الأمن السيبراني كمدخل استراتيجي للحكامة الضريبية بالمغرب: دراسة مقارنة

Cybersecurity as a Strategic Approach to Tax Governance in Morocco:
A Comparative Study

عبد العزيز موهيب Mouhib Abedelaziz

دكتور في الحقوق

أستاذ زائر بكلية الحقوق بسطات

الملخص

يُمثِّل الأمن السيبراني في العصر الرقمي مدخلاً استراتيجياً حيوياً لضمان أمن الدول واستقرار مؤسساتها الحيوية، ولا سيما في مجال الحكامة الضريبية حيث ينطلق المقال من الإشكالية الرئيسية المتمثلة في تحديد دور الأمن السيبراني في تأمين حكامة الإدارة الضريبية بالمغرب، وذلك في ظل التحول الرقمي المتسارع وتصاعد حدة التهديدات الإلكترونية المتنوعة التي تستهدف البنى التحتية المعلوماتية والبيانات الحساسة.

ويعتمد المغرب إطاراً تشريعياً مزدوجاً ومتكاملاً يجمع بين حماية الحقوق الفردية وتأمين الفضاء الرقمي. كما يتمثل هذا الإطار في قانون 13-05 المتعلق بحماية المعطيات ذات الطابع الشخصي، الذي يركز على الضمانات الجوهرية للخصوصية ويُخضع الإدارة الضريبية لالتزامات صارمة بشأن شرعية المعالجة والشفافية وتناسب الغرض وتأمين البيانات. كما يمنح الملزمين حقوقاً فعالة كحق الوصول والتصحيح. في المقابل، يركز قانون 05-20 المتعلق بالسلامة السيبرانية على الحماية الهيكلية والاستراتيجية للبنى التحتية المعلوماتية الحيوية، مُلزِماً الجهات الخاضعة له، ومنها الإدارة الضريبية في حال تصنيفها كمشغل للمرافق الحيوية، بواجبات معززة تشمل تبني منهجيات متقدمة لإدارة المخاطر، وإجراء اختبارات الاختراق، ووضع خطط استمرارية الأعمال، والإبلاغ الإلزامي عن الحوادث للوكالة الوطنية للسلامة السيبرانية (ANSI).

ومن جهة أخرى يسجل النموذج المغربي نجاحه في التكامل العضوي بين هذين التشريعين، إذ يشكل قانون 13-05 خط الدفاع الداخلي لحماية البيانات ذاتها، بينما يشكل قانون 05-20 خط الدفاع الخارجي والاستراتيجي لحماية الأنظمة والشبكات. كما يخلق هذا التكامل مساءلة مزدوجة للإدارة الضريبية أمام الأفراد عبر اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي (CNDP)، وأمام الدولة عبر الوكالة الوطنية للسلامة السيبرانية (ANSI).

رغم متانة هذا الإطار النظري، فإن تطبيقه العملي يواجه تحديات جسيمة، أبرزها صعوبة التنسيق بين الجهات الرقابية (CNDP وANSI)، والتحديات التقنية المرتبطة بسرعة تطور التهديدات الإلكترونية، ونقص الموارد البشرية والمالية، والإشكالات المتعلقة بالعامل البشري الذي يظل حلقة ضعف محتملة. لتعزيز الفعالية الحمائية، يقترح المقال آليات مثل تعزيز

التعاون المؤسسي عبر مذكرات تفاهم، واعتماد معايير دولية كإطار عمل NIST، وإطلاق برامج توعوية وتدريبية مستمرة للموظفين، وتبني مبدأ "الأمن بالتصميم" في مشاريع الرقمنة.

الكلمات المفاتيح: الأمن السيبراني، الحكامة الضريبية، حماية المعطيات الشخصية، السلامة السيبرانية، اللجنة الوطنية لمراقبة حماية المعطيات الشخصية(CNDP) ، الوكالة الوطنية للسلامة السيبرانية(ANSI)

Summary

Cyber Security in the digital age represents a vital strategic approach to ensuring the security of states and the stability of their vital institutions, particularly in the area of tax governance. The article begins with the central question of defining the role of cyber security in ensuring the governance of tax administration in Morocco; this comes amid the accelerating digital transformation and the escalation of various cyber threats targeting information infrastructure and sensitive data.

Morocco adopts a dual and integrated legislative framework that combines the protection of individual rights and the security of the digital space. This framework is embodied in Law 13-05 on the Protection of Personal Data, which emphasizes fundamental privacy guarantees and subjects tax administrations to strict obligations regarding the legality of processing, transparency, proportionality of purpose, and data security.It also grants those liable effective rights, such as the right to access and correct. In contrast, Law 05-20 on Cyber security focuses on the structural and strategic protection of critical information infrastructure, obligating subject entities, including the tax administration if classified as an operator of critical facilities, to enhanced duties, including adopting advanced risk management methodologies and conducting penetration testing.Develop business continuity plans and mandatory incident reporting to the National Cyber Security Agency (ANSI).

On the other hand, the Moroccan model demonstrates its success in the organic integration between these two pieces of legislation. Law 13-05 constitutes

the internal line of defense for protecting the data itself, while Law 05-20 constitutes the external, strategic line of defense for protecting systems and networks. The human factor remains a potential weak link. To enhance protection effectiveness, the article proposes mechanisms such as strengthening institutional cooperation through memoranda of understanding, adopting international standards such as the NIST framework, launching ongoing awareness and training programs for employees, and adopting the « security by design » principle in digitization projects.

This integration also creates dual accountability for the tax administration towards individuals through the National Commission for the Control of Personal Data Protection (CNDP), and towards the state through the National Cyber security Agency (ANSI).

Despite the strength of this theoretical framework, its practical application faces significant challenges, most notably the difficulty of coordination between regulatory bodies (CNDP and ANSI), the technical challenges associated with the rapid development of cyber threats, and the lack of human and financial resources.

Keywords: Cybersecurity, Tax Governance, Personal Data Protection, Cybersecurity Safety, National Commission for the Control of Personal Data Protection (CNDP), National Cybersecurity Agency (ANSI)

مقدمة

لقد شهد العالم في العقود الأخيرة تحولاً جذرياً في مجال تكنولوجيا المعلومات والاتصالات، حيث أصبح الفضاء السيبراني بيئة حيوية للتفاعلات الاقتصادية والاجتماعية والسياسية. ومع هذا التطور، برزت تحديات جديدة تتمثل في الجرائم السيبرانية التي تهدد أمن الأفراد والمؤسسات والدول،[1] كما يرتبط هذا الأمن، ارتباطاً وثيقاً، بأمن المعلومات، فالوصول إلى هذه الأخيرة، أو بثها أو الاطلاع عليها والمتاجرة بها، أو تشويهها واستغلالها، هو ما يقف غالب الأحيان، وراء عمليات الاعتداء على الشبكات، وعلى الإنترنت.[2]

وبظهور استخدام الكمبيوتر وربطه بالشبكة في الستينيات إلى السبعينيات من القرن الماضي، ظهرت المعالجة الأولى لجرائم الكمبيوتر في شكل مقالات صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر والتجسس المعلوماتي، حيث بزغت قوى الشر لاستغلال هذا التقدم لتحقيق أغراض شخصية رخيصة على حساب قيم المجتمع، وحقوق الأفراد والجماعة وأمنهم. فما كان من أصحاب النفوس الضعيفة إلا أن تجرَّؤوا على تحويل شبكة الأمن السيبراني إلى مسرح يرتكبون فيه العديد من الجرائم والمخالفات: فقاموا بنشر الأخبار المزيفة، وبثوا الأفكار والممارسات المناهضة للأديان السماوية وللإنسانية، ونشروا الصور الفاضحة للصغار قبل الكبار، وانتهكوا حرمة الحياة الخاصة لأفراد المجتمع، وسبوا الأشخاص وقذفوهم، وتعدُّوا على حقوق الملكية الفكرية، وقد شهد القرن الواحد والعشرين تضاعف حجم الجرائم السيبرانية كما ونوعا، بسبب ارتفاع عدد مستخدمي الإنترنت ومعدلات الجرائم بالتبعية، نتجت عنها خسائر مالية ضخمة، أرغمت العديد من الدول لتبني خطط وبرامج تتفادى بها هذا الخطر المحدق، الذي بات يدمر البنى التحتية للمعلومات وتقنية الاتصالات والشبكات، والتفكير بالتالي بجدية في إعداد استراتيجيات تروم حفظ الأمن السيبراني.[3]

وتتجلى أهمية الأمن السيبراني وفق التشريعات المقارنة في حماية الأنظمة المعلوماتية تفاديا لأي وصول غير مصرّح به الى معلومات تعد السرية فيها ذات بعد استراتيجي هام، كما يعد تسريب البيانات، والهجمات الإلكترونية، وغيرها من التهديدات أمرا غير مرغوب فيه[4].

