ISSN:2509-0291

Volume 11 issue 1
N:62 FEBRUARY 2026

جريمتي النفاذ والبقاء داخل النظام المعلوماتي في القانون الموريتاني.

الدكتور : محمد سعيد العالم

دكتوراه في القانون الخاص والعلوم الجنائية من جامعة المنار بتونس،

وأستاذ قانون خاص متعاون بكلية الحقوق والعلوم السياسية بجامعة نواكشوط.

ملخص

يتناول هذا المقال بالدراسة والتحليل جرائم الاعتداء على الأنظمة المعلوماتية في القانون الموريتاني، مركزاً على جريمتي النفاذ والبقاء داخل النظام المعلوماتي وفقاً للقانون رقم 07-2016 المتعلق بالجرائم المعلوماتية .

يبرز المقال أهمية حماية الأنظمة المعلوماتية في ظل التطور التكنولوجي وما يرافقه من تهديدات رقمية متزايدة، كما يوضح أن المشرع الموريتاني تأثر بالاتفاقية الأوروبية للجريمة الإلكترونية، فاستلهم منها تعريف النظام المعلوماتي ومفاهيم التجريم.

.يناقش البحث الركنين المادي والمعنوي لهاتين الجريمتين، وموقف الفقه من مسألة المحاولة فيهما، مبرزاً الجدل حول الطبيعة الشكلية لجريمة النفاذ .كما يستعرض النظام العقابي الموريتاني، ملاحظاً تدرج العقوبات وتشديدها في جريمة البقاء مقارنة بالنفاذ .ويختم المقال بتأكيد أهمية تبني تشريعات أكثر وضوحاً وفعالية لضمان حماية الأنظمة المعلوماتية وردع الجرائم الإلكترونية.

"The Crimes of Unauthorized Access and Maintaining Presence in an Information System under Mauritanian Law"

Mohamed Said EL ALEM

Ph.D. in Private Law and Criminal Sciences from the University of El Manar, Tunisia.

Adjunct Professor of Private Law at the Faculty of Law and Political Science, University of Nouakchott.

Abstract :

This paper examines crimes against information systems under Mauritanian law, focusing on the offenses of unauthorized access and unlawful remaining within an information system, as defined by Law No. 07-2016 on cybercrime. It highlights the growing need for digital protection amid rapid technological advancement and increasing cyber threats. The study notes that the Mauritanian legislator was influenced by the European Convention on Cybercrime, adopting its terminology and definitions. The article analyzes both the material and moral elements of these crimes and discusses the debate on the concept of 'attempt' in formal offenses like unauthorized access. It also reviews the penalties imposed, noting that Mauritanian law applies stricter sanctions for unlawful remaining than for unauthorized access. The paper concludes by stressing the necessity of clearer and more effective legal mechanisms to safeguard information systems and deter cybercriminal behavior.

نتائج البحث:

1. **نجح المشرع الموريتاني جزئياً في إدراج حماية جنائية للأنظمة المعلوماتية** من خلال القانون رقم 07-2016، إلا أن التطبيق العملي ما زال يواجه بعض الصعوبات بسبب غموض بعض المصطلحات القانونية المترجمة عن نصوص أجنبية.

2. **تأثر التشريع الموريتاني بشكل واضح بالاتفاقية الأوروبية للجريمة المعلوماتية (بودابست 2001)**، سواء في تعريف النظام المعلوماتي أو في تكييف الأفعال المجرّمة، وهو ما أضفى على القانون طابعاً دولياً لكنه قلّل من دقته في السياق المحلي.

3. **تميّز المشرع بين جريمتي النفاذ والبقاء داخل النظام المعلوماتي**، معتبراً أن جريمة البقاء تمثل ظرفاً مشدداً، مما يعكس وعياً بخطورة الاستمرار غير المشروع في الأنظمة الرقمية بعد اختراقها.

4. **وسع المشرع نطاق التجريم ليشمل المحاولة في جرائم النفاذ والبقاء**، رغم أن الفقه يثير جدلاً حول إمكانية تصور المحاولة في الجرائم الشكلية، وهو ما يعد توجهاً محل نقاش فقهي وقضائي.

5. **النظام العقابي الموريتاني يتسم بالتدرج والتشديد النسبي**، حيث تراوحت العقوبات بين السجن والغرامة، مع مراعاة طبيعة الفاعل (طبيعي أو معنوي)، وقد شدد المشرع العقوبة في جريمة البقاء مقارنة بالنفاذ.

6. **اعترف المشرع بالمسؤولية الجنائية للذات المعنوية** في الجرائم المعلوماتية، وهو توجه حديث يعزز الرقابة المؤسسية ويكرس مبدأ مساءلة الشركات والمؤسسات عن الأفعال الإجرامية التي تقع لحسابها.

7. **غياب بعض الضوابط الدقيقة في تحديد العقوبات المالية والحدود الدنيا والقصوى** يضعف من فعالية الردع ويمنح القاضي سلطة تقديرية واسعة قد تخل بمبدأ الشرعية الجزائية.

8. **يُظهر القانون الموريتاني توجهاً نحو حماية المجال الرقمي**، لكنه ما زال يحتاج إلى تحديثات تقنية وتشريعية تراعي التطور السريع لأساليب الجرائم الإلكترونية.

9. **الحماية القانونية الحالية تركز على الجانب الزجري أكثر من الوقائي**، ما يستدعي تعزيز التدابير التقنية والرقابية إلى جانب الردع الجنائي.

10. **توصي الدراسة بتبني نصوص أكثر دقة ووضوحاً**، وتكوين قضاة ومتخصصين في المجال المعلوماتي لضمان تطبيق فعال وعادل لهذا القانون المستحدث.

