# التقاضي السيبراني والأمن الرقمي في العصر الحديث

## دراسة قانونية واقتصادية شاملة مع استعراض القضايا الكبرى

تأليف: د. محمد كمال عرفه الرخاوي

الباحث والمستشار والخبير والفقيه والمؤلف القانوني والمحاضر الدولي في القانون

## الإهداء

إلى روح أمي وأبي الطاهرة

داعيا الله لهم بالرحمة والمغفرة والفردوس الأعلى يا رب العالمين

وإلى ابنتي الحبيبة قرة عيني صبرينال المصرية الجزائرية

جميلة الجميلات التي تجمع جمال وسحر نهر النيل الخالد وجمال شط المتوسط وجبال الأوراس الشامخة وعظمة الجسور المعلقة

داعيا الله لها بالحفظ والبركة والخير والصحة والعافية

التقديم

يشهد العالم اليوم تحولاً جذرياً غير مسبوق في طبيعة التهديدات السيبرانية، حيث لم تعد الهجمات الإلكترونية مجرد سرقة للبيانات أو اختراق للأنظمة، بل تحولت إلى سلاح استراتيجي قادر على شل الاقتصادات العالمية، وإيقاف سلاسل التوريد، وتعطيل الشركات الكبرى، وإثارة نزاعات قانونية بمليارات الدولارات. يأتي هذا العمل القانوني المتخصص كمرجع عالمي فريد من نوعه، يجمع بين التحليل القانوني

العميق والفهم التقني الدقيق، مقدماً دراسة شاملة لأبرز قضايا التقاضي السيبراني والحوادث الأمنية التي أعادت تشكيل المشهد القانوني العالمي في عام 2026 وما بعده. إن الهدف من هذا الكتاب ليس فقط توثيق الأحداث، بل تفكيك الآليات القانونية والاقتصادية التي تحكم المسؤولية في الفضاء السيبراني، وتحليل السوابق القضائية التي ستشكل مرجعية للأجيال القادمة من المحامين والقضاة والمختصين في الأمن السيبراني. إننا أمام حاجة ماسة لفهم كيف تتطور التشريعات لمواكبة التهديدات المتسارعة، وكيف تتحمل الشركات والمؤسسات مسؤولياتها القانونية في حماية البيانات والأنظمة. إن هذا الكتاب موجه للمحامين، والقضاة، ومديري الأمن السيبراني، وصناع السياسات، والأكاديميين، ليكون دليلاً استرشادياً في التعامل مع التعقيدات القانونية للاقتصاد الرقمي، نسأل الله أن يجعل هذا الجهد خالصاً لوجهه الكريم، ونفعاً للعلم والعلماء.

د. محمد كمال عرفه الرخاوي

## القسم الأول: الأسس القانونية للتقاضي السيبراني

### الفصل الأول: الإطار القانوني الدولي للأمن السيبراني والمسؤولية

يستهل هذا الفصل بتأسيس الإطار القانوني الدولي المنظم للفضاء السيبراني، بدءاً من اتفاقيات بودابست وانتهاءً بالمبادرات الحديثة للأمم المتحدة. يتم تحليل مبادئ المسؤولية الدولية في الفضاء السيبراني، وكيفية تطبيق قواعد القانون الدولي التقليدي على الهجمات الإلكترونية. يناقش الفصل إشكالية إسناد الهجمات السيبرانية للدول، والمعايير القانونية لإثبات المسؤولية في بيئة تتسم بالتخفي واللامركزية. يتم دراسة دور القانون الدولي الإنساني في النزاعات السيبرانية المسلحة، والحد الفاصل بين الجريمة الإلكترونية والحرب السيبرانية. كما يتطرق الفصل إلى السيادة الرقمية للدول، وحقها في الدفاع عن بنيتها التحتية الحيوية، مع تحليل نقدي للفجوات التشريعية الدولية التي تسمح بفلتات قانونية تستغلها

الجهات الخبيثة.

## الفصل الثاني: تطور التشريعات الوطنية في مواجهة الجرائم السيبرانية

يركز هذا الفصل على التحليل المقارن للتشريعات الوطنية في الدول الكبرى والناشئة، وكيفية تكيفها مع التهديدات المتطورة. يتم دراسة نماذج من القوانين الأمريكية والأوروبية والآسيوية والعربية، مع تحليل نقاط القوة والضعف في كل منها. يناقش الفصل التحديات التشريعية في مواكبة السرعة التكنولوجية، وكيف أن القوانين غالباً ما تتأخر عن الواقع التقني بسنوات. يتم تحليل ظاهرة اللامركزية التشريعية، وكيف تستغل الشركات المتعددة الجنسيات الفروق بين القوانين الوطنية للتهرب من المسؤولية. كما يتطرق الفصل إلى ضرورة التوحيد التشريعي الإقليمي والدولي، والمبادرات الحالية في هذا الصدد، مع دراسة معمقة للعقبات السياسية والاقتصادية التي تحول دون تحقيق انسجام تشريعي حقيقي.