كما يعتمد الأمن السيبراني وفق إرادة المشرع على جملة من الإجراءات تهدف أساساً إلى ضمان سرّية الأصول الرقمية وسلامتها وتوافرها. ونظراً لتغيّر مشهد التهديدات باستمرار[1]، ويوفر الأمن السيبراني الحماية من جميع أشكال الحوادث السيبرانية

---

[1] – في عصر التحول الرقمي المتسارع أصبح الامن السيبراني أحد الركائز الأساسية لحماية البنى التحتية الرقمية والبيانات الحساسة للدول والمؤسسات والافراد.

[2] جبور، منى الاشقر، (2018) السيبرانية، هاجس العصر، جامعة الدول العربية، ص 241.

[3] – يشير الأمن السيبراني عموما إلى مجموع الوسائل المعتمدة لحماية أنظمة الحاسوب والشبكات والمعلومات الرقمية من الوصول غير المصرّح به، وتسريب البيانات، والهجمات الإلكترونية، وغيرها من التهديدات. بالاعتماد على إجراءات محددة تهدف أساساً إلى ضمان سرّية الأصول الرقمية وسلامتها وتوافرها. ونظراً لتغيّر مشهد التهديدات باستمرار، يُعَدّ الأمن السيبراني مجالاً معقداً ومتطوّراً يتطلّب مقاربة متعددة المستويات تشمل حلولاً تقنية وسياسات وإجراءات وتوعية المستخدمين للحد من المخاطر وحماية الأصول الرقمية بفعالية.

[4] –يعني الامن السيبراني أمن الشبكات والأنظمة المعلوماتية، والبيانات والمعلومات والأجهزة المتصلة بالإنترنت. وعليه؛ فهو المجال الذي يتعلق بإجراءات ومقاييس، ومعايير الحماية، المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات أو للحد من آثارها في أقسى وأسوأ الأحوال.

من خلال تعزيز سلامة البنية التحتية الحيوية للمعلومات التي تعتمد عليها القطاعات الحساسة، وتأمين الشبكات والخدمات التي توفر الاحتياجات اليومية للمستعملين. ويمكن للحوادث السيبرانية أن تؤثر على البنية التحتية للمعلومات الحيوية وغير الحيوية، وربما تأخذ أشكالاً كثيرة من أشكال الأنشطة الضارة مثل استخدام روبوتات النت botnet في الهجمات المتعلقة برفض الخدمة ونشر الرسائل الاقتحامية والبرمجيات الضارة (مثل الفيروسات وبرمجيات وورم التخريبية التي تؤثر في قدرة الشبكات على العمل. وبالإضافة إلى ذلك، قد تشمل الحوادث السيبرانية أنشطة غير مشروعة مثل التصيد الاحتيالي (phishing) والتحايل لسرقة المعلومات الشخصية(pharming) ، علاوة على سرقة الهوية والخطر السيبراني آخذ في الازدياد مع تزايد الأدوات والمنهجيات وتوفرها على نطاق واسع، ومع اتساع نطاق وتطور القدرات التقنية للمجرمين السيبرانيين. وقد تعرضت البلدان على مختلف مراحل تنميتها لهذه المخاطر السيبرانية.[2]

وكغيره من التشريعات المقارنة أولى المشرع المغربي عناية كبرى لهذا الموضوع، خاصة أمام المخاطر ذات البنية المركبة والوثيرة المتزايدة، حيث شهد المغرب ارتفاعا ملحوظا في عدد وأنواع الهجمات السيبرانية، سيما أمام تقدم التكنولوجي الذي يسر استخدام الشبكة العنكبوتية والاستفادة مما تتيحه من خدمات رقمية جد متطورة.

وهو واقع صح معه القول إن العالم اليوم أصبح مطالبا أكثر من أي وقت مضى ، بتظافر الجهود وتوحيد الخطط والاستراتيجيات، والرفع من مستوى التأطير لتحقيق منسوب توعوي قادر على مواجهة كل التحديات ذات الصلة بالتحول الرقمي، وإدراك مدى خطورة التهديدات التي بات يفرضها استعمال تكنولوجيات المعلومات، كالاتصالات في الفضاء السيبراني لضمان أمن المعلومات، وتأمين الموارد البشرية والمالية المرتبطة بتقنية الاتصالات والمعلوميات، بل السعي بشكل أساسي وبإمكانيات تقنية حديثة لخلق صمام الامان ، تجنبا لكل المخاطر والأضرار التي تترتب في حال ما لم تواجه بخطط استباقية قادرة على الحد من خطورة هذه الجرائم التي تعصف بحقوق الأفراد والجماعات.

تتمتع البيانات الضريبية بطبيعة خاصة تجعل من تأمينها مسألة سيادية وليست تقنية فحسب، وذلك للأسباب التالية:

1 .طابعها السري والخاص: تشكل البيانات الضريبية، بمقتضى القانون، بيانات شخصية ومالية حساسة تتمتع بالحماية القانونية (قانون 09-08 لحماية المعطيات الشخصية). إذ تحتوي على معلومات عن الذمة المالية للملزمين، ومصادر دخولهم، واستثماراتهم، مما يفرض حماية مشددة لها.

---

[1]- والظاهر أن الأمن السيبراني يتركب من كلمتي Cyber Security وكلمة سيبر لاتينية الأصل ومعناها الأمن المعلوماتي فيصبح المقصود بالأمن السيبراني الأمن المعلوماتي وهو تعبير أشمل وأعم من أمن المعلومات لذا يمكن القول أن الأمن السيبراني هو عبارة عن مجموع الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستخدام غير مصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات الشخصية ولحماية المواطنين.

[2]- السحيباني، عبد الله (2011): كفاءة الإجراءات الإدارية في المحافظة على أمن المعلومات، رسالة ماجستير، الرياض: جامعة نايف العربية للعلوم الأمنية. ص314.

2 .أهميتها الاقتصادية والمالية: تمثل هذه البيانات العمود الفقري لتخطيط السياسة المالية للدولة، وتقدير الإيرادات، وتمويل مشاريع التنمية. أي مساس بها يهدد الاستقرار المالي الوطني.

3. مصلحة الملزمين: يحق للملزم أن تظل بياناته محمية من الوصول غير المشروع أو التسرب أو الاستغلال، مما يساهم في بناء ثقته في المنظومة الضريبية ويدفعه إلى المزيد من الشفافية.

