بالأمر أو تنتشر بصورة غير صحيحة، أو أن يتم بيعها للغير، ذلك أن هذه البيانات يحكمها مبدأ أن الجمع والتخزين الذي تخضع له لا يفيدها أنها انتقلت من نطاق الخصوصية إلى العلانية، كما أن الرضا بالتخزين والتجميع لا يعني حرية تداولها ونقلها إلى الكافة، لأن القول بخلاف ذلك سيعرضها لمخاطر جمة.

فالإطلاع على هذه البيانات قد يمتد ليخول معرفة أرقام حسابات المستهلك أو أرقام بطاقات الائتمان، والتي تشكل -عن حق- أكثر البيانات الشخصية عرضة للاعتداء بالحصول عليها عن طريق الاحتيال أو من خلال سرقة أرقام هذه البطاقات<sup>3</sup>، وذلك بعد فك الشفرات التي تحمي سريتها وكسر الحواجز الأمنية واستكشاف مواطن الضعف في الجهاز أو الشبكة، كما يمكن اكتشاف كلمة السر المعتمدة من قبل المستهلك، مما يخلق معه النفاذ إلى نظم بيانات مهمة أخرى، كتغيير اسم المدفوع لأمره في الشبكات الإلكترونية، أو المبالغ المحولة إلى حساب بنكي<sup>4</sup>.

من جهة أخرى، نجد بأن المؤسسات والمقاولات بصفة عامة تسعى جاهدة بدورها للحفاظ على زبائنها الحاليين وكذا جذب زبناء ومستهلكين جدد، وفي هذا تعتبر إحدى أهم وسائل التسويق عبر الانترنت هي متابعة وتعقب الزائرين لموقع المقولة، بهدف معرفة سلوكهم، وتتم عملية المتابعة والتعقب باستخدام برامج وأدوات وأجهزة ذكية يتم استخدامها، مثل عملية التنقيب عن البيانات "Data mining" والكوكيز والنماذج الكترونية (الاستمارة) التي يقوم الزبناء بتعبئتها عبر الموقع، وهناك وسائل أخرى غير أخلاقية مثل (Web Bugis و Spay ware) وغيرها<sup>5</sup>.

1- بن سعيد صبرينة، م س، ص 146.

2- العربي جنان، م س، ص 30.

3- بن سعيد صبرينة، م س، ص 132.

4- صليحة حاجي، الآليات القانونية لتكريس الأمن المعلوماتي، م س، ص 11.

5- خضر مصباح الطيطي، م س، ص 110.

وتعد عملية التقفي هذه والتي أضحت الكثير من الشركات الضخمة تنهجها مثل (Amazon)، من أسرع الطرق وأدقها مقارنة بالطرق التقليدية، حيث تسمح للشركات بدراسة سلوك مزيد من المستهلكين في مختلف المناطق عبر العالم، وهي أمور لا يمكن القيام بها باعتماد السبل التقليدية. أيضا تعتبر إجراء الدراسات والأبحاث المتعلقة بالتجارة الإلكترونية أكثر عمقا، حيث أنها تعطي معلومات كاملة عن القرارات التي اتخذها المستهلك، أو المواقع التي زارها وعدد الزيارات التي قام بها، والوقت الذي أمضاه بكل موقع وفي كل صفحة، مع تسجيل كل العمليات التي قام بها بالفأرة أو بلوحة المفاتيح مما يؤدي إلى دراسة سلوك العملاء والمستهلكين بشكل دقيق، وهذا ما يمكن الشركات من التنبؤ بما سيشتريه هؤلاء ووقت الشراء وكذا معرفة سبب الشراء أو سبب عدم الشراء من الانترنت<sup>1</sup>.

46

من خلال ما سبق، يتضح بأن الانترنت وإن كان يعود لها الفضل في التطور العلمي والتقني، فإنها في المقابل حملت لنا العديد من المخاطر التي تهدد خصوصية المستهلك، كونها وفرت مجموعة من السبل للترصد وتقفي الآثار، فالمعطيات التي يتم جمعها أصبحت وسيلة ومطية للكشف عن هوية للمستهلك الإلكتروني، ذلك أنها تدرس الكفاءات والسلوكيات، لترسم العادات والميولات، والأذواق ونوايا الأشخاص<sup>2</sup>.

مما جعل منها - المعطيات الشخصية - في ظل تطور التجارة الإلكترونية عاملا اقتصاديا ومؤشرا على اكتشاف الأسواق والسيطرة عليها، حيث تتكون قاعدة بيانات ضخمة عن المعطيات السلوكية لهؤلاء، بشكل يخول التعرف على المستهلكين في مختلف بقاع العالم عن كثب، وتجزئة السوق إلى قطاعات بناء على فهم ما الذي يجعل الفرد منا يوافق على شراء سلعة بعينها، منفقا في ذلك ماله الذي كد في جمعه. كما أن هذه القاعدة تعطي فكرة عن الإمكانيات المادية والعادات الاستهلاكية، مما يسمح بتوجيه إعلانات على مقاسهم، وقد ترتب عن هذه الظاهرة تطور ليس فقط في البحث عن مستهلكين جدد، وإنما الدفع بالطاقة الشرائية لأولئك الفعليين، من أجل طلب مزيد من المنتجات والخدمات من خلال الإعلانات المتنوعة المستفزة عبر المواقع الاجتماعية والبريد الإلكتروني.

## ثانيا : الحماية المقررة للخصوصية الإلكترونية للمستهلك

تمثل المعطيات الشخصية ركيزة من الركائز التي تقوم عليها التجارة الإلكترونية، إذ لطالما تزود منها أصحاب المواقع التجارية كما يتزودون من السلع، وإذا كان هذا التزود من المفترض أن يكون مشروعا محترما للضوابط القانونية، فإن التجربة أبانت على أنه غالبا ما يقع الانحراف باستعمال هذه المعطيات في غير الأغراض التي جمعت من أجلها، على اعتبار أن المستهلك الذي يقوم بمد صاحب الموقع التجاري بمعطياته الشخصية بغاية شراء سلعة أو خدمة فإنه يقوم بذلك على أساس أن هذه المعطيات لن يقع استعمالها إلا بهدف القيام بإجراءات المعاملة في إطار من السرية<sup>3</sup>. فبغية التصدي لمثل هذه الممارسات وغيرها، أصدر المشرع زمرة من المقتضيات ذات الطابع الجنائي (ب)، على أن دراسة هذه المقتضيات لن تتم إلا بعد المرور على المقتضيات الحماية التي جاء بها القانون رقم 08.09 المتعلق بحماية الأشخاص الذاتيين اتجاه معالجة المعطيات ذات الطابع الشخصي (أ).

1- خضر مصباح الطيطي، م.س، ص 110.

2- العربي جنان، م.س، ص 88.