المقدمة:

نتيجة التطور العقلي للإنسان، أصبح العالم اليوم يعيش ثورة حقيقية في مجال التكنولوجيا والاتصالات، إذ أن العالم تجاوز مرحلة الطفرة الصناعية إلى مرحلة المعلوماتية بفضل ظهور شبكات المعلومات، ووسائل الاتصال الحديثة[312]، والتي من أهمها الحاسوب الإلكتروني الذي يلعب دورا هاما في إتمام العمليات المطلوبة بطريقة سريعة ودقيقة والتي تكون خاضعة للمعالجة الآلية للبيانات،[313] ورغم أهمية هذه الوسائل في حياتنا اليومية، الا أنها أصبحت بيئة للجرائم المستحدثة والتي تعرف اليوم **"بالجرائم الإلكترونية" أو ما يسمى "بالجرائم الافتراضية" ،أو "جريمة الفضاء الإلكتروني" أو "جرائم الاعتداء على الأنظمة المعلوماتية"[314]**

ومهما تعددت وتنوعت تسميات ومصطلحات هذا النوع من الجرائم فإن جميع هذه الجرائم المرتبطة بالتكنولوجيا والاتصال فإنها تتمثل أساسا في بعض الأفعال الغير مشروعة مثل الاستخدام السيئ للحاسوب، أو اختراق النظم المعلوماتية، أو

312 فتحي محمد أنور عزت : الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، دار الكتب القانونية،الطبعة الثانية،-مصر- 2010، ص 15.

313 علي كحلون : الجرائم المتعلقة بالمحتوى المعلوماتي، مجلة القضاء والتشريع نوفمبر 2003، ص 12، 13، 15.

314 محاضرة الوفد التونسي في المؤتمر التاسع لرؤساء المحاكم العليا : الجرائم الإلكترونية الواقعة على الأشخاص في القانون التونسي، بيروت، 17-19-2018، ص 1.

الاحتيال المعلوماتي، وغيرها من الأفعال المحظورة315 ، وعلى ذلك الأساس فإن اللجنة الأوروبية قد قسمت هذا النوع من الجرائم إلى ثلاثة أصناف كلها يمثل سلوكا إجراميا مثل الاعتداء على النظم المعلوماتية، أو نظم المعالجة الآلية للمعطيات، وجرائم الاحتيال المعلوماتي ، إضافة إلى الأشكال التقليدية للجرائم مثل السرقة والاحتيال المعلوماتي316، غير أن ما يهمنا في هذا المقال هو ***جرائم الاعتداء على النظم المعلوماتية في القانون الموريتاني*** ، والتي تناولها المشرع الموريتاني في القانون رقم 07-2016 الصادر بتاريخ 20 يناير2016 المتعلق بالجرائم المعلوماتية.

وقد عرف المشرع الموريتاني النظام المعلوماتي في المادة 9 من نفس القانون بكونه "**كل نظام معزول أوكل مجموعة أنظمة مشبكة أو متقاربة، تضمن أو يضمن أحد عناصرها، تنفيذ برنامج كليا أو جزئيا بمعالجة آلية البيانات**"317.

إن المتأمل في هذا التعريف يدرك جيدا أنه تم استلهامه أو ربما ترجمته حرفيا من التعريف الوارد في الاتفاقية الأوروبية المتعلقة بالجريمة المعلوماتية والمؤرخة في 23 نوفمبر 2001، حيث عمد المشرع الموريتاني إلى ترجمة النص حرفيا مما انعكس على التعريف الذي أورده المشرع، وهو ما تجلى في عبارات غامضة مثل "**نظام معزول" أنظمة مشبكة أو متقاربة**".

ومهما يكن، وبغض النظر عن الكلمات الغامضة باللغة العربية ،نتيجة الترجمة فإن النظام المعلوماتي حسب تعريف المشرع يعني إما نظاما منفردا أو مجموعة أنظمة مترابطة فيما بينها، وهذه الأنظمة تقوم وظيفتها أساسا على أن تضمن مجتمعة أو يضمن أحد عناصرها تنفيذ برنامج محدد بشكل كلي أو جزئي بمعالجة آلية للبيانات.

ويعرف التقرير التفسيري لاتفاقية الجريمة الالكترونية الدولية الصادرة عن مجلس أوروبا النظام المعلوماتي بأنه " **أي جهاز يشمل المد خلات والمخرجات ،ويتألف من أجهزة وبرمجيات تم تطويرها من أجل المعالجة التلقائية للبيانات الرقمية، ويمكن أن يشمل المدخلات والمخرجات ،ومر افق التخزين ، ويمكن أن يشتغل لوحده ، أو أن يكون متصلا بشبكة مع غيرها من الأجهزة المماثلة "318**.

ويتبيّن من هذا التعريف أن النظام المعلوماتي يتكون من أجهزة مادية ، ومن برامج وتطبيقات مترابطة فيما بينها على أساس تنفيذ برنامج معين ،وقد يكون بشكل منفرد أوبشكل مترابط مع أجهزة أخرى"**320.319**.

تاريخيا يرجع الفقه الجنائي جرائم الاعتداء على الأنظمة المعلوماتية إلى العام 3211960، فالجرائم المرتبطة بالأنترنت ارتباطا "عضويا"، فقد بدأت منذ السبعينات وخصوصا بداية من 1971 إلى 1990، وكانت الجرائم في هذه الفترة قليلة جدا يتراوح عددها ما بين جريمة واحدة إلى ثلاثة جرائم في العالم، وأشهرها 1988 عندما تم استخدام الحاسب الآلي لسرقة بنك، بمبلغ 70 مليون دولار من بنك شيكاغو الوطني الأول First national of Chicago، وفي عام 1988 تم لأول مرة تكوين فريق طوارئ الحاسب الآلي (CERT) في جامعة كارنيجي لمواجهة هو النوع من الجرائم.

وقد أشار مركز شكاوي احتيال الانترنت (IFFC) الأمريكي، والذي تأسس سنة 2000 أنه خلال ستة أشهر فقط من تأسيسه بلغت عدد الشكاوي 6087 من ضمنها 5273 تتعلق باختراق النظم المعلوماتية للكمبيوتر322، مع الإشارة إلى أن هذه الحالات

315Salangeghenauti-Heli : la cybercriminalité 1er Edition presses polytechniques et universitaire Bomande, Lausanne, 1er Edition 2009, p 16.

316 Myriam Quémener :cyber fraude, Revue Banque 1er Edition Paris, 2011, p 9.

317 المادة 9 من قانون 2016-007 المؤرخ في 29 فبراير 2016.