لمعالجة هذا المقال نرى الانطلاق من الإشكالية الرئيسية التالية:

- **أي دور للأمن السيبراني في تأمين حكامة الإدارة الضريبية بالمغرب؟**

المبحث الأول: نطاق الأمن السيبراني كما حددها التشريع الوطني والمقارن

المبحث الثاني: دور الأمن السيبراني في تأمين حكامة الإدارة الضريبية بالمغرب

المبحث الأول: نطاق الأمن السيبراني وفق التشريع الوطني والمقارن

في ظل الاعتماد المتزايد على تكنولوجيات المعلومات والاتصالات من قبل الدول والقطاع الخاص والأفراد، برزت ضرورة حتمية لضمان الاستخدام الآمن والمناسب للفضاء الرقمي بحيث يُشكّل هذا الضمان أحد أبرز التحديات العالمية المعاصرة للوقاية من المخاطر والمهددات السيبرانية المتنامية. واستجابة لهذا التحدي، تبذل العديد من الدول جهوداً حثيثة لتعزيز أطرها التشريعية والتنظيمية لمواكبة التسارع التكنولوجي، انطلاقاً من إدراكها أن تحقيق الأمن السيبراني يمثل ركيزة أساسية لضمان استقرار المجتمعات وتحقيق التنمية الاجتماعية والاقتصادية المستدامة.

لقد أدى التسارع الكبير في وتيرة التحول الرقمي والاعتماد شبه الكلي على البنى التحتية التكنولوجية، إلى إضفاء صفة الاستعجالية على وضع أطر قانونية متينة قادرة على حماية الأنشطة في الفضاء السيبراني، وتعزيز الثقة في المعاملات الإلكترونية التي يجريها الأشخاص الطبيعيون والاعتباريون على حد سواء. وعليه، اتجهت العديد من الدول إلى سن تشريعات ولوائح تنظيمية ملزمة في مجال الأمن السيبراني، بهدف تأمين نظم المعلومات، وضمان نجاعة عملية التحول الرقمي، والتصدي للجرائم السيبرانية، وحماية البيانات الشخصية والحيوية من سوء الاستخدام.

المطلب الاول: الجهود المبذولة في تعزيز التشريعات السيبرانية

لحماية البيانات الضريبية وغيرها من المعطيات ذات البعد الاستراتيجي الفردية منها والجماعية، بذلت مجهودات ملحوظة سواء على المستوى الإقليمي الدولي (أولا) أو على المستوى الوطني (ثانيا) كانت نتيجتها الفعلية ظهور ترسانات قانونية إلى حيز الوجود رغبة من المنتظم الدولي في خلق نوع من المواكبة لهذا التقدم التكنولوجي الهائل.

أولا: الجهود المبذولة في تعزيز التشريعات السيبرانية على المستوى الدولي.

استجابة للتهديدات السيبرانية المتطورة، سارعت العديد من الدول والمنظمات الدولية إلى تطوير أطرها التشريعية والتنظيمية، وبهذا الصدد قامت فرنسا بتعزيز ترسانتها القانونية في مجال الأمن السيبراني بشكل ملحوظ عام 2013 من خلال

قانون البرمجة العسكرية، إذ فرض هذا التشريع التزامات جديدة على المشغلين ذوي الأهمية الحيوية (Opérateurs d'importance Vitale -OIV)، بإلزامهم تعزيز أمن نظم المعلومات التي يستعملونها. كما ألزم القانون مشغلي شبكات الاتصالات بالمشاركة الفاعلة في رصد الهجمات السيبرانية التي تستهدف عملائهم، وقرر عقوبات رادعة على الجهات التي تخل بهذه الالتزامات.

ولنفس الغاية سعت الولايات المتحدة الأمريكية أيضاً إلى مواءمة تشريعاتها مع طبيعة التهديدات، حيث أقرت في عام 2015 إطاراً قانونياً شاملاً يحدد معايير وقواعد الحماية من التهديدات السيبرانية، بهدف حماية البنى التحتية الحرجة، وفي سبيل النجاعة الوقائية اتخذ الاتحاد الأوروبي بدوره خطوات تشريعية جادة، تمثلت في اعتماد توجيه (Directive) بشأن أمن الشبكات وأنظمة المعلومات) توجيه (NIS في عام 2016، بهدف رفع مستوى القدرات الأمنية cybersecurity للدول الأعضاء. كما شكّل اعتماد اللائحة العامة لحماية البيانات (GDPR) في عام 2018 نقلة نوعية في حماية البيانات الشخصية لمواطني الاتحاد، حيث وضع معايير صارمة لمعالجتها وفرض عقوبات مالية كبيرة على المخالفين.

كما أسهمت الأمم المتحدة من خلال فريق الخبراء الحكوميين (GGE) في وضع إطار معياري، حيث تم في عام 2013 الإقرار بتطبيق مبادئ وقواعد القانون الدولي على الفضاء السيبراني، مما يمهد الطريق لتنظيم سلوك الدول في هذا المجال.

ثانيا: الجهود المبذولة في تعزيز التشريعات السيبرانية على المستوى الوطني.

لقد انخرط المغرب في مسار تشريعي وتنظيمي متصاعد وذلك منذ عام 2011 في مسار طموح يهدف إلى تطوير القدرات الوطنية في أمن نظم المعلومات وتعزيز الثقة الرقمية.

1-الإطار الاستراتيجي: مما لا شك فيه أن هذا المسار قد تكلل باعتماد الاستراتيجية الوطنية للأمن السيبراني في عام 2012، والتي مثلت الخارطة طريق للمجهود الوطني في هذا المجال.

كما تم إصدار التوجيهات الوطنية لأمن نظم المعلومات، التي باشرت الإدارات والمؤسسات العمومية تطبيقها اعتباراً من عام 2014، كما بدل المغرب مجهودات ملحوظة لتحقيق الأمن السيبراني حيث عمل على محاكاة وتكييف أفضل الممارسات الدولية في مجال الأمن السيبراني، والتي تتشكل من خلال عدة أطر استراتيجية وتشريعية رئيسية:

أ-الاتحاد الأوروبي (المصدر الرئيسي للإلهام):

- توجيه NIS (Network and Information Security Directive): يركز على تعزيز أمن الشبكات ونظم المعلومات على مستوى الاتحاد، ويُلزم الدول الأعضاء برفع قدراتها الوطنية وفرض إخطارات بالاختراقات، هذا التوجيه أثر بشكل مباشر على استراتيجية المغرب فيما يخص حماية البنى التحتية الحرجة.

- اللائحة العامة لحماية البيانات (GDPR): تعتبر معيارًا ذهبيًا في حماية البيانات الشخصية. كان لها الأثر الأكبر في صياغة القانون 09-08 المغربي لحماية المعطيات الشخصية، حيث سعت المغرب إلى تحقيق "الملاءمة" معها لتسهيل تدفق البيانات مع الشريك الأوروبي.

– توجيه NIS 2 وتوجيه Resilience of Critical Entities (CER): يوسعان نطاق القطاعات الخاضعة للتنظيم ويزيدان من المتطلبات الأمنية، وهو اتجاه تتجه إليه التشريعات الحديثة.

ب–منظمات ومعايير دولية:

– اتفاقية بودابست (اتفاقية الجريمة الإلكترونية): تقدم إطارًا قانونيًا دوليًا لمكافحة الجريمة الإلكترونية وتسهل التعاون القضائي. المغرب ليس طرفًا فيها بعد، لكن تشريعاته تأخذ بعين الاعتبار مبادئها.

– المعيار الدولي لإدارة أمن المعلومات، الذي أصبح مرجعًا للمؤسسات المغربية التي تسعى للحصول على الاعتماد وتعزيز نضجها الأمني.

– التقارير والإرشادات الصادرة عن الاتحاد الدولي للاتصالات ((ITUوالمنتدى العالمي للأمن السيبراني ((GFCE توفر إرشادات للدول في بناء استراتيجياتها الوطنية.

