**صفية لكطيطي**

دكتورة في القانون الخاص

أستاذة زائرة بجامعة محمد الخامس

رئيسة المركز الوطني للدراسات الاستراتيجية والتحول الرقمي


# الأمن السيبراني

## "دراسة مقارنة"


DAR AL AFAK

COPY


تقديم

**الأستاذ الدكتور رياض فخري**

مدير مختبر البحث قانون الأعمال

بجامعة الحسن الأول بسطات المملكة المغربية

المستشار القانوني للاتحاد العربي للتمكين الرقمي




**الطبعة الأولى**

**2025**

# فهرس المحتويات


مقدمة ..... 1

**الباب الأول: آليات تحقيق الأمن السيبراني ..... 15**

**الفصل الأول: الآليات القانونية لتحقيق الأمن السيبراني ..... 19**

المبحث الأول: التدابير التقنية والتنظيمية لإدارة الأخطار السيبرانية ..... 20

المطلب الأول: التدابير المعتمدة في قانون الأمن السيبراني ..... 22

الفقرة الأولى: إجراءات حماية نظم المعلومات المفروضة على الهيئات ..... 25

الفقرة الثانية: الإجراءات الأمنية المفروضة على البنيات التحتية ذات الأهمية الحيوية ... 29

الفقرة الثالثة: إجراءات حماية نظم المعلومات المفروضة على المتعهدين ..... 34

المطلب الثاني: التدابير التقنية المعتمدة في قانون خدمات الثقة بشأن المعاملات الالكترونية .. 37

الفقرة الأولى: نظام التشفير كآلية لتحقيق أمن المعطيات ..... 39

أولا: تعريف وسائل خدمة التشفير ..... 39

ثانيا: القيود الواردة على وسائل التشفير ..... 42

ثالثا: التقنيات المصاحبة لنظام التشفير ..... 43

الفقرة الثانية: آليات تأمين المعاملات الالكترونية ..... 47

أولا: التوقيع الالكتروني ..... 48

ثانيا: الخاتم الالكتروني ..... 51

ثالثا: الختم الزمني الالكتروني ..... 52

رابعا: خدمة الإرسال الالكتروني المضمون ..... 53

خامسا: التيقن من موقع الانترنت (الموقع الالكتروني) ..... 55

المبحث الثاني: المواجهة الزجرية كآلية لتصدي للجريمة السيبرانية ..... 57

المطلب الأول: مكافحة الجريمة السيبرانية وفق القواعد المقررة في مجموعة القانون الجنائي 58

الفقرة الأولى: مواجهة قانون مكافحة الإرهاب للجريمة السيبرانية ..... 59

أولا: جريمة الإرهاب المرتكبة عبر الفضاء السيبراني ..... 61

ثانيا: جريمة الإشادة بالإرهاب المرتكب عبر الفضاء السيبراني ..... 64

الفقرة الثانية: مكافحة الجرائم الماسة بنظم المعالجة الآلية للمعطيات ..... 66
أولا: جريمة الدخول أو البقاء عن طريق الاحتيال لنظام المعالجة الآلية للمعطيات ..... 68
ثانيا: جريمة عرقلة سير نظام المعالجة الآلية للمعطيات ..... 72
ثالثا: جريمة التلاعب بالمعطيات الموجودة داخل النظام المعلوماتي ..... 74
رابعا: جريمة تزوير الوثائق المعلوماتية أو استعمالها ..... 76
خامسا: جريمة التعامل غير الشرعي في معطيات النظام المعلوماتي ..... 77
المطلب الثاني: التصدي للجريمة السيبرانية في إطار القوانين الخاصة ..... 79
الفقرة الأولى: ردع الجرائم المرتكبة بواسطة الوسائل الالكترونية ..... 80
أولا: حماية المصنفات الرقمية ..... 80
ثانيا: حماية المعطيات ذات الطابع الشخصي ..... 88
ثالثا: حماية خدمات الثقة بشأن المعاملات الالكترونية ..... 92
الفقرة الثانية: ردع الجرائم الماسة بالنظام المعلوماتي ..... 98
أولا: حماية نظم معلومات الإدارة الجمركية ..... 99
ثانيا: دور قانون البريد والمواصلات ..... 99