318 التقرير التفسيري لاتفاقية الجريمة الإلكترونية الصادر عن مجلس أوروبا في 23 نوفمبر 2001.

319 ذكره خالد ممدوح في كتابه : "التقاضي الإلكتروني" دار الفكر الجامعي الإسكندرية 2009، ص 298.

320 علي كحلون : الجريمة المعلوماتية وتوجهات محكمة التعقيب مجلة القضاء والتشريع 2013.

321 عبد العال الدريدي : الجرائم الإلكترونية، المركز القومي للإصدارات القانونية مصر 2012،الطبعة الاولى ، ص 23.

322 يونس عرب :ورقة عمل مقدمة إلى مؤتمر الأمن العربي، تنظيم المركز العربي للدراسات والبحوث الجنائية، أبو ظبي، 2002، ص 1.

تتعلق فقط بعدد الشكاوى لا عدد المتضررين، كما كشفت تقارير أمريكية أن خسائر العالم تقدر بحوالي مائة وأربعة عشر مليار دولار سنويا323

و تشير الإحصائيات في الجزائر إلى أن الاعتداء على النظم المعلوماتية في الجزائر يتراوح ما بين 200إلى 250 اعتداء يوميا324.

هذه الإحصائيات المختلفة تؤكد مدى انتشار الجرائم الواقعة على النظم المعلوماتية، ولذلك كان لابد للقانون الجزائي أن يتصدي لهذه الجرائم بنصوص جزائية خاصة، إذ أن النصوص التقليدية أصبحت عاجزة عن مسايرة هذه الجرائم، وهو ما سار عليه المشرع الموريتاني على غرار الكثير من التشريعات المقارنة، ومن هنا نطرح الإشكالية التالية:

ما مدى توفيق المشرع الموريتاني في تكريس حماية جنائية ناجعة للأنظمة المعلوماتية من شأنها ردع السلوكيات غير المشروعة في المجال الافتراضي؟

ان الإجابة عن هذه الإشكالية تتطلب منا ابرازمظاهرتجريم النفاذ والبقاء داخل النظام المعلوماتي في مطلب1 ثم نظام العقوبة مطلب2.

المطلب الأول: تجريم النفاذ والبقاء داخل النظام المعلوماتي.

يعتبر الاعتداء على سرية النظم المعلوماتية هواية مفضلة لدى محترفي الإجرام المعلوماتي، بغاية إبراز قدراتهم الفنية العالية، وإثبات مهاراتهم في كسر سرية الأنظمة المعلوماتية، بهدف الحيازة الغير مشروعة لكلمات المرور، واختراق هذه النظم ومن ثم العبث بها وإتلافها، وسرقة محتواها، والاستيلاء على المكتسبات المادية

ويأخذ الاعتداء على سرية النظم المعلوماتية صور متعددة، من أهمها النفاذ مع البقاء دون وجه حق (الفقرة الأولى) إضافة إلى البقاء داخل النظام المعلوماتي والاستمرار فيه (الفقرة الثانية).

الفقرة الأولى: جريمة النفاذ الى النظام المعلوماتي.

يشكل النفاذ مع البقاء دون وجه حق في نظام معلوماتي أو في جزء منه، صورة من صور الاعتداء على سرية النظم المعلوماتية .

وقد جرم المشرع الموريتاني هذا الفعل في المادة 6 من رقم 2016-007 على أنه **"كل من يقوم أو يحاول القيام عن قصد وبدون حق بالنفاذ إلى كل أو جزء من نظام معلوماتي يعاقب..."325.**

يتضح من خلال هذه المادة تجريم فعل النفاذ دون وجه حق إلى نظام معلوماتي أو إلى جزء منه.

ولم يعرف المشرع الموريتاني النفاذ كما أنه لم يتطرق الى الطرق التي يمكن من خلالها النفاذ، لكن بالرجوع إلى التقرير التفسيري لاتفاقية بوادست الأوروبية المتعلقة بالجريمة المعلوماتية نجد أن عبارة **"النفاذ غيرالقانوني"** تشكل الجريمة الأساسية الخطيرة الموجهة ضدّ أمن أنظمة الكومبيوتر، وتشمل جميع الصور التي يتم النفاذ دون وجه حق سواء كان ذلك بمعنى **"قرصنة" أو "كسر" أو "اختراق الكومبيوتر"**326.

فالنفاذ هو فعل الدخول غير المصرح به بكامل أو داخل جزء من نظام معلوماتي، وتعتبر جريمة النفاذ أكثر جرائم النظم المعلوماتية شهرة وانتشارا **327**

323 سليمان قواري : أعمال المؤتمر الدولي الرابع عشر مرجع سابق، ص 3.

324أمحمدي بوزينة : أعمال الملتقى الوطني، آليات مكافحة الجريمة الإلكترونية ،الجزائر، 29 مارس 2017، ص 79.

325 المادة 6 من القانون رقم 2016-007.

326 التقرير التفسيري لاتفاقية بوادبست، 2001.

327 Caroline HEYMANS :Nos instruments pénaux sont ils efficaces pour la lutter contre les infractions de criminalité informatique ? université catholique de Louvain Mémoire Master Belgique 2014_2015 P 37

وقد جرم المشرع فعل النفاذ دون وجه حق في المادة 6 من القانون المتعلق بالجريمة الالكترونية، وهي نفسها جريمة المادة 323/1 من المجلة الجنائية الفرنسية**328**

وتتكون هذه الجريمة من عنصرين، عنصر السلوك المادي المتمثل في فعل الدخول، إضافة إلى النية الإجرامية.**329**

وتشير عبارة **"دون وجه حق"** التي أوردها المشرع إلى الدخول الغير مرخص، سواء كان الدخول في كامل النظام أم في جزء منه فقط.

ولم يتعرض المشرع الموريتاني -كما أسلفنا -إلى الطريقة التي يتم بها النفاذ، وهو نفس التوجه المشرع التونسي حين جرّم النفاذ في المادة 199 مكرّر م.ج **"... كل من ينفذ..."** دون تحديد وسيلة النفاذ**330**.