3- عبد المجيد كوزي، الحماية الجنائية للمعطيات في المجال المعلوماتي، المجلة المغربية للقانون الجنائي والعلوم الجنائية، 2016، العدد الثالث، ص



## أ: تحمين خصوصية المستهلك الإلكتروني من خلال قانون حماية الأشخاص الذاتيين اتجاه معالجة المعطيات ذات الطابع الشخصي

لقد حرصت العديد من التشريعات على بسط مظلة الحماية لتشمل نظم المعالجة الآلية للمعطيات، والمغرب بدوره، لم يخرج عن هذا المجرى، حيث أصدر المشرع قانونا يعنى بحماية الأشخاص الذاتيين اتجاه معالجة معطياتهم ذات الطابع الشخصي<sup>1</sup>، وهو تشريع يندرج في سياق التطورات التي يشهدها المغرب للدفع بالحرية إلى أعلى مستوى والمساهمة في تأهيل المخططات التي وضعها المغرب في مجال الحكومة الإلكترونية والمغرب الرقمي، أما الهدف منه فيتمثل بالخصوص في حماية المعطيات التي يدلي بها الأشخاص الذاتيين عبر الشبكة العنكبوتية، إذ لا يخفى على أحد ما يثيره التبادل الإلكتروني للمعطيات من مشاكل<sup>2</sup>. هذا وقد جاء هذا القانون بالعديد من مقتضيات الحماية التي من شأنها أن تزرع، إلى حد ما، نوعا من الأمان والسرية اتجاه البيانات والمعطيات<sup>3</sup> التي قد يدلي بها المستهلك عند طلبه مثلا لمنتوج معين عبر شبكة الانترنت أو عند ملئه لأحدى الاستمارات على هذه الشبكة، حيث أقر له حقوقا (1)، ووضعت التزامات على عاتق كل مسؤول عن المعالجة (2).

### 1: حقوق المستهلك بمناسبة معالجة معطياته الشخصية

يراد بمعالجة المعطيات ذات الطابع الشخصي كل عملية أو مجموعة عمليات تنجز بمساعدة طرق آلية أو بدونها، وتطبق على المعطيات ذات الطابع الشخصي، مثل التجميع أو التسجيل أو الاستعمال أو الإيصال عن طريق الإرسال أو الإذاعة أو أي شكل آخر من أشكال إتاحة المعلومات، أو التقريب أو الربط البيئي<sup>4</sup>. بعبارة أدق، فالبيانات لكي يكون لها معنى يجب أن تحول إلى صورة أو شكل يوصل المعرفة، وهذا ما يسمى بمعالجة البيانات، حيث يتم إخضاع هذه الأخيرة للعديد من التحويلات بترتيبها وفرزها في تسلسل منطقي أو حسابي معين، كما لو قامت إحدى المقاولات بتجميع بيانات حول عدد من المستهلكين إلكترونيا، سواء من خلال المعلومات والبيانات التي أدلى بها هؤلاء بمحض إرادتهم أو من خلال سبل أخرى - كما سلف وأشرنا في محطات سابقة -، وترتيبها وتصنيفها في قطاعات أو فئات طبقا لخصائص مشتركة، كتصنيف المبيعات على أساس نوع المنتج الذي يفضلونه أو نوع المستهلك أو منطقة البيع<sup>5</sup>.

فالبيانات يتم الحصول عليها في شكل خام، وهي بذلك لا تقدم معنى ولا فائدة إلا إذا حولت لصور أو أشكال توصل إلى المعرفة (معلومات). و تتمثل عمليات تحويل البيانات إلى معلومات في تصنيفها وتخزينها، وذلك

- 1- قانون رقم 08.09 حول حماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي الصادر بتاريخ 18 فبراير 2009، منشور بالجريدة الرسمية عدد 5700 بتاريخ 23 فبراير 2009، ص 552.
- 2- زكرياء بوشوروة، م س، ص 138.
- 3- يراد بالمعطيات ذات الطابع الشخصي كل معلومة كيفما كان نوعها بغض النظر عن دعائها، بما في ذلك الصوت والصورة، والمتعلقة بشخص ذاتي معرف أو قابل للتعرف عليه، إذا كان بالإمكان التعرف عليه بصفة مباشرة أو غير مباشرة، ولا سيما من خلال الرجوع إلى رقم التعريف أو عنصر من عناصر عدة مميزة لهويته البدنية أو الجينية أو الفيزيولوجية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية، عبد الحكيم زروق، م س، ص 310.
- 4- البند الثاني من المادة الأولى من قانون 08.09 المتعلق بحماية الأشخاص الذاتيين اتجاه معالجة المعطيات ذات الطابع الشخصي.
- 5- رشيد بن الشيخ الفقون، م س، ص 29.



بوضعها في فئات تبا للخصائص المشتركة، و جعلها سهلة الاسترجاع لغرض المعالجة<sup>1</sup>. أمام هذه الممارسات التي تمس بخصوعية المستهلك الالكروني، تدخل المشرع ليخول له حقوقا مهمة، سواء قبل إجراء هذه المعالجة أو بعدها.

### 1.1 : حقوق المستهلك قبل الإقدام على المعالجة

الحصول على موافقته قبل الإقدام على معالجة معطياته: أي إخبار المعني بمضمون المعالجة وكيفية إنجازها

والغايات المتوخاة منها، فالمعطيات المتعلقة بالمستهلك لا يمكن أن تكون محلا للمعالجة إلا بعد الحصول على موافقته الصريحة بشكل لا يحتمل الشك، غير أن إجبارية الحصول على الموافقة ليست مطلقة وإنما ترد عليها بعض الاستثناءات التي تبررها أسباب قانونية ومنطقية محددة في الفقرة 3 من المادة 4 من قانون 08.09<sup>2</sup>.

ضبط عملية نقل المعطيات الشخصية نحو بلد أجنبي: إذ لا يجوز لكل مسؤول عن المعالجة أن ينقل معطيات ذات طابع شخصي إلى دولة أجنبية إلا إذا كانت هذه الدولة تضمن مستوى حماية كاف<sup>3</sup> للحياة الشخصية والحريات والحقوق الأساسية للأشخاص إزاء المعالجة التي تخضع أو قد تخضع لها هذه المعطيات، حيث تعهد اللجنة الوطنية قائمة الدول المتوفرة فيها المعايير المحددة<sup>4</sup>.

على أنه واستثناء من أحكام المادة السالفة الذكر، يمكن للمسؤول المذكور أن ينقل معطيات ذات طابع شخصي نحو دولة لا تتوفر فيها الشروط المتطلبة لكن شريطة الحصول على الموافقة الصريحة للشخص الذي تخصه المعطيات، أو أن يكون النقل ضروريا<sup>5</sup>، أو أن يتم تنفيذا لاتفاق ثنائي أو متعدد الأطراف يكون المغرب عضوا فيه؛ أو بناء على إذن صريح<sup>6</sup> ومعلل للجنة الوطنية وذلك إذا كانت المعالجة تضمن مستوى كاف من الحماية للحياة الشخصية وكذا للحريات والحقوق الأساسية للأشخاص، لاسيما بالنظر إلى بنود عقد أو نظام داخلي تخضع له<sup>7</sup>.