2–الأطر التنظيمية والتشريعية: تم تنزيل مضامين هذه الاستراتيجية عبر إصدار نصوص قانونية ولوائح تنظيمية محددة. ففي عام 2016، أعدت إدارة الدفاع مرسوماً يتعلق بتحديد إجراءات حماية نظم المعلومات الحساسة للبنيات التحتية ذات الأهمية الحيوية. وتلا ذلك إصدار قرار لرئيس الحكومة في عام 2018، حدد الشروط الواجب توفرها في المفتشين المعتمدين لتدقيق نظم المعلومات الحساسة، وكيفيات إجراء هذا التدقيق (الافتحاص)، مما يعكس حرص المغرب على إضفاء الطابع الرسمي والمهني على عمليات المراجعة الأمنية.

وفي ظل التطورات التقنية المتسارعة والتهديدات السيبرانية المتنامية، برزت الحاجة الملحة إلى وجود إطار قانوني شامل ومتين. يهدف هذا الإطار إلى حماية نظم المعلومات الوطنية والبنى التحتية الحيوية، وتعزيز ثقة الأفراد والقطاع الخاص في الفضاء الرقمي. واستجابة لهذه المتطلبات، صدر القانون رقم 05.20 المتعلق بتعزيز الأمن السيبراني بالمغرب، بتنفيذ الظهير الشريف رقم 1.20.69 الصادر في 25 يوليو 2020. تتناول هذه الورقة المضامين الأساسية لهذا القانون وأهدافه الاستراتيجية.

المطلب الثاني: الأهداف والإطار العام للقانون رقم 05.20

يهدف القانون إلى وضع قواعد قانونية واضحة لتعزيز الحماية والثقة في الاقتصاد الرقمي، وضمان استمرارية الأنشطة الاقتصادية والاجتماعية. كما يندرج في إطار تنزيل مضامين الاستراتيجية الوطنية للأمن السيبراني، ولا سيما ما يتعلق بحماية نظم المعلومات التابعة للدولة والجماعات الترابية والبنى التحتية الحيوية (أولا) كما يهدف المشرع المغربي وعلى غرار الأنظمة التشريعية المقارنة إلى تفعيل الأطر القانونية للأمن السيبراني: الوقاية، التعاون والحوكمة (ثانيا) لضمان سلامة المعطيات ذات البعد الحيوي والاستراتيجية ضمانا للاستقرار الاجتماعي والاقتصادي.

أولا: تعزيز الحماية: آليات الإبلاغ والتنسيق

يفرض القانون على الهيئات الخاضعة له (مؤسسات الدولة والجماعات الترابية والمؤسسات العامة) الامتثال للتوجيهات الصادرة عن السلطة الوطنية المختصة. كما يلزم هذه الهيئات بتنفيذ تدابير تقنية وتنظيمية لإدارة المخاطر السيبرانية وتفادي الحوادث.

ومن جهة أخرى يوجب تعيين مسؤول عن أمن نظم المعلومات وإعداد خطط لضمان استمرارية الأنشطة واستئنافها في حالات الطوارئ.

كما ينص المشرع على وجوب إبلاغ السلطة الوطنية للأمن السيبراني بأي حادث سيبراني يؤثر على أمن أو سير نظم المعلومات بهدف هذا الإجراء إلى تمكين السلطة من التدخل السريع وتقديم الحلول المناسبة للتغلب على الآثار الناجمة عن الحوادث.

ويفرض المصادقة على البنى التحتية ذات الأهمية الحيوية التي تعتمد على نظم معلومات حساسة إذ يخضعها لفحوصات ومراجعات أمنية (Audits) تتم من قبل جهات معتمدة من السلطة الوطنية.

يمتد نطاق القانون ليشمل فئات أخرى مثل: مشغلي شبكات المواصلات العامة و · مزودي خدمات الإنترنت وكذا مقدمي خدمات الأمن السيبراني ومقدمي الخدمات الرقمية ومنشئي منصات الإنترنت.

كما يلزم هذه الجهات بتنفيذ تدابير حماية تقنية وتنظيمية، والاحتفاظ بالبيانات التقنية التي تساعد في تحديد هوية المصدر في حالة وقوع حوادث سيبرانية.

وعموما يعزز الإطار الاستراتيجي المغربي التشريعات السيبرانية عبر استراتيجية وطنية شاملة (2030) ترتكز على أربعة محاور رئيسية: الحوكمة الوطنية للأمن الرقمي، أمن الفضاء السيبراني، تطوير القدرات البشرية والوعي، وتعزيز التعاون الوطني والدولي.

وتشمل هذه الجهود تحديث الإطار القانوني، تنمية الكفاءات المتخصصة، إطلاق حملات التوعية، ودعم الابتكار، بالإضافة إلى التعاون الدولي لتبادل الخبرات والمعرفة لمواجهة التهديدات السيبرانية المتنامية .

كما تمثل هذه الاستراتيجية إطارًا محوريًا، تحدد أهداف المغرب وأولوياته وخطط عمله في مجال الأمن السيبراني، ولتقوية الإطار القانوني والمؤسساتي عمل المشرع على تعزيز وتطبيق النصوص القانونية والمعايير المتعلقة بالأمن السيبراني في القطاعات الحيوية، وإنشاء مراكز متخصصة مثل مركز الابتكار في الأمن السيبراني .

ولتنمية القدرات والمهارات الوطنية استثمر المغرب في برامج تدريب مكثفة لتكوين أطر متخصصة، ودعم التعليم العالي في مجالات الأمن السيبراني، كما كثف من البرامج والفقرات الهادفة لحملات التوعية

التي تشمل عامة المواطنين والمؤسسات حول مخاطر التهديدات السيبرانية والممارسات الآمنة عبر الإنترنت .

ولأجل حكامة جيدة سعى المشرع إلى خلق نوعا من التعاون بين القطاعين العام والخاص الهدف منه تبادل المعلومات حول التهديدات وتحسين الاستجابة للحوادث، مع إشراك جميع الفاعلين في منظومة الأمن السيبراني .

ثانيا–تفعيل الأطر القانونية للأمن السيبراني: الوقاية، التعاون والحوكمة

يُمثل الإبلاغ عن حوادث الأمن السيبراني ركيزة أساسية في التشريعات المعاصرة، حيث يُلزم القانون الجهات المعنية بالإفادة عن أي خلل أمني قد يؤثر على نظم المعلومات الخاصة بعملائها. كما يفرض اتخاذ التدابير الوقائية والعلاجية الكفيلة بمنع وقوع التهديدات السيبرانية أو التخفيف من حدتها حال تحققها، وذلك بهدف حماية تلك النظم من أي اختراق أو مساس بسلامتها.

وعلاوة على ذلك، يركز المشرع على جانب الوقاية والتوعية بمخاطر الفضاء السيبراني، حيث يُخوّل السلطة الوطنية المختصة مهمة نشر التوصيات والإرشادات الوقائية بشكل دوري عبر منصاتها الرقمية. تستهدف هذه الحملات التوعوية كلاً من الإدارات الحكومية، والجماعات الترابية، والمؤسسات العامة، والبنيات التحتية ذات الأهمية الحيوية، بالإضافة إلى متعهدي القطاع الخاص والمواطنين.

كما يُبرز التشريع دور التعاون وتبادل المعلومات بين المصالح الحكومية المختصة في مواجهة الهجمات السيبرانية، حيث يُرسي القانون رقم 05.20 إطاراً مؤسسياً للتعاون بين السلطة الوطنية للأمن السيبراني والجهات المعنية بمكافحة الجرائم الإلكترونية التي تستهدف نظم المعالجة الآلية للبيانات. وتسهم السلطة، وفقاً لهذا الإطار، في دعم البرامج الوطنية الرامية إلى تعزيز الثقة في الخدمات الرقمية، وتطوير آليات حماية البيانات الشخصية والحساسة.

ولتعزيز القدرات الدفاعية في مواجهة التحديات السيبرانية، يُولي التشريع أولويةً واضحةً لتعزيز أواصر التعاون وتبادل الخبرات مع المنظمات والمؤسسات الأجنبية المماثلة، سعياً لبناء منظومة أمنية دولية متكاملة.