**الفصل الثاني: مدى حكامة الآليات المؤسساتية في تحقيق الأمن السيبراني ..... 103**

المبحث الأول: دور المؤسسات الرقابية في تحقيق الأمن السيبراني ..... 104
المطلب الأول: مظاهر تدخل المؤسسات المعتمدة في قانون الأمن السيبراني ..... 104
الفقرة الأولى: اللجنة الاستراتيجية للأمن السيبراني ..... 105
الفقرة الثانية: لجنة إدارة الأزمات والأحداث السيبرانية الجسيمة ..... 107
الفقرة الثالثة: السلطة الوطنية للأمن السيبراني ..... 108
أولا: مهام السلطة الوطنية للأمن السيبراني ..... 109
ثانيا: دور المديريات التابعة للسلطة الوطنية للأمن السيبراني ..... 111
المطلب الثاني: تجليات تدخل المؤسسات المعتمدة في القوانين الخاصة ..... 115
الفقرة الأولى: الوكالة الوطنية لتقنين المواصلات « anrt » ..... 116
الفقرة الثانية: السلطة الوطنية لخدمات الثقة بشأن المعاملات الالكترونية ..... 118

الفقرة الثالثة: دور اللجنة الوطنية لحماية المعطيات ذات الطابع الشخصي ..... 125
أولا: الإخبار والتحسيس ..... 126
ثانيا: الاستشارة والاقتصاد ..... 127
ثالثا: الحماية ..... 127
رابعا: التحري والمراقبة ..... 128
خامسا: اليقظة القانونية والتكنولوجية ..... 129
المبحث الثاني: مكافحة أجهزة العدالة الجنائية للجريمة السيبرانية ..... 131
المطلب الأول: الأجهزة الأمنية الدولية المختصة في مكافحة الإجرام السيبراني ..... 131
الفقرة الأولى: تدخل المنظمة الدولية للشرطة الجنائية (الانتربول) ..... 132
الفقرة الثانية: تدخل جهاز الشرطة الأوروبية (اليوروبول) ..... 136
المطلب الثاني: الأجهزة الأمنية الوطنية المختصة بمكافحة الإجرام السيبراني ..... 138
الفقرة الأولى: دور الأجهزة الأمنية في الولايات المتحدة الأمريكية ..... 139
أولا: شرطة الواب (Web police) ..... 139
ثانيا: مركز تلقي شكاوي جرائم الانترنت IC3 ..... 140
ثالثا: نيابة جرائم الحاسوب والاتصالات ..... 141
الفقرة الثانية: دور الأجهزة الأمنية الفرنسية في ردع الجريمة السيبرانية ..... 141
أولا: المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات والاتصالات (OCLCTIC) ... 142
ثانيا: وحدة التحقيق المختصة في الاحتيال بتكنولوجيا المعلومات ..... 144
ثالثا: القسم الوطني لقمع جرائم المساس بالأموال والأشخاص ..... 145
رابعا: مركز مكافحة الجريمة الرقمية (C3N) التابع لقوات الدرك الوطنية التابعة للشرطة الوطنية 146
خامسا: المديرية الفرعية لمكافحة الجريمة السيبرانية SDLC ..... 147
الفقرة الثالثة: دور الأجهزة الأمنية المغربية في ردع الجريمة السيبرانية ..... 148
أولا: مصلحة مكافحة الجرائم المرتبطة بالتكنولوجيا الحديثة ..... 149
ثانيا: المكتب الوطني لمكافحة الجريمة المرتبطة بالتكنولوجيات الحديثة ..... 150
ثالثا: وحدة الآثار الرقمية بمعهد علوم الأدلة الجنائية التابع للمديرية العامة للأمن الوطني ..... 151

الباب الثاني: حدود فعالية آليات ضمان الأمن السيبراني ..... 155

الفصل الأول: مدى نجاعة الآليات الزجرية في تحقيق الأمن السيبراني ..... 159

المبحث الأول: محدودية مجموعة القانون الجنائي في مواجهة الجريمة السيبرانية ..... 160

المطلب الأول: عدم ملاءمة القواعد الجنائية التقليدية مع خصوصية الإجرام السيبراني. 161

الفقرة الأولى: جريمة النصب المعلوماتية ..... 161

الفقرة الثانية: جريمة السرقة المعلوماتية ..... 167

المطلب الثاني: ضعف النصوص الزجرية المنظمة للجريمة السيبرانية ..... 173

الفقرة الأولى: قصور النصوص الزجرية المتعلقة بالمس بنظم المعالجة الآلية للمعطيات ... 174