ولئن لم يتعرض المشرع الموريتاني لطرق النفاذ، فإن المشرع الفرنسي أيضا لم يفرق بين طرق النفاذ، حيث اعتبرت محكمة استئناف باريس أن القانون قد عنى كل طرق الدخول الغير شرعي للأنظمة المعلوماتية لمعالجة البيانات دون استثناء.

وهو ما جعل أحد الفقهاء الفرنسي يطرح التساؤل حول الطبيعة القانونية لجريمة النفاذ هل هي جريمة حينية أم مستمرة وقد انقسم الفقهاء إلى شقين.

-الشق الأول :جريمة مستمرة باعتبارها تمتد لفترة وهي الفترة التي يبقى فيها الجاني متصل بالنظام.

-الشق الثاني : يرى بأنها جريمة حينية، باعتبارها تشبه جريمة السرقة، إذ لا تستغرق إلا الوقت الكافي لتنفيذها ولكنها جريمة حينية ذات أثر ممتد**331**.

و تقوم جريمة النفاذ سواء تم النفاذ بشكل كامل أم في جزء فقط من النظام ،وهو ما أشارت إليه المادة 6 من القانون رقم 2016-007 حيث استعمل المشرع عبارة "النفاذ إلى كل أو جزء من النظام".

ولا تقوم الجريمة إلا إذا كان هذا النفاذ دون وجه حق أي دون ترخيص ،وهو ما يتضح من خلال عبارة المشرع **"بدون حق"** إذ يشترط في النفاذ أن يكون دون ترخيص لكي يتكون الركن المادي للجريمة ، كما تقوم الجريمة بمجرد النفاذ إلى النظام المعلوماتي دون حق سواء كان النظام محميا أم غير محمي، وإن كان هناك جدل فقهي حول هل تقوم جريمة النفاذ إذا لم يكن النظام المعلوماتي محمي بأدوات وأساليب الحماية المعروفة(التشفير..)**333332**.

لكن المشرع الوطني لم يشترط أن يكون النظام المعلوماتي محميا ليجرم النفاذ، وهو ما ذهب إليه المشرع الفرنسي والتونسي أيضا حيث أن مفهوم الشرعية ينحصر في الجانب القانوني وليس الجانب الفني فعبارة النفاذ جاءت مطلقة، وعبارة القانون إذا جاءت مطلقة تؤخذ على إطلاقها تطبيقا لمبدأ التأويل الضيف للنص الجزائي**334**.

ويوسع المشرع في نطاق التجريم في جريمة النفاذ ، بحيث يجرم محاولة النفاذ الى النظام المعلوماتي، وهو توجه قد يكون توجه محل انتقاد للمشرع الموريتاني، إذ لا يمكن تصور المحاولة في جريمة النفاذ، باعتبار أن جريمة النفاذ جريمة شكلية تتحقق بمجرد وقوع النشاط المادي دون حاجة لتحقيق نتيجة إجرامية وبالتالي لا يكون هناك مجال للحديث عن المحاولة، فلا يعد مجرد حيازة كلمة مرور من قبل من ليس له الحق فيها شروعا في هذه الجريمة**335**.

---

328 Art 323/1 du code pénal Français.

329 Jean Pradel :les infractions relative a l informatique revue internationale de droit compare N°2 Avril_juin 1990 P 823

330 قانون عدد 89 لسنة 1999 المؤرخ في 2 أوت 1999.

331 منية ترايديت غمارسة :جرائم المعلوماتية في القانون التونسي ;القانون المقارن والقانون الدولي، دار الكتاب، تونس ،الطبعة الأولى، 2015، ص 54.

332 Jean Pradel op.cit. P 824

333 علي كحلون، الجريمة المعلوماتية وتوجهات محكمة التعقيب مرجع سابق

334 منية ترايديت غمارسة، مرجع سابق، ص 55.

335 فتحي محمد أنور عزت : الأدلة الإلكترونية، مرجع سابق، ص 299.

فتجريم المحاولة في جريمة النفاذ وهي جريمة شكلية أثار جدلا فقهيا كبيرا بين الفقهاء القانونيين، إذ يصعب تصور المحاولة في الجرائم الشكلية.

فالفقه الجنائي يشترط ركنين أساسين لتوفر أركان المحاولة :وهما الشروع في تنفيذ الجريمة إضافة إلى عدم إتمام هذه الجريمة لأمر خارج عن إرادة الجاني، **336**وبالتالي فإن الإشكال يتعلق بالركن الأول للمحاولة في الجرائم الشكلية وهو البدء بالتنفيذ، إذ يصعب التفريق بين البدء في التنفيذ وبين الأفعال التي يمكن أن تشكل أفعالا تحضيرية .

ويبدو أن المشرع الموريتاني تأثر بالفقه الفرنسي الذي اعتبر المحاولة في جريمة النفاذ ممكنة.

وقد أثار إشكالية تحديد البدء في التنفيذ النائب الفرنسي THYRAUD في مناقشات داخل البرلمان الفرنسي، لكن المقرر في البرلمان الفرنسي رد على النائب بأنه يمكن كشف محاولات اختراق الأنظمة بطريقة غير مشروعة من خلال جرائد موجودة داخل الأنظمة المعلوماتية تحفظ في ذاكرتها محاولات الاختراق الغير المشروعة وبالتالي يمكن تصور المحاولة في الاختراق حتى ولو كانت جرائم شكلية، **337** ورغم ذلك فإن هناك جانب من الفقه كبير يرى بأنه لايمكن تصور المحاولة في جريمة النفاذ باعتبارها من الجرائم الشكلية وخصوصا في المجال المعلوماتي.

ويتحقق الركن المعنوي لجريمة النفاذ بمجرد أن يكون الجاني على علم بأنه يقوم بعمل يحجره القانون، إذ يكفى لقيام هذه الجريمة أن يكون الجاني قد قام بفعلته **"عن قصد"** وهو ما يعني توفر العلم والإرادة، دون القصد الجزائي الخاص، أي دون الحاجة إلى توفر نتيجة إجرامية، أو ضرر في النظام المعلوماتي.