وفي إطار تقوية حوكمة الأمن السيبراني، يحدد القانون المهام والصلاحيات المخولة للجنة الاستراتيجية للأمن السيبراني والسلطة الوطنية للأمن السيبراني واللجنة الوطنية لإدارة الأزمات السيبرانية الجسيمة. ويتضمن أيضاً إمكانية إجراء عمليات التدقيق الأمني لضمان الالتزام بالمعايير والسياسات المعتمدة.

ولا يقتصر تأثير هذا التشريع على حماية الاقتصاد والمجتمع فحسب، بل يسهم أيضاً في تطوير البيئة الوطنية للأمن السيبراني، مما يعزز بدوره نمو قطاعات الاستشارات والتدقيق الأمني ومراقبة الحوادث السيبرانية، فضلاً عن تطوير منتجات تأمين الشبكات ونظم المعلومات.

كما يشتمل القانون على نصوص زجرية صارمة لضمان الامتثال لأحكامه، حيث يُجرّم الأفعال التي من شأنها الإخلال بالالتزامات المنصوص عليها، كعدم الإبلاغ عن حوادث الاختراق، أو تخزين البيانات الحساسة خارج النطاق الجغرافي الوطني، أو عرقلة عمليات التدقيق الأمني، أو عدم تنفيذ القرارات الصادرة عن السلطة الوطنية للأمن السيبراني.

المبحث الثاني: دور الأمن السيبراني في تأمين حكامة الإدارة الضريبية بالمغرب.

تمثل المنظومة الضريبية في أي دولةٍ العمود الفقري لسياستها المالية، كونها الأداة الأكثر فاعلية في تعبئة الموارد العمومية وتوجيه الاقتصاد وتحقيق التوزيع العادل للثروة[1]. وفي إطار مساعيه المتواصلة لتحديث أدوات الحكامة الاقتصادية، يبرز مشروع القانون الإطار رقم 69.21 المتعلق بالإصلاح الضريبي، الذي أقرته المملكة المغربية في يوليوز 2021، كمحاولةٍ جريئةٍ لإعادة هيكلة النسق الجبائي الوطني بشموليةٍ غير مسبوقة.

لا ينفصل هذا المسعى الإصلاحي عن سياقه الزمني بالغ التعقيد، والذي تميز بتداخل أزماتٍ دوليةٍ طاحنة، أبرزها الجائحة الكونية (كوفيد-19) وتداعياتها العميقة على المالية العمومية[2]، والاضطرابات الجيوسياسية والاقتصادية الناجمة عن الحرب في أوكرانيا وما صاحبها من ارتفاعاتٍ غير مسبوقةٍ في أسعار الطاقة والمواد الغذائية[3]. هذا إلى جانب معضلاتٍ هيكليةٍ محليةٍ متفاقمة، يأتي في مقدمتها نوبات الجفاف المتلاحقة وتأثيرها المباشر على الأمن المائي والغذائي، ومن ثمَّ على الحيز المالي المتاح للحكومة،[4] وذلك لتحقيق الأهداف الاستراتيجية التالية:

1-تحليل الأسس التشريعية والمؤسساتية التي يقوم عليها مشروع الإصلاح، ومدى اتساقه مع التوجهات الاستراتيجية الكبرى للدولة.

2-تقويم مدى نجاعته النظرية في تحقيق غاياته المعلنة، ولا سيما تعزيز العدالة الضريبية من خلال مرتكزي المساواة والإنصاف[5]، وضمان الاستدامة المالية عبر ترشيد النفق وتحسين مردودية الجباية.

3-رصد وتشخيص المعضلات والتحديات العملية والإجرائية والإدارية التي قد تعترض سبيل تنفيذه على أرض الواقع، بعيداً عن التنظير.

4-تقديم جملة من الآليات والمقترحات القابلة للتطبيق، الكفيلة بتعزيز فاعليته وضمان تحقيق النتائج المرجوة منه، سعياً نحو إرساء نظامٍ ضريبيٍ عصري، عادلٍ، وفعّال.

المطلب الأول: الإصلاح الضريبي في المغرب في ظل الأزمات المتعددة

[1] -Bird, R. M., & Zolt, E. M. (2005). Redistribution via Taxation: The Limited Role of the Personal Income Tax in Developing Countries. UCLA Law Review, 52, 1627-1695.

[2] -IMF (2021). Fiscal Monitor: A Fair Shot. International Monetary Fund, Washington, D.C., April.

[3] -World Bank (2022). Commodity Markets Outlook: The Impact of the War in Ukraine on Commodity Markets. April.

[4] -Ministère de l'Économie et des Finances (2022). Projection de la croissance économique et orientations budgétaires. Rapport, Rabat..

[5] -الطاهر، محمد. (2018). العدالة الضريبية بين النظرية والتطبيق. مجلة المنازعات التجارية، (5)، 45-72.

شكلت الأزمات المتعاقبة التي عرفها الاقتصاد العالمي، بدءاً من الجائحة الصحية ومروراً بالاضطرابات في سلاسل التوريد وانتهاءً بارتفاع التضخم، ضغوطاً هيكلية على المالية العمومية في المغرب. كاستجابة لهذه التحديات، تسارعت وتيرة الإصلاحات الهيكلية، حيث تبلورت جهود إصلاح النظام الضريبي كمحور استراتيجي لتعبئة الإيرادات وتمويل السياسات العمومية في إطار النموذج التنموي الجديد. يجسد مشروع قانون الإطار الضريبي تتويجاً لهذه الجهود، مستنداً إلى توصيات المناظرة الوطنية الثالثة حول الضرائب (ماي 2019) والتوجيهات الدستورية المؤكدة على مبدأي الإنصاف والمساهمة التضامنية في النفقات العمومية[1].

1-الإطار القانوني والإصلاحي: من التوصيات إلى التشريع

يرتكز مشروع قانون الإطار على جملة من المبادئ التأسيسية تهدف إلى إرساء نظام ضريبي "فعال ومنصف ومتوازن". وتتمثل أهدافه الجوهرية في:

تعزيز العدالة الضريبية والاجتماعية: من خلال توسيع الوعاء الضريبي، ومكافحة التهرب الضريبي، وترشيد الإعفاءات والحوافز الضريبية (النفقات الضريبية)، وإدماج القطاع غير المهيكل.

تحسين الحكامة الضريبية: عبر تبسيط الإجراءات، ورقمنة العمليات، وتعزيز آليات الشفافية ومحاربة الغش.

ضمان الاستدامة المالية: بتعبئة موارد إضافية تقدر بـ 2-3% من الناتج المحلي الإجمالي لتمويل برامج التنمية.

ولضمان جدولة زمنية واضحة، فرضت المادة 19 من القانون تنزيل أحكامه المتعلقة بالضرائب الرئيسية (ضريبة القيمة المضافة، الضريبة على الشركات، الضريبة على الدخل، الضرائب المحلية) خلال أمد زمني محدد(2022-2026) .

لكن وعلى الرغم من وضوح الرؤية التشريعية، فإن عملية التنفيذ تواجه عدة إشكاليات نقدية:

الإشكالية الزمنية: يشكل الأجل القانوني المحدد بخمس سنوات (2026) تحدياً مؤسسياً كبيراً. إن التأخر الملحوظ في إدخال تغييرات جذرية عبر قوانين المالية السنوية (كما لوحظ في قانون المالية 2022) يثير تساؤلات جادة حول الجدوى الزمنية لتنفيذ هذا الإصلاح الجذري ضمن الإطار المحدد.