الفقرة الثانية: قصور قانون مكافحة الإرهاب ..... 180

المبحث الثاني : تفعيل التدابير الزجرية للتصدي للجريمة السيبرانية ..... 184

المطلب الأول: اعتماد آليات توسيع التجريم لمواجهة الجريمة السيبرانية ..... 185

الفقرة الأولى: الجرائم الواقعة على النظام المعلوماتي ..... 186

أولا: جريمة التعامل في العملات الالكترونية (البتكوين) نموذجا ..... 186

ثانيا: جريمة تضخم البريد الالكتروني (Spam) ..... 189

ثالثا: جريمة السطو الالكتروني على العلامة التجارية ..... 191

رابعا: جريمة العبث بالأدلة الرقمية ..... 193

الفقرة الثانية: الجرائم المرتبطة بالمحتوى ..... 194

أولا: جريمة التنمر السيبراني Cyber bullying ..... 195

ثانيا جريمة الترويج لممارسة أنشطة القمار ..... 197

المطلب الثاني: السياسة العقابية الحديثة لمواجهة الجريمة السيبرانية ..... 198

الفقرة الأولى: التشديد العقابي في الجرائم السيبرانية ..... 199

أولا: تغليظ العقوبات السالبة للحرية وزيادة العقوبات المالية ..... 199

ثانيا: مسألة الشخص الاعتباري جنائيا ..... 202

الفقرة الثانية: العقوبات الإضافية في الجرائم السيبرانية ..... 205

أولا: إغلاق المؤسسة أو حجب الموقع الالكتروني ..... 206

ثانيا: الحرمان من استعمال أي شبكة معلوماتية ..... 208
الفقرة الثالثة: إدراج العقوبات البديلة للعقوبات السالبة للحرية ..... 210
**الفصل الثاني مدى فعالية الآليات الإجرائية في ضمان الأمن السيبراني ..... 214**
المبحث الأول: تحديات إجراءات البحث والتحقيق في الجريمة السيبرانية وسبل تجاوزها .215
المطلب الأول: محدودية آليات البحث والتحقيق في الجريمة السيبرانية..... 216
الفقرة الأولى: الانتقال ومعاينة مسرح الجريمة السيبرانية ..... 217
الفقرة الثانية: صعوبات إجراءات التفتيش وحجز الدليل الرقمي ..... 221
أولا: عوائق إجراءات التفتيش ..... 222
ثانيا: عوائق إجراء الحجز في الجريمة السيبرانية ..... 231
الفقرة الثالثة: قصور الشهادة والخبرة في إثبات الجريمة السيبرانية ..... 233
أولا: محدودية الشهادة التقليدية..... 233
ثانيا: محدودية الخبرة التقليدية ..... 236
المطلب الثاني: تفعيل آليات البحث والتحقيق بقواعد جديدة..... 239
الفقرة الأولى: تطوير إجراءات التفتيش والحجز التقليدية في الجريمة السيبرانية ..... 240
أولا: اعتماد ضوابط حديثة للتفتيش..... 240
ثانيا: اعتماد إجراءات حديثة لعملية الحجز ..... 245
الفقرة الثانية: الاعتماد على الإجراءات المستحدثة كآلية للحصول على الدليل الرقمي .....249
أولا: اعتماد تقنية الاختراق كآلية لكشف الجريمة السيبرانية..... 249
ثانيا: اعتماد آليات خاصة بالحفظ وتسجيل البيانات الالكترونية وجمعها ..... 250
ثالثا: إلزام المؤسسات والأشخاص بالإدلاء بالبيانات بناء على أمر قضائي ..... 254
المبحث الثاني: عوائق التعاون الدولي في الجريمة السيبرانية وسبل تجاوزها ..... 260
المطلب الأول: تأثير تباين التشريعات في فعالية التعاون الدولي..... 261
الفقرة الأولى: عدم وجود نموذج موحد للنشاط الإجرامي ..... 261
الفقرة الثانية: اختلاف النظم القانونية الإجرائية ..... 263
الفقرة الثالثة: ضعف التنسيق والتواصل بين أعضاء المجتمع الدولي ..... 264
المطلب الثاني: العوائق الإجرائية للتعاون الدولي وسبل تجاوزها..... 264