جدير بالذكر أن جريمة النفاذ تعاقب عليها المادة 6 من الاتفاقية العربية لمكافحة تقنية المعلومات والموقع عليها من طرف موريتانيا 21/12/2010**338**.

ب جريمة البقاء في النظام المعلوماتي:

نصّت المادة 7 من قانون رقم 2016- 007 على أنه "**كل من يقوم أو يحاول القيام عن قصد وبدون حق بالاستمرار داخل نظام معلوماتي أو في جزء منه يعاقب...**" ويتضح من هذه المادة أنّ المشرع يجرم البقاء داخل النظام المعلوماتي إذا لم يكن دون وجه حق وهو ما أشار إليه بعبارة "**بالاستمرار**".

البقاء أو الاستمرار في نظام الحاسوب يعني سيطرة المحترف على تفاعل الحاسوب مع حركة الدخول والخروج، فالبقاء في النظام المعلوماتي هي جريمة مستقلة عن جريمة النفاذ.

فالبقاء Maintenir se لا تعني قيام المحترف بارتكاب إتلاف أو تعطيل، وإنما يعني أن المحترف قام بالتحكم في نظام المعالجة الآلية للمعطيات، والتحكم قد يكون بأي وسيلة**339** ويعرف الفقيه Bufflant البقاء أنه **"يكون هناك بقاء بصفة غير شرعية عندما ينفذ شخص غير مسموح له بالنفاذ صدفة أو عن طريق الخطأ إلى النظام ويبقى مترتبط عمدا عوضا عن قطع الاتصال فورا "340**،وقد يتم البقاء في نظام معلوماتي أو في جزء منه لمدة طويلة.**341**

وجريمة البقاء مثل النفاذ لا تقتصر على كامل النظام بل يكفي البقاء في جزء منه لتكتمل أركان الجريمة،**342** وهو ما أشارت إليه المادة 7 من القانون الموريتاني **"الإستمرار داخل نظام معلوماتي أو جزء..."**

ولم يتعرض المشرع لصور البقاء لكن الفقه الجنائي يميز بين ثلاث صور من صور البقاء تشكل كل منهما فعلا إجراميا :

---

336 فرج القصير :القانون الجنائي العام ،مركز النشر الجامعي .تونس.2006،ص101

337 منينة تراديت غمارسة، مرجع سابق ص 103

338 المادة 6 من الاتفاقية العربية لمكافحة تقنية المعلومات.

339 فتحي محمد أنور عزت : مرجع سابق، ص 306.

340 جلال صولة، الجرائم المعلوماتية : رسالة تخرج من المعهد الأعلى للقضاء 2003-2004، ص 123.

341 Jean Pradel op.cit. P823

342 منية تراديت ، مرجع سابق، ص 58.

–البقاء داخل نظام معلوماتي من طرف شخص مرخص له لكنه لم ينسحب، أو تجاوز الوقت المسموح له به.

–البقاء قد يكون عن طريق الصدفة ،أو عن طريق الخطأ لكنّ لم ينسحب الشخص الموجود داخل النظام، فإذا لم ينسحب فورا من النظام فإن جريمة البقاء غير الشرعي قد تقوم عليه، إذا توافر الركن المعنوي وهو علم الجاني بأنه يقوم بفعل يحجره القانون، فهي جريمة قصدية تقوم بتوفر القصد الجنائي العام، وهذا ما أشار إليه المشرع الموريتاني في المادة7 من قانون رقم 2016-007 بعبارة "عن قصد"

–جريمة البقاء قد تأخذ صورة أخرى في حالة الوقت التي يطبع فيه الشخص نسخة من معلومات في حين انه لم يكن مسموح له سوى بالرؤية والإطلاع فقط343.

ويرى جانب من الفقه وهو الأقرب للصواب إلى اعتبار أن جريمة البقاء داخل النظام تبدأ منذ اللحظة الأولى التي يبدأ فيها الجاني بالدخول داخل النظام المعلوماتي أو يستمر في التجول بداخله بعد انتهاء الوقت المحدد ل له 344

وكما هو الحال في جريمة النفاذ فان المشرع يعاقب أيضا على محاولة البقاء ،ويلاحظ أن ركن المحاولة في جريمة البقاء أوضح من المحاولة في النفاذ، باعتبار إن الجاني قد ينفذ بطريقة شرعية لكنه حين يتجاوز الوقت المسموح له أو حين يرفض الخروج ويستمر داخل النظام أو جزء منه فان إشكال البدء ي التنفيذ قد لا يطرح كبير إشكال نظرا لتوفر النية الإجرامية .

نخلص من ذلك إن المشرع الموريتاني يجرم فعل البقاء داخل النظام المعلوماتي أو في جزء منه إذا كان ذلك البقاء دون وجه حق وعن سابق توفر قصد جنائي باعتبار إن البقاء دون وجه حق يشكل على غرار النفاذ صورة من صور الأفعال الماسة بسرية النظام المعلوماتي ، وقد رتب عقوبات جزائية لهذه السلكويات غير المشروعة.

المبحث المطلب الثاني: عقوبات الاعتداء على الأنظمة المعلوماتية

رتب المشرع الموريتاني على انتهاك أسرا النظم المعلوماتية عقوبات جزائية، ويبدو أن المشرع الموريتاني في تنظيمه للنظام العقابي قد تدرج، أو تراوح بين التخفيف والتشديد حسب طبيعة كل جريمة على حدى، سواء كان الجاني شخصا طبيعيا أم معنويا، وعلى العموم فقد تراوحت عقوباته بين العقوبات الأصلية والتكميلية ،المسلطة على لأشخاص الطبيعيين (الفقرة الأولى)أوا العقوبات المسلطة على الذات المعنوية(الفقرة الثانية) .

فقرة1: العقوبات المسلطة على الشخص الطبيعي

أقر المشرع الموريتاني جملة من العقوبات في جرائم الاعتداء على الأنظمة المعلوماتية ،وقد تراوحت هذه العقوبات مابين التخفيف والتشديد حسب طبيعة التجريم ،وحسب خطورتها، وعموما فان هذه العقوبات المسلطة على الشخص الطبيعي فإنها تتخذ صنفين من العقوبات :

أ- **العقوبات السجينة:**

وهي العقوبات الماسة بحرية الجاني، وتختلف حسب كل جريمة، من الجرائم الماسة بالأنظمة المعلوماتية.