منع الاستقراء المباشر: عرف المشرع الاستقراء المباشر في الفقرة الثالثة من المادة 10 من قانون 08.09 بأنه

"إرسال أي رسالة موجهة للترويج المباشر أو غير المباشر لسلع أو خدمات، أو لسمعة شخص يبيع سلعاً أو يقدم خدمات"، فالأمر يتعلق بتوجيه خطابات معدة للترويج التجاري إما لسلع أو لخدمات، وإما لسمعة التاجر صاحب

1- وتكمن أهمية عمليات التصنيف والتخزين في جعل البيانات سهلة الاسترجاع لغرض المعالجة، وسهلة العرض والاستخدام لمستعملها، لهذا توصف البيانات بأنها الفرق الذي يصنع الفرق. خالدي فراح، دور نظام المعلومات التسويقية في اتخاذ القرارات التسويقية، أطروحة دكتوراه في علوم التسويق، جامعة محمد خيضر، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، بسكرة، الجزائر، 2013-2014، ص 40.

2- إذا كانت المعالجة تشكل التزاما فرضه القانون، إما على الشخص المعني نفسه وإما على المسؤول عن المعالجة، فلا حاجة لموافقة أو رضا الأشخاص المعنيين، وإلا سوف يحول ذلك دون تنفيذ الالتزام.

- إذا كانت المعالجة ضرورية لتنفيذ عقد حيث يتعلق الأمر بتنفيذ التزام تعاقدى أو تنفيذا للإجراءات السابقة عن العقد.

- حالة الحفاظ على المصالح الحيوية للشخص المعني بالمعطيات، إذا كان من الناحية البدنية (مرض مثلا أو عاهة تحول دون قدرته عن التعبير عن رضاه عن المعالجة) أو القانونية (فقدان الأهلية مثلا أو المفقود إذا لا يمكن الحصول على موافقة المعني بالأمر). غير قادر عن التعبير عن رضاه عن المعالجة.

3- انظر المادتين 46 و 47 من المرسوم رقم 2.09.165، صادر في 25 من جمادى الأولى 1430 (21 ماي 2009) لتطبيق القانون رقم 08.09 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي؛ الجريدة الرسمية عدد 5744 بتاريخ 24 جمادى الآخرة 1430 (18 يونيو 2009)، ص 3571.

4- المادة 43 من قانون 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي.

5- يمكن للمسؤول عن المعالجة نقل معطيات ذات طابع شخصي نحو دولة لا تتوفر فيها الشروط المتطلبة في حالة ما إذا كان النقل ضروريا: أ) للمحافظة على حياة هذا الشخص؛ ب) للمحافظة على المصلحة العامة؛ ج) احتراماً لالتزامات تسمح بضمان إثبات حق أمام العدالة أو ممارسته أو الدفاع عنه؛ د) تنفيذا لمقتضيات عقد بين المسؤول عن المعالجة والمعني، أو لإجراءات سابقة على التعاقد متخذة بطلب من هذا الأخير؛ هـ) لإبرام أو تنفيذ عقد مبرم أو سيمر بين المسؤول عن المعالجة وأحد الأغيار وذلك لمصلحة الشخص المعني؛ و) تنفيذا لإجراء متعلق بتعاون قضائي دولي؛ ز) الوفاية من إصابات مرضية أو فحصها أو معالجتها.

6- انظر المادة 48 من المرسوم رقم 2.09.165، السالف الذكر.

7- المادة 47 من قانون 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي.

تلك السلع أو الءءماء. بمعنى آءر؁ فإننا أمام عملية إشهارية ءءارية ممضة؁ يلءاً إليها ءءار؁ مسءغلين قواعء بباءات مهمة؁ ءشمل عناوين المسءهلكين الاءءرونية وأرقام هوائفهم؁ أرقام الفاكس؁ ءيلكس الء؁ بءية ءوءيه مضامين ءءارية إشهارية إلى فءاء مءءلفة من الأشءاء المرصوءين في ضوء معاءير اءءماعية واقتصادية مءروسة من أجل عرض السلعة أو الءءمة الملاءمة لها عبر وسائل الاءءال المءكورة<sup>1</sup>.

وهكذا يءء المسءهلكون أنفسهم مضطرين لاسءقبال رسائل غير مرغوب فيها ءروء لءءماء مشبوهة ءشوش عليهم باسءمرار ءون إءن مسبق<sup>2</sup>؁ لذلك ءاءء الماءة السالفة الذكر لءمنع هذا النوع من السلوكاء ما لم يعرب المعنيون عن موافءتهم على اسءعمال معطائهم الشءصية من ءهءة؁ ورضاهم المسبق على اسءقبال الاسءقراءاء من ءهءة أخرى<sup>3</sup>.

## 2.1: ءقوق المسءهلك بعء الموافقة على المعالءة

إن الشءص وبعء أن يعرب عن رضاه وموافءته على المعالءة ءنشأ له مءموعة من الءقوق ءسب كل مرءلة من مراحل المعالءة وذلك وفق الشكل ءالئ:

**الءق في الإعلام:** اعءرف المشرع للمعني بالمعالءة -أي المسءهلك في مقامنا- بعء أن يءلي بما يءبء هوءته؁ أن يءصل من المسؤؤل عن المعالءة في فءراء معقولة؁ وعلى الفور؁ وءون عوض؁ على ءأكبء بأن معطائءه ذاء الطابع الشءصئ المعءلة به ءعالء أو لا ءعالء؁ وكذا على معلومااء مرءبءة على الأقل بغافاء المعالءة وفءاء المعطائاء الءئ ءنصب عليها؁ والمرسل إليهم؁ أو فءاء المرسل إليهم الءئ أوصلء إليهم المعطائاء ذاء الطابع الشءصئ؁ وبالمعطائاء الءئ ءخضع للمعالءة؁ والمنطق الءئ يءكم كل معالءة آلية للمعطائاء ذاء الطابع الشءصئ المعءلة به<sup>4</sup>.