إشكالية التعقيد والتبسيط: يبقى تعقيد النصوص الضريبية حاجزاً أمام الامتثال الطوعي. إن تبسيط اللغة والإجراءات ليس مجرد تحسين تقني، بل هو شرط أساسي لتحقيق الشمولية، وخفض تكاليف الامتثال، ومكافحة التهرب الضريبي غير المقصود الناجم عن سوء الفهم.

إشكالية الرقمنة والحصول على المعلومات: تتعدى الرقمنة مجرد تحويل العمليات الورقية إلى رقمية. إنها تستلزم تحولاً جوهرياً في نموذج عمل الإدارة الضريبية، يعتمد على تحليل البيانات الضخمة Big Data للكشف عن المتهربين، وإكمال

[1]- ينص الفصل 39 من دستور 2011 "على الجميع أن يتحمل، كل على قدر استطاعته، التكاليف العمومية، التي للقانون وحده إحداثها وتوزيعها، وفق الإجراءات المنصوص عليها في هذا الدستور".

الإقرارات تلقائياً، وتقديم خدمات إلكترونية تفاعلية. كما يجب أن يتم هذا التحول في توازن دقيق مع حماية حقوق الخصوصية والأمن السيبراني.

إشكالية بناء القدرات البشرية: نجاح أي إصلاح ضريبي مرهون بكفاءة العنصر البشري. يتطلب تطوير الإدارة الضريبية استثماراً مستمراً في تدريب وتأهيل الكوادر على المهارات التقنية (تحليل البيانات، الاقتصاد) والمهارات الاجتماعية (خدمة دافعي الضرائب) لمواكبة تعقيدات النظام الجديد.

2–آليات مقترحة لتعزيز فعالية الإصلاح

يشهد العصر الرقمي تحولات متسارعة تفرض تطوير أطر تشريعية سيبرانية متكاملة وفعالة. وفي ظل المسار الإصلاحي الذي يقوده المغرب في هذا المجال، تبرز الحاجة إلى آليات عملية لتعزيز فعالية هذه الإصلاحات وضمان تحقيق أهدافها وذلك عن طريق خلق إطار متكامل لآليات تعزيز فعالية الإصلاح التشريعي السيبراني من خلال:

أ–تعزيز أنظمة الرصد والتقييم القائمة على النتائج:

مما لا شك فيه أن بناء نظام فعال للرصد والتقييم يعتبر حجر الزاوية في ضمان نجاح الإصلاحات التشريعية السيبرانية ويتطلب ذلك:

- **تطوير مؤشرات أداء رئيسية (KPIS) نوعية وكمية**

– **مؤشرات كفاءة التشريع:** مثل زمن معالجة البلاغات السيبرانية، وتكلفة تطبيق الآليات الدفاعية، ونسبة الامتثال الطوعي للتشريعات.

– **مؤشرات العدالة السيبرانية:** مثل مؤشر توزيع الحماية القانونية بين القطاعات، ومؤشر المساواة في الوصول إلى آليات الحماية.

– **مؤشرات الأثر:** مثل نسبة تقليل الجرائم الإلكترونية المسجلة، ومستوى ثقة المستخدمين في الخدمات الرقمية.

- **إنشاء منصة وطنية للرصد والتقييم**

– نظام متكامل يجمع البيانات من مختلف الجهات المعنية (الوكالة الوطنية للأمن السيبراني، وزارة العدل، الشرطة القضائية، القطاع الخاص).

– استخدام تقنيات الذكاء الاصطناعي وتحليل البيانات للكشف عن الأنماط والثغرات في التطبيق العملي للتشريعات.

– تقارير دورية نصف سنوية لتقييم مدى تقدم تنفيذ الاستراتيجية الوطنية للأمن السيبراني.

ب–تفعيل التعاون بين الجامعات وصناع السياسات:

يمثل الربط بين الأكاديميين وصناع القرار ركيزة أساسية لتطوير تشريعات سيبرانية قائمة على الأدلة:

- **إنشاء مراكز امتياز للأبحاث السيبرانية** -Establishing centers of excellence in cybersecurity law and policy within major universities.

– تطوير برامج بحثية مشتركة بين الجامعات والوزارات المعنية تركز على السياسات التشريعية والتطبيقات العملية.

– منح الية للبحث في مجالات ناشئة مثل: تنظيم الذكاء الاصطناعي، حماية البيانات الحيوية، الأطر القانونية لتقنيات البلوكشين.

- **برامج التبادل المعرفي**

– برنامج زمالة لتبادل الخبراء بين الجامعات والمؤسسات التشريعية.

– ورش عمل مشتركة دورية لعرض نتائج الأبحاث ومناقشة التحديات التشريعية العملية.

– منصة رقمية لتشارك الأبحاث والدراسات بين الأكاديميين وصناع السياسات.

ج–ترشيد النفقات الضريبية والإعفاءات في القطاع السيبراني عن طريق:

- **تقييم جدوى الإعفاءات والحوافز الضريبية**

– إخضاع جميع الإعفاءات الضريبية المقدمة للشركات العاملة في مجال الأمن السيبراني لتحليل دقيق للكلفة والعائد.

– تقييم أثر الإعفاءات الضريبية على تنمية القطاع السيبراني الوطني وجذب الاستثمارات الأجنبية.

– إجراء مراجعة دورية (كل 3 سنوات) للحوافز الضريبية لتعديلها أو إلغائها وفقاً للنتائج المتحققة.

- **تطوير آلية تمويل مبتكرة للاستثمار السيبراني**

– إنشاء صندوق خاص لتمويل المشاريع السيبرانية المبتكرة ذات الأولوية الوطنية.

– نظام ائتماني ميسر للشركات الصغيرة والمتوسطة العاملة في مجال الأمن السيبراني.

– شراكات استثمارية بين القطاع العام والخاص لتمويل البنى التحتية السيبرانية الحرجة.

د–حملات التوعية والتبسيط للتشريعات السيبرانية عن طريق:

- **تطوير أدلة تشريعية مبسطة**

– إصدار أدلة تشرح القوانين السيبرانية بلغة مبسطة وميسرة للمواطنين والشركات.

– تطوير منصة رقمية تفاعلية تقدم شروحات مرئية ومكتوبة للالتزامات والحقوق السيبرانية.

– إنشاء خطوط استشارية مجانية لتقديم الإرشادات القانونية السيبرانية.

- **برامج التوعية المتخصصة وذلك ب:**

– إدراج التوعية القانونية السيبرانية في المناهج التعليمية بمختلف المستويات.

– حملات توعوية تستهدف فئات محددة (كبار السن، الأطفال، رواد الأعمال).

– برامج تدريبية للمهنيين (محامون، قضاة، موظفون عموميون)

هـ- إنشاء مراجعة تشريعية تشاركية باعتماد:

- منصات تشاورية رقمية تمكن المواطنين والخبراء من المشاركة في صياغة وتعديل التشريعات السيبرانية.
- لجان استشارية متخصصة تضم ممثلين عن القطاع الخاص والأكاديميين والمجتمع المدني.

- **تعزيز التعاون الدولي**

-تكثيف عملية الانضمام إلى الاتفاقيات الدولية المتعلقة بالأمن السيبراني

- تبادل الخبرات والمعرفة مع الهيئات الدولية المتخصصة
- توطين أفضل الممارسات الدولية مع مراعاة الخصوصيات المحلية.

المطلب الثاني: الأمن السيبراني ودوره في تأمين حكامة الإدارة الضريبية بالمغرب.