فقد قرر المشرع عقاب الجاني في جريمة النفاذ دون وجه حق إلى النظام المشرع المعلوماتي بعقوبة حدها الأعلى ثلاث سنوات ،أما الحد الأدنى فهو سنة كاملة، ولم يشترط المشرع حصول الضرر في جريمة النفاذ، بل يكفي مجرد النفاذ لكي يعاقب الجاني.

أما في عقوبة البقاء دون وجه حق في نظام معلوماتي، فإن المشرع قد حدّد العقوبة السجنية سنتين كحدّ أدنى، وأربع سنوات كحدّ أقصى.،وهنا يمكن أن نلاحظ أن المشرع الموريتاني لم يحدّد عقوبة واحدة لجريمتين النفاذ والبقاء، بل شدّد في جريمة البقاء، أو اعتبر أن البقاء في نظام معلوماتي هو ظرف تشديد ، فهو لم يحدد كما أسلفنا عقوبة واحدة لجريمتي النفاذ والبقاء، كما فعل

343 منية ترادیت، مرجع سابق، ص 59.

344 منية ترادیت ، مرجع سابق، ص 60.

المشرع الفرنسي في المادة 1-323 من م المجلة الجنائية الفرنسية، إذ أقر عقوبة سجينة حددها بسنتين سواء في جريمة النفاذ أم البقاء، إلاّ أنه رفع من جريمة النفاذ في حاله حصول ضرر إلى ثلاث سنوات**345**،وهوتقريبا نفس التوجه سار عليه المشرع التونسي، إذ أنه لم يفرق في العقوبة بين جريمتي النفاذ والبقاء، أي أقر لها عقوبة واحدة في المادة 199 مكرر من م.الجزائية، حيث حدّد شهرين كأدنى عقوبة سجنية، وعام واحد كحدّ أقصى**346** ،فالحدّ الأقصى في جريمة النفاذ المجرد في القانون التونسي هي عام واحد، وكذلك أيضا المشرع الفرنسي.

أما المشرع الموريتاني فحدّد ثلاث سنوات كحدّ أقصى في جريمة النفاذ وأربع سنوات في جريمة البقاء، وهذا يعد تشديدا وتكريسا للنزعة العقابية، كما يعدّ اجتهادا ومحاولة لإضفاء خصوصية على النص التجريمي بطابعه الخاص، وربما يكون قد نجح في ذلك إلى حدّ بعيد باعتبار أن جريمتي النفاذ والبقاء جريمتان مستقلتان عن بعضهما البعض فالمشرع الموريتاني شدّد في جريمة البقاء، باعتبار أن البقاء لا يمكن تصوره دون النفاذ، وبالتالي البقاء في النظام بعد النفاذ يعتبر طرف تشديد، وهذا اجتهاد منطقي بالنظر إلى خطورة هذا النوع من الجرائم.

أمّا جريمة إعاقة النظام المعلوماتي ،أو إدخال بيانات معلوماتية داخل نظام معلوماتي ف، فقد اقر المشرع الموريتاني عقوبة أدنى تتمثل في سنتين، وعقوبة أقصى قدرها أربع سنوات هذه الجريمة يقابلها في التشريع الفرنسي جريمتين المادة 2-323 م.ج.ف**347**،حيث أن المشرع الفرنسي أقرّ خمس سنوات كعقاب في هذه الجريمة، ولم يحدّد الحدّ الأدنى بل اكتفى بالتنصيص على الحدّ الأقصى، ويلاحظ من خلال هاتين الجريمتين في التشريع الموريتاني والفرنسي، أن المشرع الموريتاني قد أعطى سلطة تقديرية للقاضي في تسليط العقوبة بين أربع سنوات كحدّ أقصى وسنتين كحدّ أدنى، وبينما المشرع الفرنسي لم ينص على الحدّ الأدنى ،كما نلاحظ أيضا أن جريمة إدخال بيانات في القانون التونسي يعاقب عليها بخمس سنوات أيضا لكنه أضاف خصوصية غير موجودة في القانون الفرنسي والموريتاني، وهي مضاعفة هذه العقوبة إلى 10 سنوات سجن إذا ارتكبت من طرف شخص أثناء مباشرته لنشاطه المهني حسب منطوق الفصل 199 مكرّر الفقرة الخامسة**348**.

وقد أعطى المشرع الموريتاني للقاضي حرية اختيار بين العقوبة السجنية أو العقوبة الماسة بالذمة المالية.

ب -العقوبات الماسة بالذمة المالية.

رغبة من المشرع في التصدي للجرائم الماسة النظم المعلوماتية فقد اقر عقوبات مالية إلى جانب العقوبات السجنية ،كما يلاحظ أنه يتدرج في الترفيع من الخطايا المالية كلما كانت الجريمة أخطر، فقد حدّد في جريمة النفاذ عقوبة مالية تتراوح بين 100000 أوقية و 2000000، بينما رفع العقوبة في جريمة البقاء من 200000 أوقية إلى 3000000 أوقية، ويلاحظ أيضا من خلال العقوبات المالية أن المشرع أعطى خصوصية كبيرة لجريمة البقاء داخل النظام المعلوماتي، إذ لم يجعل عقوبتهما واحدة سواء العقوبة السالبة للجريمة أم العقوبة المالية، وهو ما يدل على أنه لم يساوي بينهما عن دراية وقصد.

أما جريمة تعطيل النظام أو إدخال بيانات إضافية بشكل غير مشروع داخل نظام معلوماتي، فقد حدّد العقوبة بنفس العقوبة التي قرّرها بجريمة البقاء، وهي مبلغ 200000 أوقية، أو 3000000 أوقية، ولم يتعرض المشرع الموريتاني لحالة إذا ما كانت هذه الجريمة قد تم ارتكابها من طرف موظف أثناء تأديته لمهامه، كما فعل المشرع التونسي.