**الءق في ءءصءء:** إء يمكن أن يعءري المعطائاء الشءصية نقصان أو ءطاء؁ كما يمكن أن يطرأ عليها ءءءير وءءوءير بعء ءءصءل ءءصءب غير مءطابقة مع الواقع؁ الشئء الءئ من شأنه أن يؤءر على ءقوق وسمعة الشءص المعني؁ مما يؤلء لهذا الآخر الءق في مءالبة المسؤؤلين عن المعالءة بأن يباشروا ءءئين وءصءء أو مءو المعطائاء الءاطئة أو إءام الناقصة منها بأءسب الأحوال؁ وقء ءءء المشرع أءلاء أقصاه 10 أيام للاستءابة لمءل هذه الطلباء وإلا ءق اللءوء إلى اللءئة الوطنية لءماء المعطائاء الشءصية الءئ ءكلف في هذه الءالة أءء أعضائها بالءءقء والعمل على مباشرة ءءصءءاء اللازمة في أقرب الآءال؁ وأثناء هذا الوقت يءاط المعني بالأمر علما بمآل طلبه<sup>5</sup>.

**الءق في ءءرض:** نصء على هذا الءق الماءة 9 من قانون 09.08؁ ءء ءولء للمعني بالمعالءة أن يءعرض لأسباب مشروعة على القفاء بمعالءة معطائءه الشءصية؁ سواء قبل المعالءة أو أثناء إنءازها؁ إء يءق للمعني أن يرفض المعالءة قبل إءرائها أو أثناء إنءازها وذلك بسءب موافءته السابقة.

- العربي ءنان؁ م س؁ ص 94-95

2 - ءروء الاسءقراءاء المباشرة ءون مراعاة ما ءءءه من مضابقة وأءر نفسي سئء لدى المسءقبل؁ ذلك أن باءء وءءف الرسالة يكون هو ءروءء وءءءرف بالءءءاء وءءماء؁ من ءون أن ءراعي ما قء يءال هذا المسءقبل من مشاكئل نفسية وعائلية واءءماعية وغيرها.

عءء الءكمم زروق؁ ءنظم ءبائل الإلاءروني للمعطائاء القاءونية عبر الأنءرءئء؁ الطبعة الأولى؁ ءار الأمان؁ 2016؁ ص 314.

4 - عءء الءكمم زروق؁ م س؁ ص 313.

5- العربي ءنان؁ م س؁ ص 92-93.

2: التزامات المسؤول عن المعالجة<sup>1</sup>

حماية للحياة الخاصة للمستهلك، وجه المشرع خطاباً آمراً من خلال المادة الأولى من قانون 08.09 لكل مسؤول عن المعالجة ووضع على عاتقه عديداً من الالتزامات، لعل أبرزها:

**الالتزام بسرية وسلامة المعالجات :** يعنى بسرية المعلومات التأكد من عدم الاطلاع الغير مصرح به عليها، فضلاً عن تحديد حدود وصلاحيات الاستخدام، مع تحديد من له صلاحية التعديل أو الإدخال أو الحذف أو الإضافة أو القراءة فقط من بين المصرح لهم بوجه عام<sup>2</sup>، كما يشمل هذا الالتزام أن يعمل المسؤول عن المعالجة على أن تستبعد صراحة المعطيات من الاستخدام الخاص أو النقل اللامأذون إلى جهة ثالثة، كما أنه مطلوب من المسؤول أيضاً أن يتأكد من أن المقاوله من الباطن قد قدمت ضمانات من شأنها تأمين البيانات، ومسألة الرقابة هذه ينبغي أن تكون محددة في العقد<sup>3</sup>.

أما سلامة المعالجات فتعني ضمان عدم تغيير المعلومات المخزنة أو المنقولة بشكل غير ملائم، سواء بقصد أو بدون قصد<sup>4</sup>، وعليه ففي هذه الحالة لا يكفي أن نحافظ على سرية المعلومات، بل أيضاً اتخاذ التدابير اللازمة لحمايتها من التغيير<sup>5</sup>.

وقد عالج المشرع مسألة "سرية وسلامة المعالجات والسر المهني" في الفرع الثالث من خلال المادة 23 من قانون 09.08.

لأجل هذا فإنه يجب على المقاولات أن تضمن بأن تتم عمليات المعالجة في إطار من السرية والشفافية، ويتعين أن تتخذ الإجراءات التقنية والتنظيمية اللازمة لتحقيق هذا الهدف بالشكل الذي يمكن من خلاله التصدي لمختلف المخاطر التي يمكن أن تمس هذه السرية<sup>6</sup>.

ومما تجب الإشارة إليه هنا أن المقاوله يتعين عليها أن تضمن عنصر سرية البيانات حتى عندما تخول أمر المعالجة لمقاوله أخرى من الباطن، ففي هذه الحالة تبقى المقاوله الأصلية مسؤولة عن معالجة البيانات الشخصية التي تقوم بها المقاوله من الباطن بما يتوافق مع حماية هذه البيانات، وتكون مسألة الضمان هذه في إطار تعاقدى —أي عند إبرام العقد من الباطن—، إذ والحالة هذه يتحتم على المقاوله من الباطن أن تستخدم البيانات وفق نفس الطريقة التي كان يتحتم على المقاوله الأصلية أن تعالج البيانات في إطارها<sup>7</sup>.

1- نص البند الخامس من المادة الأولى من قانون 08-09 على أن المسؤول عن المعالجة هو الشخص الذاتي أو المعنوي أو السلطة العامة أو المصلحة أو أي هيئة تقوم، سواء بمفردها أو باشتراك مع آخرين بتحديد الغايات من معالجة المعطيات ذات الطابع الشخصي ووسائلها...، وعليه فهذا المسؤول قد يكون مقاوله أو إدارة أو مصلحة أو أية هيئة أخرى يضع المستهلك معلومات ومعطيات شخصية متعلقة به بين يديها بمناسبة إجرائه لمعاملة معينة معها.

2- منصور بن سعيد القحطاني، مهددات الأمن المعلوماتي وسبل مواجهتها، رسالة لنيل شهادة الماستر في العلوم الإدارية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، 2008-2009، ص 21.

3- Maria Winkler, la protection des données dans l'entreprise – un mode d'emploi pour sa mise en œuvre, articles spécialisés, 2011, p 113, publié sur file:///C:/Users/ordi/Downloads/Documents/2\_11\_Fachb\_Winkler\_Datenschutz\_fr\_Druckdatei.pdf

4- منصور بن سعيد القحطاني، م س، ص 21.

5- خالد بن سليمان الغثير ومهندس محمد بن عبد الله، أمن المعلومات بلغة ميسرة، الطبعة 1، مكتبة الملك فهد الوطنية الرياض 2009 ص 23.

6- Maria Winkler, Op. cit, p 113.

7- Maria Winkler, Op.cit, p 113.

**تقنين عملية الربط البيئي :** يتعلق الأمر بشكل من أشكال المعالجة يتمثل في ربط صلة بين معطيات أحد ملفات المستهلكين مع معطيات ملف أو عدة ملفات أخرى حول نفس المستهلك يمسخها مسؤول أو مسؤولون آخرون أو يمسخها نفس المسؤول ولكن لغرض آخر<sup>1</sup>، فاعتبارا لما تشكله من خطورة كونها تتيح فرصة لتشكيل ملف يتناول مزيجا من التفاصيل التي تحكي عن خصوصية المستهلك، لأجل ذلك تدخل المشرع وأخضعها لوجوب الحصول على إذن مسبق<sup>2</sup>.