تكتسي البيانات الضريبية طابعاً بالغ الحساسية، إذ لا تقتصر على الأرقام والمبالغ فحسب، بل تمتد لتشمل أسراراً تجارية ومالية للشركات، ومعلومات شخصية ومالية مفصلة للأفراد (المادة 1 من القانون 13-05). وفي ظل التحول الرقمي المتسارع الذي تشهده الإدارة الضريبية المغربية، أصبحت هذه البيانات عرضة لمجموعة من التهديدات الإلكترونية المتطورة، مما يفرض ضرورة وجود إطار قانوني رصين وآليات تقنية فاعلة لحمايتها. ومن هذا المنطلق، يتدخل التشريع المغربي بتشكيلتين أساسيتين: أولاهما تتمثل في القانون 13-05 المتعلق بالمبادئ الأساسية لحماية خصوصية الأفراد فيما يتعلق بمعالجة بياناتهم الشخصية، الذي ينصب على إنشاء اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي (CNDP) كجهة رقابية مستقلة، وثانيتهما في القانون 05-20 المتعلق بالسلامة السيبرانية[1]، الذي يركز على حماية البنى التحتية المعلوماتية الحيوية للدولة. وعليه، تبرز الإشكالية المحورية للمقال: إلى أي حد يشكل هذان التشريعان إطاراً متكاملاً وفعالاً لوقاية البيانات الضريبية من المخاطر الإلكترونية؟ وما هي التحديات العملية التي تعترض تطبيقهما الكامل؟

أولا: الإطار القانوني المزدوج لحماية البيانات الضريبية: بين حماية الحقوق وتأمين الأنظمة

يتميز النهج التشريعي المغربي بتبني رؤية مزدوجة تجمع بين حماية الحقوق الفردية وتأمين الفضاء الرقمي، مما ينعكس بشكل واضح على حماية المنظومة الضريبية.

ففي ظل التحول الرقمي المتسارع لأجهزة الدولة، أصبحت البيانات الضريبية، بوصفها عصب الاقتصاد وأداة السيادة المالية، عرضة لمخاطر إلكترونية متطورة ومتشعبة. ولمواجهة هذه التحديات، تبنت المملكة المغربية إطاراً تشريعياً متقدماً يعتمد على نهج متعدد المستويات.

يجسد القانون 13-05 المتعلق بالحماية القانونية للأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، والقانون 05-20 المتعلق بالسلامة السيبرانية، معاً نموذجاً تشريعياً متكاملاً. لا يقوم هذا النموذج على التعايش بل على التكامل

[1]-القانون رقم 05-20 هو قانون مغربي يهدف إلى تعزيز الأمن السيبراني من خلال وضع إطار قانوني يحدد قواعد وتدابير حماية نظم المعلومات الحساسة للبنيات التحتية ذات الأهمية الحيوية، الإدارات العمومية، والمؤسسات العمومية والخاصة، بالإضافة إلى تحديد مسؤوليات السلطة الوطنية للأمن السيبراني.

العضوي، حيث يوفر الأول حماية جوهرية (Substantive Protection) للفرد في معطياته، بينما يوفر الثاني حماية هيكلية (Structural Protection)للمنظومة المعلوماتية ككل. تهدف هذه الورقة إلى تفكيك هذا التكامل وتحليل آليات اشتغاله في حماية المنظومة الضريبية.

أ–حماية الحقوق الفردية في إطار القانون 13–05: نحو ضمانات جوهرية للخصوصية

يؤسس القانون 13–05 لتصور متقدم للحماية القانونية، حيث ينتقل بالبيانات الضريبية من مجرد أرقام إدارية إلى "معطيات ذات طابع شخصي" تتمتع بضمانات دستورية وقانونية. يتجلى هذا التصور من خلال محورين أساسيين:

1–عبء الالتزامات على عاتق الإدارة الضريبية بوصفها مسؤولة عن المعالجة يمنح القانون الإدارة الضريبية صفة "مسؤولة عن المعالجة"، مما يفرض عليها عبئاً فعالياً (Positive Obligation) يتمثل في مجموعة من المبادئ الحاكمة:

– **مبدأ الشرعية والشفافية** :(Lawfulness and Transparency) لا تكفي مشروعية الغرض الضريبي وحده، بل يجب أن تكون المعالجة متوافقة مع الشروط الدقيقة المنصوص عليها في المادة 6 (كالحصول على الموافقة أو ضرورة التنفيذ القانوني). كما يفرض المبدأ وجوب إعلام الملزمين، عند جمع البيانات، بهويتها والغرض من المعالجة والمستلمين المحتملين، مما يعزز الشفافية ويحول دون "التعامل في الخفاء."

– **مبدأ تناسب الغرض**: تُحصر معالجة البيانات حصراً في "الأغراض الضريبية المحددة سلفاً". يحول هذا المبدأ دون تحويل البيانات الضريبية لاستخدامات أخرى (كالتسويق أو التخطيط الاجتماعي) دون أساس قانوني صريح، مما يضمن عدم الانزياح عن الغاية الأصلية.

– **مبدأ التأمين وسلامة المعطيات** :(Integrity and Confidentiality) يعد الفصل 6-1 من أشد الالتزامات إلزامية. فالإدارة ملزمة ليس فقط باتخاذ "التدابير التحذيرية الملائمة" بل "لموذجها"، أي تلك المتناسبة مع طبيعة البيانات الحساسة والمخاطر المحدقة بها. يتطلب هذا تنفيذ تدابير تقنية صارمة كالتشفير (Encryption) في حالة التخزين والنقل، وإخفاء الهوية(Pseudonymization) ، وإنشاء أنظمة تحكم دقيقة في صلاحيات الولوج (Access Control Policies).

2–تمكين الملزم (Data Subject) من خلال الحقوق الفعالة: كمقابل للالتزامات، يخلق القانون 13–05 توازناً قوياً بمنح الملزمين مجموعة من الحقوق الإجرائية:

– **حق الوصول (Right of Access) المادة 24**: يمثل هذا الحق حجر الزاوية في الرقابة الفردية. فهو يمكن الملزم من التحقق من دقة البيانات، والاطلاع على المنطق الأساسي للقرارات الآلية (كتقييم المخاطر الضريبية)، والكشف عن أي معالجة غير مشروعة.

– **حق التصحيح والتحديث (Right to Rectification) المادة 25**: يضمن هذا الحق جودة وموثوقية القاعدة البياناتية الضريبية. فإمكانية الملزم تصحيح خطأ ما لا تحميه فقط من قرار ضريبي غير سليم بناء على معلومات خاطئة، بل تخدم المصلحة العامة بالإبقاء على بيانات الإدارة دقيقة وموثوقة.

وبالتالي، يشكل القانون 13-05 الإطار القانوني الذي يحول الملزم من مجرد خاضع للسلطة الضريبية إلى شريك فاعل في ضمان نزاهة ودقة النظام الضريبي الرقمي.

ب–تأمين البنى التحتية في إطار القانون 05–20: نحو حماية استراتيجية للمرافق الحيوية

إذا كان القانون 13-05 يركز على حماية "المعطى"، فإن القانون 05-20 يتجه صوب حماية "الحاضنة" أو "الوعاء" الذي يحتوي هذا المعطى، أي البنية التحتية المعلوماتية. ينتقل هذا القانون بمستوى الحماية من المستوى الفردي إلى المستوى الاستراتيجي والأمن القومي، خاصة إذا ما تم تصنيف الإدارة الضريبية كمشغل للمرافق الحيوية.(OIV)

1–الانتقال من الالتزام العام إلى الالتزام المعزز: يضع القانون 05-20 تصنيفاً هرمياً للمنشآت. تصنيف الإدارة الضريبية كمشغل للمرافق الحيوية (بموجب المادة 8) يخرجها من نطاق الالتزامات العامة (المواد 20 و21) ليدخلها في نطاق الالتزامات المعززة (المواد 21 و22 و23). هذا التصنيف ليس إجراءً شكلياً بل هو اعتراف بالدور الاستراتيجي للمنظومة الضريبية في استقرار الدولة اقتصادياً وأمنياً.