ولم يكتفي المشرع الموريتاني بتسليط العقاب على الشخص الطبيعي فحسب بل أيضا كرّس المسؤولية الجزائية للذات المعنوية، وسلّط عليها عقوبات في حالة ارتكابها لإحدى هذه الجرائم.

345.Article 223-1 du code pénal Français

346 المادة 199 مكرّر فقرة أولى من المجلة الجزائية التونسية.

347.Article 223-1 du code pénal Français

348 بلعسلي ويزة :االمسؤولية الجزائية للشخص المعنوي عن الجريمة الإقتصادية أطروحة دكتوراة ، جامعة مولود معمري 2014، ص 96.

الفقرة الثانية: العقوبات المسلطة على الذات المعنوية.

نصّت المادة 34 من القانون الموريتاني رقم 2016-007 المتعلق بالجريمة السبرانية أن الأشخاص الاعتباريين مسئولون جنائيا عن الجرائم المنصوص عليها في هذا القانون ،وكذلك أيضا المادة 96 من قانون رقم 2017-020المتعلق بحماية البيانات ذات الطابع الشخصي، المسؤولية الجزائية للذات المعنوية، وبالتالي إقرار عقوبات مالية وإدارية في حالة اعتدائهم على الأنظمة المعلوماتية.

وقد استثني المشرع الموريتاني الدولة والجماعات المحلية والمؤسسات العمومية، وعلة هذا الاستثناء، أن الدولة لا يمكن أن تكون طرفا في النزاع باعتبارها من يملك

الحق في العقاب، ويسلط العقوبة، إذ يرى جانب من الفقه الجنائي عدم إمكانية إسناد المسؤولية الجزائية للدولة باعتبار مركز السيادة، وبالتالي فإن الدولة لا يمكن أن تكون موضوعا الجنائي، هذا التبرير أورده وزير العدل الفرنسي في جلسة برلمانية خلال مناقشة قانون العقوبات الفرنسي الجديد ،وهوالموقف تبناه المشرع الموريتاني في استبعاد الدولة والجماعات المحلية والمؤسسات العمومية من المؤاخذة الجزائية في إطار الجريمة المعلوماتية، وكذلك أيضا في قانون حماية البيانات ذات الطابع الشخص، غير أنه كرّس المسؤولية الجزائية للذات المعنوي في جرائم الاعتداء على النظام المعلوماتي ووسع في نظامها.

وتستند المسؤولية الجزائية للذات المعنوية في نطاق المعلوماتية في الجرائم التي تتم ارتكابها لصالحهم، أو لحسابهم من قبل شخص طبيعي سواء كان يتصرف فرديا أو بصفته عضوا في هيئة من هيئات الشخص الاعتباري ويمارس سلطة إدارة داخلها.

وقد حدّد المشرع بعض السلط المسئولة جنائيا في حالة ارتكاب إحدى الجرائم في نظام المعلوماتية.

أ- سلطة تمثل الشخص الاعتباري

ب- سلطة لاتخاذ القرارات باسم الشخص الاعتباري

ج- سلطة لممارسة رقابة داخل الشخص الاعتباري

ويمكن أن تطال المسؤولية الجزائية للذات المعنوية حسب مقتضيات الفصل 34 من قانون رقم 2016-007 هؤلاء الأشخاص في حالة إذا ما كان غياب المراقبة، أو رقابة الشخص المعنوي كان سببا لارتكاب إحدى هذه الجرائم

هذا التوسع في نطاق التجريم يعكس رغبة المشرع في التصدي للإجرام المعلوماتي، من خلال إسناد المسؤولية الجزائية للذات المعنوية وهو ما يحتم على الذات المعنوية ضرورة الرقابة، ومراقبة المسئولين**349**.،إضافة إلى أنّ المشرع نص صراحة أن مسؤولية الشخص الاعتباري لا تحول دون مسؤولية الشخص الطبيعي الذي يرتكب نفس الأفعال سواء كان بصفته فاعلا أصليا أو مشاركا وهو ما عبر عنه بعبارة "المتواطئين"، وهو نفس التمشي الذي تبناه في قانون حماية المعطيات الشخصية، وقد أقر العقوبات التالية للشخص المعنوي في إطار ارتكابه لإحدى هذه الجرائم.

1- الغرامة التي يساوي حدها الأقصى خمسة أضعاف تلك المقررة على الأشخاص الطبيعيين ،ويلاحظ أنه لم ينص على تحديد العقوبة بالحدّ الأدنى أو الحدّ الأقصى للغرامة وهو بذلك لم يترك السلطة التقديرية للقضاة بين الحدّ الأقصى والحدّ الأدنى، وهو ما يمكن أن ينزل بالغرامة إلى مستوى بسيط**350**، وبالتالي فإن العقوبة ستفقد نجاعتها ووظيفتها، كما أنه خرق لمبدأ شرعية الجرائم والعقوبات الذي ينص أن الجريمة والعقوبة بحسب أن تكون محددة بنص صريح، فالقاضي لا يختلق القانون ،وإنما يطبق القانون وبالتالي فإن عدم التنصيص على مناط العقوبة سيترك الحرية للقاضي في تسليط الغرامة، وهو خطأ يجب تداركه**351**.

349 المادة 34 من قانون رقم 2016-007.

350بلعسلي ويزة، مرجع سابق، ص 86.

351 المادة 34 من قانون 2016-007.

2- الحلّ: إذا تعلق الأمر بشخص اعتباري أو بعقوبة سجن يتجاوز خمس سنوات إذا يتعلق الأمر بشخص طبيعي ،ويلاحظ هنا أن المشرع قرّر عقوبة الحلّ إذا كانت العقوبة المستوجبة للسجن تفوق خمس سنوات، سواء كانت من طرف شخص اعتباري أو طبيعي، وبالتالي أقصى الجرائم المتعلقة بالاعتداء على الأنظمة المعلوماتية، باعتبار أن العقوبات المستوجبة للسجن فوق خمس سنوات في هذا القانون هي فقط الجرائم المتعلقة بالمادة الإباحية للأطفال، أو الجرائم المرتكبة من طرف عصابة منظمة.