**حفظ المعطيات لمدة معقولة :** يقصد بهذا الالتزام بأن المعطيات الشخصية يمكن أن تظل ممسوة من طرف المسؤول عن المعالجة طالما ظلت الحاجة التي من أجلها جمعت قائمة، وبمفهوم المخالفة "إذا انتهى وقضي الغرض الذي جمعت من أجله المعطيات فإنه ينبغي تدميرها"<sup>3</sup>.

وقد نص المشرع على هذا الالتزام في الفقرة (هـ) من البند الأول من المادة 3 من قانون 08-09، حيث أوجبت هذه الفقرة " أن تكون المعطيات الشخصية محفوظة ... طوال مدة لا تتجاوز المدة الضرورية لإنجاز الغايات التي تم جمعها ومعالجتها لاحقا من أجلها".

ويعتبر (Jean FRAYSSINET) أن هذا المقتضى يكتسي أهمية كبرى، لأنه يمنع أن يبقى الشخص منزعا وقلقا طوال حياته بسبب معلومات تخصه تم جمعها ومعالجتها في يوم من الأيام لتحقيق غايات معينة، لذا يطلق على هذا المبدأ "الحق في النسيان"<sup>4</sup>، كذلك تزداد أهمية هذا المبدأ حين نعلم بأن بقاء المعطيات بيد المسؤول عن المعالجة يمكن أن يفتح المجال أمام خضوعها لنوع من سوء المعاملة وسوء المعالجة<sup>5</sup>.

**واجب الإخبار :** إذ يجب على المسؤول عن المعالجة أو من يمثله إخبار<sup>6</sup> كل شخص تم الاتصال به مباشرة قصد تجميع معطياته الشخصية بشكل مسبق وصریح بحوية المسؤول عن المعالجة وعند الاقتضاء هوية مثله، وبغايات المعالجة المعدة لها المعطيات ومضمونها، وكيفية إنجازها والغايات المرجوة منها وبكل المعلومات الإضافية الأخرى<sup>7</sup>. وفي حال جمع المعلومات في شبكات مفتوحة فإنه يجب أن يحاط الشخص علما بأن معطياته من الممكن تداولها على تلك الشبكات دون أية ضمانات على سلامتها وأن قراءتها أو استعمالها من لدن الغير دون ترخيص أمر محتمل<sup>8</sup>.

- 1 - الفقرة الأخيرة من المادة الأولى من قانون 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع لشخصي.
- 2 - المادة 12 من قانون 09.08.

3 - Maria Winkler, Op Cit, p 113.

4- أوردته إمان التيس، التجارة الإلكترونية وضوابط حماية المستهلك في المغرب، أطروحة لنيل شهادة دكتوراه في القانون الخاص، جامعة مولاي اسماعيل، كلية العلوم القانونية والاقتصادية والاجتماعية بمكناس، نونبر 2014، ص 309-310.

5- Laurène BARRAU et Alexandre TESSONNEAU, Protection des données personnelles et risques juridiques pour l'entreprise, Revue Eco Management, n° 147, avril 2013, cet article sur le site d'Économie et Management [www.cndp.fr/revueEcoManagement](http://www.cndp.fr/revueEcoManagement), p 28.

6- يجب أن يحترم هذا الأخبار مجموعة من البيانات التي أوردتها الفقرة (ج) من المادة الأولى من قانون 08.09.

7- مثل الفئات التي سترسل إليها المعطيات الشخصية، وما إذا كان الجواب عن الأسئلة اختياريا أو إجباريا، وكذا العواقب المحتملة لعدم الجواب.

8- غير أن الحق في الأخبار هذا ليس مطلقا وإنما ترد عليه بعض الاستثناءات التي نصت عليها المادة 6 من قانون 09.08 من قبيل الحالة التي يكون فيها المعنى بالأمر على علم مسبقا بأن معطياته ذات الطابع الشخصي يمكن أن تتداول في الشبكات دون ضمانات السلامة، وأنها قد تتعرض للقراءة والاستعمال من لدن أغير غير مرخص لهم.

**الحصول على الإءذن المسبق:** إن المعطيات الشخصية ذات الطابع الحساس<sup>1</sup>، وكذا المعطيات الجينية<sup>2</sup>، إلى جانب تلك المتعلقة بالمخالفات أو الإءانات أو التءاءير الوقائية<sup>3</sup>، ءون نسيان المعطيات المضمنة ببطاقة التعريف الوطنية للمعني بالأمر تخضع لوءوب الحصول على الإءذن المسبق، ونفس الإءذن يجب الحصول عليه إذا تعلق الأمر باستعمال المعطيات ذات الطابع الشخصي لغايات أخرى غير تلك التي جمعت لأجلها، مع مراعاة الاستثناءات المنصوص عليها قانونا<sup>4</sup>.

**وءوب الحصول على التصريح المسبق:** في الحالات الأخرى الغير مذكورة أعلاه، أي حين لا يكون المسؤول عن المعالجة ملزما قانونا بالحصول على الإءذن المسبق، فإنه يكون ملزما بتقديم تصريح لءى اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي، وذلك بغرض تمكين اللجنة المذكورة من ممارسة الاختصاصات المخولة لها<sup>5</sup>، وإن كان البعض يقول بأن هذا التصريح واجب في كل معالجة، حيث يسري حتى على الحالات التي تقرر فيها الإعفاء من الحصول على الإءذن المسبق<sup>6</sup>.

### ب: الحماية الجنائية لخصوصية المستهلك في التجارة الإلكترونية

اتخذت الجريمة المعلوماتية بالمغرب خلال العقود الأخيرة صورا متعددة، وأمام القصور الذي أبانت عنه القوانين التقليدية، ءفع المشرع إلى سن العديد من المقتضيات الجنائية من أجل سد ذلك الفراغ التشريعي في مجال مكافحة هذه الجرائم<sup>7</sup>، كما أن وعي المشرع المغربي بخصوصية الإءرام المعلوماتي كأحد أهم مظاهر التطور التكنولوجي، وانعكاساته على أمن المجتمع المغربي ءفعه إلى أخذ هذه الظاهرة على محمل الجد<sup>8</sup>. ويعد القانون رقم 03-03 المتعلق بمكافحة الإرهاب أول قانون تضمن إشارة صريحة للإءرام المعلوماتي في المغرب<sup>9</sup>، ليزءاء اهتمام المشرع بهذا الصنف من الجرائم ويتوء بإلحاق العديد من النصوص الجنائية سواء بمقتضيات القانون الجنائي أو ببعض النصوص الخاصة<sup>10</sup>، خاصة القانون رقم 03-07 المتعلق بالإءلال بسير نظم المعالجة الآلية للمعطيات. ولبحث الموضوع أكثر سنحصره في فءتين من الجرائم: تلك التي تستهدف المس بنظم المعالجة الآلية للمعطيات (1)، إلى جانب الجرائم التي تستهدف المعطيات والوءائق المعلوماتية (2).