2–طبيعة الالتزامات المعززة:

– واجب الأمن (Security Duty) المادة 21: يتجاوز هذا الواجب مفهوم "التدابير الملائمة" ليصل إلى "جميع التدابير التقنية والتنظيمية الملائمة". هذا يشمل تبني منهجيات إدارة المخاطر السيبرانية (Cybersecurity Risk Management)وفق أفضل المعايير) كإطار عمل NIST أو(ISO/IEC 27001 ، وإجراء اختبارات اختراق دورية (Penetration Testing)، ووضع خطط استمرارية الأعمال (Business Continuity Plans) والتعافي من الكوارث.(Disaster Recovery Plans)

– واجب الإبلاغ الإلزامي (Mandatory Notification Duty) المادة 22: يعد هذا الالتزام من أبرز ملامح القانون 05-20. فالإبلاغ عن حوادث السلامة السيبرانية للوكالة الوطنية للسلامة السيبرانية (ANSI) ليس مجرد إشعار، بل هو آلية لتفعيل "الذكاء الجماعي (Collective Intelligence) "في مواجهة التهديدات. يتيح هذا للإدارة الاستفادة من الخبرة المركزية للوكالة ويسمح للدولة بتتبع نمط الهجمات والاستجابة الوطنية الموحدة، وبالتالي تحويل الحادث من مجرد خلل فني إلى قضية أمن قومي يتم إدارتها بمنهجية مؤسساتية.

ج–التداخل والتكامل بين التشريعين: نحو نموذج حماية متعدد المستويات (A Multi-Layered Defense Model)

يكمن نجاح المنظومة التشريعية المغربية في عدم فصلها بين حماية الحقوق الفردية وأمن المنظومة الوطنية، بل في نسجها في نموذج متكامل.

1–التكامل الوظيفي بين التأمين والسلامة: يمكن تحليل هذا التكامل عبر استعارة عسكرية توضيحية:

– القانون 13-05: خط الدفاع الداخلي :يمثل الحماية على مستوى "البيانات في حالة السكون و"البيانات أثناء الاستخدام .(Data in Use) "فهو ينظم من يمكنه الدخول إلى البيانات (المصادقة)، وماذا يمكنه أن يفعل بها (الترخيص)، وكيف يتم تخزينها (التشفير). إنه حماية من التهديدات الداخلية (سواء كانت متعمدة أو غير مقصودة) ومن التسربات.

– القانون 05-20: خط الدفاع الخارجي والاستراتيجي: يمثل الحماية على مستوى "البيانات أثناء الانتقال (Data in Transit) "وحماية الأنظمة والشبكات ذاتها. فهو مصمم لصد الهجمات الخارجية المنظمة) الاختراقات، هجمات الحرمان من الخدمة، البرمجيات الخبيثة .(كما أن خطط الاستجابة للحوادث التي يفرضها تمثل "قوات التدخل السريع" للاحتواء والتعافي.

2–التكامل القانوني: تعزيز المساءلة :(Accountability) يخلق التقاء التشريعين مساءلة مزدوجة للإدارة الضريبية:

– مساءلة أمام الفرد (في إطار 13-05): حيث يمكن للملزم اللجوء إلى اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي (CNDP) في حالة انتهاك حقوقه.

– مساءلة أمام الدولة (في إطار 05-20): حيث تفرض الوكالة الوطنية للسلامة السيبرانية (ANSI) عقوبات في حالة عدم الامتثال لالتزامات الأمن والإبلاغ.

هذا التداخل يجعل من الصعب على الإدارة التهرب من مسؤولياتها، كما أنه يخلق "شبكة أمان" لا تترك ثغرات للمتلاعبين.

ثانيا: إشكالية تعدد الجهات الرقابية وآليات التنسيق

يبرز هنا تحدي التنسيق بين الجهتين الرقابيتين المنوط بهما تطبيق هذين القانونين: اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي (CNDP) والوكالة الوطنية للسلامة السيبرانية (ANSI) ففي حالة حدوث خرق للبيانات الضريبية، قد تتداخل الاختصاصات: فـ CNDP تختص بمراقبة مدى احترام حقوق الأفراد والمعالجة conforme للقانون 13-05، بينما تختص ANSI بمعالجة "حادثة السلامة" من الناحية التقنية وتقييم تأثيرها على المرفق الحيوي. ولتفادي هذا التعقيد، يفترض أن يعمل التشريع على تعزيز آليات التنسيق والتكامل بينهما، كما ينص على ذلك المادة 44 من قانون 05-20، والتي تلزم ANSIبإبرام اتفاقيات للتعاون مع مختلف المؤسسات، بما فيهاCNDP ، لضمان عمل متجانس يحقق الحماية الشاملة دون ثغرات أو ازدواجية.

ثالثا: التحديات العملية وسبل تعزيز الحماية السيبرانية للبيانات الضريبية

رغم متانة الإطار القانوني النظري، فإن التطبيق العملي لا يخلو من تحديات جسيمة تتطلب مواجهة فعالة.

أ– معوقات التطبيق بين التقنية والموارد البشرية:

يواجه تطبيق هذه القوانين تحدياً تقنياً يتمثل في السرعة الجنونية لتطور تهديدات الأمن السيبراني (كبرامج الفدية والتصيد الاحتيالي)، والتي تتطلب تحديثاً مستمراً للإجراءات الوقائية، وهو أمر يستنزف موارد مالية كبيرة. كما يشكل العامل البشري أحد أبرز نقاط الضعف، حيث أن أي خطأ من موظف (كالنقر على رابط تصيد أو استخدام كلمة مرور ضعيفة) يمكن أن يُفشل أغلب الإجراءات التقنية المتطورة. ويضاف إلى ذلك التحدي القانوني المتمثل في صعوبة تحديد المسؤولية بدقة عند حدوث خرق بين الإدارة الضريبية ومقدمي خدمات التكنولوجيا لديها.

ب–آليات وآفاق تعزيز الفعالية الحمائية لتعزيز فعالية الحماية، يمكن اقتراح جملة من الآليات، منها:

1 – **تعزيز التعاون المؤسسي** : تفعيل مذكرة تفاهم عملية بين CNDP و ANSIوالمديرية العامة للضرائب لتوحيد الجهود وإجراء عمليات تدقيق مشتركة.

2 – **الاعتماد على المعايير الدولية** : تبني الإدارة الضريبية لإطار عمل أمني معترف به عالمياً مثل إطار عمل NIST)الهوية، الحماية، الكشف، الاستجابة، الاستعادة) لتنظيم وتحسين استجابتها للتهديدات.

3 – **التوعية المستمرة** : إطلاق برامج تدريبية إلزامية ومستمرة لموظفي الإدارة الضريبية لرفع مستوى الوعي بالأمن السيبراني وتحويلهم من "حلقة ضعف" إلى "خط دفاع" أول.

4–**تبني مبدأ "الأمن بالتصميم"**: ضمان أن تكون مشاريع الرقمنة الجديدة (كالبوابة الضريبية) مصممة بمعايير أمنية عالية منذ انطلاقها وليس كإضافة لاحقة.

وخلاصة القول إن التشريع المغربي، من خلال القانون 13–05 والقانون 05–20، يكون قد وضع أسساً قانونية متقدمة ومتكاملة لحماية البيانات الضريبية، جمعت بين حماية الحقوق الفردية (CNDP) وتأمين البنى التحتية المعلوماتية الحيوية(ANSI) إلا أن فعالية هذا الإطار تبقى رهينة بمدى توفير الإرادة السياسية والموارد المالية والبشرية الكافية لتطبيقه على أرض الواقع. فمواكبة التهديدات الإلكترونية تتطلب نهجاً استباقياً ديناميكياً قائماً على التقييم المستمر والتحديث الدوري والتعاون الوثيق بين جميع الأطراف المعنية، لضمان حماية المال العام والحقوق الفردية في آن واحد، والحفاظ على الثقة في المنظومة الضريبية الوطنية كرافعة أساسية للتنمية.