3- عقوبة ماسة بالنشاط المهني مثل الحظر النهائي أو لمدة أقصاها خمس سنوات.

4- عقوبة ماسة بوجود الشركة: الإغلاق النهائي أو لمدة أقصاها خمس سنوات لواحدة أو أكثر من مؤسسات الشركة التي شاركت في ارتكاب الجريمة.

5- الاستبعاد من الصفقات العمومية بشكل دائم أو لمدة أقصاها خمس سنوات.

6- عقوبة ماسة بالذمة المالية: أي الحجر أو مصادرة الشيء الذي استخدم أو الذي كان موجها لارتكاب الجريمة أو الشيء الذي نتج عنها:

7- عقوبة ماسة بالسمعة: أي إلصاق قرار قضائي ونشره سواء عن طريق الصحافة المكتوبة أو عن طريق أي وسيلة اتصال وخصوصا بالطرف الإلكترونية.

وقد أضاف المشرع بعض العقوبات التكميلية فإن المشرع نص في المادة 37 من قانون 2016-007 ا لتي قد تطال الشخص المعنوي و الطبيعي معا

–في حالة الإدانة بسبب جريمة ارتكبت عن طريق دعامة اتصال، يمكن للقاضي أن يأمر بنشر القرار عن نفس الدعامة، وعلى نقصه المحكوم عليه وأن يكون عن طريق مستخرج في الصفحة الأولى خلال خمسة عشر يوما الموالية لليوم الذي أصبحت فيه الإدانة نهائية.

–أيضا حجز المعدات والتجهيزات والآليات والبرامج المعلوماتية وكل الوسائل والبيانات المترتبة بالجرائم، وذلك مع الاحتفاظ الغير من ذوي النوايا الحسنة، تصادر الأجهزة والمعدات، وإتلاف البرامج المتعلقة بالجريمة.

❖ قائمة المراجع

القو انين الوطنية والدولية والتقارير:

الاتحاد الأوروبي) .2001 .(التقرير التفسيري لاتفاقية الجريمة الإلكترونية الدولية .مجلس أوروبا، ستراسبورغ.

القانون الفرنسي رقم 323-1 من المجلة الجنائية الفرنسية .(Code pénal français)

القانون الموريتاني رقم 2016-07 الصادر بتاريخ 20 يناير 2016، المتعلق بالجرائم المعلوماتية.

القانون الموريتاني رقم 2017-20، المتعلق بحماية البيانات ذات الطابع الشخصي.

محكمة استئناف باريس) .1995 .(قرار يتعلق بالدخول غير المشروع إلى الأنظمة المعلوماتية وفق المادة 323-1 من المجلة الجنائية الفرنسية.

مركز شكاوي احتيال الإنترنت .(2000) .(Internet Fraud Complaint Center - IFFC) التقرير نصف السنوي الإلكتروني .واشنطن: وزارة العدل الأمريكية.

فريق الطوارئ الحاسوبي (1988) .(Computer Emergency Response Team - CERT) تقرير حول الاختراقات ا جامعة كارنيجي ، الولايات المتحدة.

بنك شيكاغو الوطني الأول .(1988) .(First National Bank of Chicago) قضية سرقة إلكترونية عبر الحاسب الآلي بقيمة 70 مليون دولار.

هيئة الأمم المتحدة المعنية بالجريمة والعدالة .(2019) .(UNODC) تقرير الجريمة السيبرانية والتنمية المستدامة . نيويورك.

اللجنة الأوروبية لمكافحة الجريمة الإلكترونية) .2002 .(التقرير السنوي حول الجريمة المعلوماتية في أوروبا .بروكسل.

منظمة الشرطة الجنائية الدولية (الإنتربول)) .2020 .(تقرير حول الاتجاهات الحديثة في الجريمة الإلكترونية .ليون، فرنسا.

المراجع المتخصصة باللغة العربية والفرنسية:

فتحي محمد أنور عزت : الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، دار الكتب القانونية، الطبعة الثانية،-مصر- 2010.

علي كحلون : الجرائم المتعلقة بالمحتوى المعلوماتي، مجلة القضاء والتشريع في تونس نوفمبر 2003.

محاضرة الوفد التونسي في المؤتمر التاسع لرؤساء المحاكم العليا : الجرائم الإلكترونية الواقعة على الأشخاص في القانون التونسي، بيروت، 17-19-2018.

.

خالد ممدوح: "التقاضي الإلكتروني" دار الفكر الجامعي الإسكندرية 2009.

1 علي كحلون : الجريمة المعلوماتية وتوجهات محكمة التعقيب مجلة القضاء والتشريع في تونس 2013.

عبد العال الدريدي : الجرائم الإلكترونية، المركز القومي للإصدارات القانونية، الطبعة1 مصر 2012.

يونس عرب :ورقة عمل مقدمة إلى مؤتمر الأمن العربي، تنظيم المركز العربي للدراسات والبحوث الجنائية، أبو ظبي، 2002.

أمحمدي بوزينة : أعمال الملتقى الوطني، آليات مكافحة الجريمة الإلكترونية ،الجزائر، 29 مارس 2017.

منية تراديت غمارسة :جرائم المعلوماتية في القانون التونسي ;القانون المقارن والقانون الدولي، دار الكتاب، تونس ،الطبعة الأولى، 2015.

فرج القصير :القانون الجنائي العام ،مركز النشر الجامعي .تونس.2006.

بلعسلي ويزة :االمسؤولية الجزائية للشخص المعنوي عن الجريمة الإقتصادية أطروحة دكتوراة ، جامعة مولود معمري 2014.

Caroline HEYMANS :Nos instruments pénaux sont ils efficaces pour la lutter contre les infractions de criminalité informatique ? université catholique de Louvain Mémoire Master Belgique 2014_2015

Jean Pradel :les infractions relative a l informatique revue internationale de droit compare N°2 Avril_juin-1990

1Salangeghenauti-Heli : la cybercriminalité 1er Edition presses polytechniques et universitaire Bomande, Lausanne, 1er Edition 2009.

1Myriam Quémener :cyber fraude, Revue Banque 1er Edition Paris, 2011