1 - راجع البءء الثالث من المادة الأولى من قانون 09.08

2 - باستثناء المعطيات المستعملة من لءن مستءءمي الصحة لأغراض طبية، سواء تعلق الأمر بالطلب الوقائي أو بالفحوصات أو العلاجات؛

3 - باستثناء تلك المنفءة من لءن أعوان القضاء.

4 - تطرق لهذه الاستثناءات البءء الرابع من المادة الأولى من قانون 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي.

5 - الفقرة الأخيرة من المادة 12 و المادة 13 من قانون 09.08.

6 - العربي جنان، م س، ص 110.

7 - أمين أعزان و عبد السلام جاكيمي، الحماية التقنية والجنائية للنظم المعلوماتية، المءلة المغربية للقانون الجنائي والعلوم الجنائية، 2015، العدد الثالث، ص 61

8 - عبد الحكيم زروق، م س، ص 448.

9 - ظهير شريف رقم 140-03-1 صادر في 26 من ربيع الأول 1424 (28 ماي 2003) بتنفيذ القانون رقم 03-03 المتعلق بمكافحة الإرهاب.

10 - كما هو الشأن بالنسبة للمادة 32 من قانون 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية التي تجرم استيراد أو توريد أو استءلال أو استعمال إءءى وسائل أو خدمات التشفير ءون الإءلاء بالتصريح أو الحصول على الترخيص المنصوص عليهما في المءءتين 13 و 14 من نفس القانون. كما نجد المادة 35 ءء عاقبت على كل استعمال غير قانوني للعناصر الشخصية لإنشاء الوقائع المتعلقة بتوقيع الغير، وحماية لءجية الشهادة الإلكترونية جرمت المادة 37 الاستمرار في استعمال الشهادة المذكورة بعد انتهاء مءة صلاحيتها أو بعد إلغائها.

## 1: الجرائم التي تستهدف المس بنظم المعالجة الآلية للمعطيات

حرص المشرع المغربي من خلال القانون رقم 03-07 المتتم لمجموعة القانون الجنائي والمتعلق بالإخلال بسير نظم المعالجة الآلية للمعطيات، والذي يحتوي على تسعة فصول من 3-607 إلى 11-607، على مواكبة الجريمة المعلوماتية وتوفير نوع من الحماية الجنائية للوثيقة الإلكترونية وللمعطيات ذات الطابع الشخصي، حيث سعى إلى وضع الإطار القانوني الخاص بتجريم الأفعال التي تمس نظام المعالجة الآلية، ولعل أبرز هذه الأفعال :

### ◀ الدخول أو البقاء غير المشروع في النظام المعلوماتي<sup>1</sup>:

يقصد بفعل الدخول، الولوج إلى المعلومات المخزنة بالحاسب الآلي، ممن ليس له الحق في هذا الولوج، ويتحقق هذا الفعل إما بالدخول المباشر إلى المعلومات أو عن طريق الاعتراض غير المشروع لعمليات الاتصال من أجل الدخول إلى النظام السالف الذكر<sup>2</sup>. أما البقاء غير المشروع فهو " عبارة عن نشاط إجرامي يتمثل في بقاء المتهم داخل النظام المعلوماتي بعد دخوله إليه عرضاً أو عن طريق الخطأ، ضداً على إرادة من له الحق في السيطرة على هذا النظام"<sup>3</sup>، وبالتالي نلاحظ بأن المشرع قد افترض سوء نية ذلك الشخص ساقته المعلوماتية لنظام شخص آخر دون أن يحاول الخروج منه، بل إن عنصر البقاء هذا حسب البعض<sup>4</sup> "هو ما يجعل هذه الجرائم من جرائم العمد"، فبقاؤه وعدم انسحابه من النظام من شأنه أن يمس بسرية المعطيات التي يحتويها النظام، مما يكون معه التجريم مشروعاً من خلال إتيان فعل سلمي هو عدم الخروج.

### ◀ جريمة عرقلة سير النظام أو إحداث خلل فيه:

عاقب الفصل 5-607 من ق ج بالحبس من سنة إلى ثلاث سنوات وبالغرامة من 10.000 إلى 200.000 درهم أو بإحدى هاتين العقوبتين " كل من عرقل عن عمد سير نظام المعالجة الآلية للمعطيات أو أحدث خللاً فيه"، ويبدو جلياً من خلال هذا الفصل أن المشرع يشترط العمد لقيام الجريمة، مما يضعنا أمام جريمة عمدية يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصره: العلم والإرادة. أما عن الركن المادي لهذه الأخيرة فيتحقق عن طريق توقيف أو تعطيل نظام المعالجة الآلية للمعطيات عن أداء نشاطه العادي والمتنظر منه القيام به أي كانت الوسيلة المستخدمة، على اعتبار أن المشرع لم يشترط حصول الجريمة بوسيلة معينة بذاتها.

وبالتالي "فقد تكون وسيلة العرقلة مادية (تكسير الحاسوب، سكب سائل عليه، قطع شبكات الاتصال...)، كما قد تتخذ شكلاً معنوياً إذا وقعت على الكيانات المنطقية للنظام كالبرامج والمعطيات، وذلك بإدخال برنامج فيروس خبيث، أو ملئها بمعلومات ومعطيات تفوق سعتها الحقيقية..."<sup>5</sup>. أما فيما يخص الخلل الذي قد يطال النظام فيتخذ صوراً متعددة، من بينها بطؤ عمل النظام المعلوماتي أو توقف المعالجة الآلية للمعطيات<sup>6</sup>.

1- قد يتحقق فعل الدخول بعدد من الطرق " ففي بعض الحالات قد لا يتطلب فعل الدخول أكثر من تشغيل برنامج الحاسوب أو فتح البرنامج الذي يعمل بواسطته النظام، وفي حالات أخرى، يتطلب الدخول وسائل أكثر تعقيداً، كما في حالة الحصول على الشفرات الخاصة بالدخول باستخدام جهاز فك الشفرة ". عبد الحكيم زروق: م س، ص 453

2- عبد الوهاب لعبل، م س، ص 50 و 52

3- عبد السلام بنسليمان، الإجماع المعلوماتي في التشريع المغربي، دراسة نقدية مقارنة في ضوء آراء الفقه وأحكام القضاء، الطبعة الأولى، دار الأمان، الرباط، 2017، ص 78.

4- عبد المجيد كوزي، م س، ص 113.

5- أورده عبد الحكيم زروق، م س، ص 457.

6- أمين أعزان، عبد السلام جاكيمي، م س، ص 64.