الفقرة الأولى: إشكالية الاختصاص القضائي وسبل تجاوزها ..... 265
أولا: الاختصاص القائم على أساس مبدأ إقليمية النص الجنائي ..... 265
ثانيا: الاختصاص القائم على أساس مبدأ شخصية النص الجنائي ..... 267
ثالثا: الاختصاص القائم على مبدأ العينية ..... 270
الفقرة الثانية: إشكاليات المساعدة القضائية وسبل تجاوزها ..... 273
أولا: الإنابة القضائية الدولية ..... 274
ثانيا: تبادل المعلومات ..... 276
الفقرة الثالثة: تسليم المجرمين في إطار الجريمة السيبرانية ..... 279
أولا: تسليم المجرم السيبراني على وفق الشروط المقررة للجريمة التقليدية ..... 281
ثانيا: أثر جنسية المجرم السيبراني على تفعيل التسليم ..... 286
ثالثا: إشكالية تعدد طلبات التسليم ..... 289
خاتمة ..... 293
لائحة المراجع المعتمدة ..... 301
فهرس المحتويات ..... 323

DAR AL AFAK
COPY

يشهد العالم اليوم ثورة رقمية غير مسبوقة، حيث تتغلغل التكنولوجيا في كافة جوانب حياتنا اليومية، من التواصل والتجارة إلى الخدمات الحكومية والبنية التحتية الحيوية. ومع هذا التطور الهائل، يبرز تحدٍّ ملحّ يهدد استقرار وأمن المجتمعات، ألا وهو الأمن السيبراني. فالأنظمة المعلوماتية، التي أصبحت عصب الحياة الحديثة، عرضة لتهديدات متزايدة التعقيد والتطور، مما يستدعي ضرورة ملحة لوضع استراتيجيات وسياسات فعالة لحمايتها.

وعموما تكمن فائدة هذا الكتاب في أنه يتناول جملة التحديات التي تعيق تحقيق الأمن السيبراني في السياقات المغربية والعربية والدولية، مثل الفجوة الرقمية، ونقص الوعي بأهمية الأمن السيبراني، وضعف البنية التحتية التقنية والقانونية. كما يحلل فعالية الإجراءات الوقائية والدفاعية المتخذة لمواجهة الجرائم السيبرانية، ويقدم توصيات لتطوير السياسات والقوانين المتعلقة بالأمن السيبراني، مع التركيز على أهمية التعاون الإقليمي والدولي في هذا المجال مستهدفا تقديم رؤية مستقبلية للأمن السيبراني في المغرب والعالم العربي، وتبني استراتيجيات شاملة ومستدامة لمواجهة التحديات المتزايدة في هذا المجال.

وبذلك يستهدف الكتاب فئة واسعة من القراء، بما في ذلك صناع القرار والسياسات، والباحثين والأكاديميين، والمتخصصين في مجال الأمن السيبراني، والمهتمين بالشأن الرقمي. كما يسهم في إثراء النقاش حول إشكالات الأمن السيبراني، وتقديم رؤى وتوصيات عملية لتعزيزه في المغرب والمنطقة العربية.

من المؤكد ان هذا الكتاب بما احتواه يشكل إضافة نوعية للمكتبة القانونية المغربية والعربية في مجال الأمن السيبراني، كما أن الاستنتاجات التي توصل إليها والتوصيات التي قدمها تشكل لا محالة نواة رؤية علمية وعملية لتعزيز الأمن السيبراني في المغرب والمنطقة العربية انطلاقا من الإيمان بأن تحقيق الأمن السيبراني يتطلب تضافر جهود كافة الأطراف المعنية، من حكومات وقطاع خاص ومجتمع مدني، من أجل بناء فضاء سيبراني آمن وموثوق يستفيد منه الجميع.

## تقديم

**الأستاذ الدكتور رياض فخري**

مدير مختبر البحث قانون الأعمال
بجامعة الحسن الأول بسطات المملكة المغربية
المستشار القانوني للاتحاد العربي للتمكين الرقمي

مكتبة دار السلام

الهاتف - الفاكس : 05 37 72 58 23
Site web : www.darassalam.ma
E-mail : contact@darassalam.ma

الثمن : 100 درهم

9 789920 519953