## 2: الجرائم التي تستهدف المعطيات والوثائق المعلوماتية

سوف نقسم دراسة هذه الجرائم إلى شطرين، ندرس في الأول تلك التي يكون محلها بيانات نظام المعالجة المعلوماتية (1.2)، وفي الثاني تلك التي ترد على الوثائق المعلوماتية (2.2).

### 1.2: الاعتداء العمدي على بيانات نظام المعالجة المعلوماتية

تعتبر جريمة الاعتداء على بيانات نظام المعالجة الآلية من الجرائم العمدية التي ترد على "محل وموضوع محدد هو المعطيات الموجودة داخل النظام، أي تلك التي يحتويها النظام وتشكل جزءا منه"<sup>1</sup>. أما عن نشاطها الإجرامي فيتضح من خلال الفصل 6-607 بأنه يتجسد في القيام "بإدخال معطيات في نظم المعالجة الآلية للمعطيات أو إتلافها أو حذفها منه أو تغييرها، أو تغيير طريقة معالجة هذه المعطيات أو إرسالها عن طريق الاحتيال". وعليه فالسلوك الإجرامي بالنسبة لهذه الجريمة يتجسد في القيام بعملية من العمليات أعلاه، إذ يكفي أن يصدر عن الجاني إحداها فقط سواء ب:

-إدخال معطيات في نظام المعالجة الآلية: فقيام الجاني بمجرد إدخال معطيات جديدة في النظام أو إضافتها إلى البيانات المتواجدة فيه يقيم المسؤولية الجنائية في حقه، وهذا "راجع إلى طبيعة هذه البيانات والمعطيات، ذلك أنها لا تعدو أن تكون سوى رموز يتم إعدادها حسب منطق معين وتسلسل مدروس في غاية من الدقة، وبمجرد المساس بذلك التنظيم، ولو بإدخال عناصر أجنبية عليها، من شأنه أن يحدث اضطرابا عليها وعلى طريقة تحليلها"<sup>2</sup>.

-الإتلاف: يقصد بالإتلاف "التعدي على البرامج والمعطيات والبيانات المخزنة من خلال التلاعب بها أو إلغائها، سواء بإدخال معلومات مصطنعة، أو بإتلاف معلومات مخزنة بشكل يمنع الاستفادة منها، فتصبح بذلك هذه المعلومات غير صالحة للاستعمال وغير ذات أهمية"<sup>3</sup>، مع الإشارة هنا إلى أن المشرع في هذا الفصل أخذ بالمفهوم الواسع للإتلاف الذي قد ينصرف إما على كل من المعلومات بالنظام أو على جزء منها فقط.

- تغيير المعطيات أو تغيير طريقة معالجتها أو إرسالها: يقصد بتغيير المعطيات أو تغيير طريقة معالجتها أو إرسالها "تغيير المعطيات الموجودة داخل نظام للمعالجة الآلية للمعطيات واستبدالها بمعطيات أخرى، أو إجراء تغيير في مراحل ومكونات طريقة معالجتها أو إرسالها، وذلك بهدف الحصول على نتائج مغايرة عن تلك التي صمم النظام من أجلها"<sup>4</sup>.

-التدمير: التدمير هو كل عمل من شأنه أن يلحق ضررا بشيء ما فيؤدي إلى إفساده وانعدام جدواه<sup>5</sup>، ويعد تدمير المعلومات من بين صور الإتلاف الأكثر تصورا في الواقع العملي، ويتخذ شكلين رئيسيين، محو المعطيات كلياً أو إخفائها وعدم إتاحة فرصة الوصول إليها<sup>6</sup>.

### 2.2: تزوير الوثيقة المعلوماتية واستعمالها

التزوير في صورته التقليدية هو تغيير الحقيقة في محرر بإحدى الطرق التي حددها القانون تغييراً من شأنه أن يرتب ضرراً للغير، أما " التزوير المعلوماتي فهو تغيير الحقيقة في المستندات المعالجة آلياً والمستندات المعلوماتية، وذلك

1- عبد الحكيم زروق، م س، ص 459.

2- عبد المجيد كوزي، م س، ص 121.

3- عبد السلام بنسليمان، م س، ص 90.

4- عبد الحكيم زروق، م س، ص 461.

5- وليد العاكوم، م س، ص 18.

6- عبد الوهاب لعل، م س، ص 60.



بنية استعمالها " <sup>1</sup>. وقد نص المشرع على هذا الفعل الجرمي من خلال الفصل 7-607 <sup>2</sup> ليكون بذلك قد حصن مصالح المتعاقدين عبر شبكة الانترنت، خاصة وأن "فعل التزوير بوصفه أحد أنماط الغش المعلوماتي، عرف تزايداً سريعاً في الآونة الأخيرة، وذلك بالقدر الذي تحل فيه المحررات الإلكترونية محل المستندات العادية في شتى المجالات" <sup>3</sup>، فلأجل هذا كان لا بد من مجابهة هذه الظاهرة سواء في صورتها المادية أو المعنوية.

**بالنسبة للتزوير المعنوي** نص المشرع على طرقة الثلاث في الفصل 353 من القانون الجنائي <sup>4</sup>:

- تغيير إقرار أولي الشأن
- جعل واقعة مزورة في صورة واقعة صحيحة
- جعل واقعة غير معترف بها في صورة واقعة معترف بها.

ولعل ما يميز هذا التزوير أن مهمة الكشف عنه تكتنفها صعوبات عدة، باعتباره لا يبرز بالعين المجردة، فكشفه يتطلب المزيد من التحقيق والفحص والتمحيص في مضمون المحرر لمعرفة ما إذا كان صحيحاً أو غير صحيح، وطبعاً هذه العملية تحتاج لدوي الخبرة والكفاءة لما لهم من قدرة على كشف التزوير، ولما يتوفرون عليه من أدوات ووسائل تمكن من ذلك <sup>5</sup>.

**أما فيما يخص التزوير المادي** فيتم عن طريق التدخل من خلال النظام المعلوماتي وذلك عبر تغيير المحررات بالحذف بإزالة كلمة أو رقم أو رمز معين، أو عن طريق الإضافة بزيادة رقم على مبلغ معين، أو بإضافة عبارات أو بيانات غير صحيحة، أو بخلق محرر لم يكن له وجود، فيقوم بتسجيل بيانات لم تصدر عن المتعاقدين أو ذوي الشأن، أو إثبات وقائع كاذبة أو غير معترف بها، أو إغفال معلومة أو إيرادها على وجه غير صحيح <sup>6</sup>.

وقد نص المشرع المغربي على طرقة في الفصلين 352 و354 من ق.ج على سبيل الحصر وفق الشكل التالي:

- وضع إمضاءات أو أختام أو بصمات مزورة: وذلك بأن ينسب المحرر المزور إلى شخص لم يصدر عنه، على أساس أن ظهور إمضاء شخص أو ختمه في محرر يعني أن ما يتضمنه قد صدر عنه، فالإمضاء وما في حكمه هو رمز الشخصية ودليلاً، ويكون الإمضاء مزوراً متى وضع الجاني إمضاء شخص آخر في المحرر.
- تغيير المحرر أو الكتابة أو التوقيع أو زيادة كلمات: كزيادة رقم أو ملئ فراغات متروكة على بياض، أو عن طريق الحذف بإزالة كلمة أو رقم، أو باخو أو الشطب أو الطمس الخ، "فكل تعديل مادي يدخله الجاني على المحرر، سواء اتخذ صورة إضافة أو حذف، أو ملئ فراغات أو استبدال لكلمة أو عبارة أو رقم أو توقيع، من شأنه أن يغير مضمون المحرر" <sup>7</sup> يدخل في نطاق التزوير المادي.

- 1- سمية مزغيش، م س، ص 51.
- 2- الفصل 7-607: "يعاقب... كل من زور أو زيف وثائق المعلومات أياً كان شكلها، إذا كان من شأن التزوير أو التزييف إلحاق ضرر بالغير... وتطبق نفس العقوبة على كل من استعمل وثائق المعلومات المشار إليها في الفقرة السابقة وهو يعلم أنها مزورة أو مزيفة".
- 3- عبد الحكيم زروق، م س، ص 463.
- 4- ينص الفصل 353 من ق ج بأنه "يعاقب بالسجن المؤبد كل واحد من رجال القضاء أو الموظفين العموميين أو الموثقين أو العدول ارتكب بسوء نية، أثناء تحرير ورقة متعلقة بوظيفته، تغيير في جوهرها أو في ظروف تحريرها، وذلك إما بكتابة اتفاقات تخالف مراسمه وما أملاه الأطراف المعنية، وإما بإثبات صحة وقائع يعلم أنها غير صحيحة، أو بإثبات وقائع على أنها اعتراف بما لديه، أو حدثت أمامه بالرغم من عدم حصول ذلك، وإما بحذف أو تغيير عمدي في التصريحات التي تلقاها.
- 5- عبد اللطيف بن موسى، الحماية الجنائية للمحرر الإلكتروني من التزوير المعلوماتي، مجلة العلوم الجنائية، 2014، العدد الأول، ص 97.
- 6- زكريا بوشورة، م س، ص 130.
- 7- جميلة عباوي، الحماية الجنائية للمعاملات الإلكترونية، المجلة المغربية للقانون الجنائي والعلوم الجنائية، 2016، العدد 3، ص 85.

- وضع أسماء وصور أشخاص آخرين مزورة: يتحقق التزوير المادي في هذه الحالة بقيام الجاني باستعمال أو إبدال شخصيته بشخصية الغير، حيث يتسمى باسم شخص آخر ويوقع على المحرر بالاسم الذي انتحله. ويمكن تصور وقوع التزوير المعلوماتي للصورة عبر الحاسب الآلي والأجهزة المساعدة له والتي منها (Scanner) عن طريق رسم الصورة ونقلها إلى جهاز الحاسب الآلي، أو إدخالها على بيانات مخزنة في ذاكرة الحاسب الآلي نفسه وعرضها على الشاشة دون طباعة ورقية، سيما أن التزوير المعلوماتي لا يتطلب المستند الورقي المكتوب أو المطبوع<sup>1</sup>. وإذا كان الأمر لا يطرح أي إشكال بالنسبة للآراء السالفة، حيث ارتأت بأن مسألة إسقاط التزوير العادي على ذلك المعلوماتي مسألة لا تثير أي إشكال، فإن الأستاذ علمي مشيشي الإدريسي يرى بأن الإحالة الضمنية للمادة 607-7 على القواعد العامة لا يمكن قبولها لا منطقيا ولا قانونا، نظرا لما يتميز به الزور المعلوماتي من خصوصيات لا يمكن أن تنفع معها الجرائم المثبتة في الزور الكلاسيكي، لأجل ذلك يقترح الأستاذ إضافة مادة تحمل رقم 607-7 مكرر تلي مباشرة المادة 607-7 تنص على:

"يقصد بتزوير أو تزيف وثائق المعلومات في المادة السابعة، تغيير أو محو معطيات، تكون مجمعة، معالجة أو مرسله نظام معلوماتي، أو القيام بأية وسيلة تكنولوجية بتغيير الاستعمال الممكن للمعطيات في النظام المذكور، وذلك بهدف تغيير المدى القانوني لتلك المعطيات"<sup>2</sup>.

## خاتمة:

إن موضوع الحماية القانونية لخصوصية المستهلك في التجارة الإلكترونية يعد من المواضيع المتجددة باستمرار، لارتباطه وتأثره بالتطورات الحاصلة، خاصة بعد دخول التقنية في حياتنا اليومية عبر أجهزة متعددة، مختلفة ومتنوعة، حتى أصبحنا نعيش في مجتمع شفاف، لا أحد فيه على طبيعته المعهودة، فهو مراقب أينما حل وارتحل. يقول فرانك موريس، وهو محام في مكتب (Epstein Becker and Green) في واشنطن: "فقط أولئك الذين تعرضوا لتجربة مؤلمة يشعرون بخطورة الأمر، أما الآخرون فالغالب الأعظم أنهم غير واعين بأهميتها"<sup>3</sup>، فالمسألة تكسني خطورة قصوى، لارتباطها بحياة الفرد الخاصة بما تحمله من أسرار، والتي أضحت وسيلة تعتمد لتمرير المنتجات والخدمات بعدما كانت حتى عهد قريب غاية، مما يطرح أمام المشرع المغربي كما هو الشأن بالنسبة لباقي دول المعمور تحديات عديدة، تشريعية وهيكلية ومؤسسية، في أفق التوفيق بين حماية هذه الحياة والتقدم التكنولوجي في ظل هذا الزمن الموجه.

ولعل ما يطرح التحدي على نحو أكبر هو طبيعة هذه البيئة الإلكترونية، وتنظيمها الذي لا يدرك له نطاق، في غياب تام لأي هيئة مركزية، إلى جانب خضوعها المطلق للعديد من القوى الاقتصادية، الشيء الذي يتطلب تعاوناً بين سائر دول المعمور من أجل التصدي لمختلف هذه المخاطر.

1- عبد اللطيف بن موسى، الحماية الجنائية للمحرر الإلكتروني من التزوير المعلوماتي، مجلة العلوم الجنائية، 2014، العدد الأول، ص 96.

2- محمد علمي مشيشي الإدريسي، دراسة مقارنة حول ملائمة مشروع القانون الجنائي مع المبادئ والقواعد المعتمدة في منظومة حقوق الإنسان، الطبعة الأولى، دون ذكر المطبعة 2011، ص 215.

3- بن سعيد صبرينة، م س، ص 1.