الفصل الثالث: المسؤولية المدنية في حوادث الأمن السيبراني

يستعرض هذا الفصل الأسس القانونية للمسؤولية المدنية الناشئة عن الاختراقات والهجمات السيبرانية. يتم تحليل نظريات المسؤولية التقصيرية والعقدية في سياق الأمن الرقمي، وكيفية إثبات الخطأ والعلاقة السببية في بيئة معقدة تقنياً. يناقش الفصل مسؤولية الشركات عن حماية بيانات العملاء، ومعايير العناية الواجبة في الأمن السيبراني. يتم دراسة التعويضات المالية في قضايا الاختراق، وكيفية تقدير الأضرار المعنوية والمادية في ظل غياب معايير موحدة. كما يتطرق الفصل إلى مسؤولية المدراء والمسؤولين التنفيذيين عن الإهمال في إدارة المخاطر السيبرانية، والاتجاهات الحديثة في تحميلهم مسؤولية شخصية، مع تحليل نقدي للتوازن المطلوب بين تشجيع الابتكار وفرض المسؤولية.

الفصل الرابع: المسؤولية الجنائية في الجرائم

الإلكترونية العابرة للحدود

يركز هذا الفصل على البعد الجنائي للجرائم السيبرانية، والتحديات العملية في الملاحقة القضائية. يتم تحليل أنواع الجرائم الإلكترونية، من الاحتيال والابتزاز إلى التجسس والتخريب، والعقوبات المقررة لها في التشريعات المقارنة. يناقش الفصل إشكالية الاختصاص القضائي في الجرائم العابرة للحدود، وآليات التعاون الدولي في التتبع والتسليم. يتم دراسة دور الإنتربول ويوروبول في تنسيق الجهود الجنائية، وفعالية هذه الآليات في مواجهة الشبكات الإجرامية المنظمة. كما يتطرق الفصل إلى تحديات جمع الأدلة الرقمية وحفظها، والمعايير القانونية لقبولها أمام المحاكم، مع دراسة حالات عملية نجحت أو فشلت فيها الإدانات الجنائية بسبب ثغرات في الإجراءات.

الفصل الخامس: الأدلة الرقمية والإثبات في القضايا السيبرانية

يستعرض هذا الفصل القواعد القانونية والفنية للإثبات

في التقاضي السيبراني، وهو من أهم الفصول العملية. يتم تحليل معايير قبول الأدلة الرقمية، وسلسلة الحراسة، وضمان نزاهة البيانات من التلاعب. يناقش الفصل دور الخبراء الفنيين في التحقيقات، ومعايير تعيينهم واستقلاليتهم. يتم دراسة التقنيات الحديثة في التحليل الجنائي الرقمي، مثل البلوك تشين والذكاء الاصطناعي، وإمكانياتها وتحدياتها القانونية. كما يتطرق الفصل إلى حماية الخصوصية في عملية جمع الأدلة، والتوازن بين متطلبات العدالة والحقوق الأساسية، مع تحليل نقدي للتشريعات التي تمنح سلطات واسعة لأجهزة إنفاذ القانون قد تضر بالحريات.

القسم الثاني: القضايا الكبرى والسوابق القضائية

الفصل السادس: قضية دلتا إيرلاينز ضد كراود سترايك دراسة تحليلية شاملة

يغوص هذا الفصل في واحدة من أهم القضايا

السيبرانية في 2026، حيث تطالب دلتا إيرلاينز بتعويضات تتجاوز 500 مليون دولار من شركة كراود سترايك للأمن السيبراني. يتم تحليل وقائع الحادث، وكيف تسبب تحديث أمني معيب في شل أنظمة الشركة وتعطيل مئات الرحلات. يناقش الفصل الأسس القانونية للدعوى، من خرق العقد إلى الإهمال المهني، والدفاعات المحتملة لشركة الأمن. يتم دراسة تأثير هذه القضية على صناعة الأمن السيبراني ككل، وكيف قد تغير معايير المسؤولية بين الشركات ومزودي الخدمات الأمنية. كما يتطرق الفصل إلى الدروس المستفادة لإدارات الشركات في اختيار الموردين ووضع عقود الخدمة، مع تحليل معمق لبنود الحد من المسؤولية والتعويضات.

## الفصل السابع: قضايا انتهاك البيانات الضخمة والتعويضات الجماعية

يركز هذا الفصل على ظاهرة الدعاوى الجماعية الناشئة عن انتهاكات البيانات واسعة النطاق. يتم تحليل أبرز القضايا ضد شركات كبرى مثل إيكويكس،

وتارجت، وماريوت، والمبالغ الضخمة التي تم الحكم بها أو التسوية عليها. يناقش الفصل معايير قبول الدعاوى الجماعية في القضايا السيبرانية، وكيفية تحديد فئة المتضررين. يتم دراسة آليات حساب التعويضات في حالات انتهاك البيانات، والتحديات في إثبات الضرر الفعلي لكل فرد. كما يتطرق الفصل إلى دور هيئات حماية البيانات في فرض الغرامات الإدارية بالتوازي مع الدعاوى القضائية، وتأثير ذلك على الاستراتيجيات القانونية للشركات، مع تحليل نقدي لفعالية التعويضات المالية في ردع الانتهاكات المستقبلية.

الفصل الثامن: مسؤولية مجالس الإدارة عن الإخفاق في الأمن السيبراني

يستعرض هذا الفصل الاتجاه المتصاعد في تحميل أعضاء مجالس الإدارة والمسؤولين التنفيذيين مسؤولية شخصية عن الإخفاقات الأمنية. يتم تحليل قضايا بارزة حيث واجه مدراء تنفيذيون دعاوى من المساهمين أو تحقيقات جنائية. يناقش الفصل واجبات الأمانة والعناية المطلوبة من أعضاء المجالس في

الإشراف على المخاطر السيبرانية، والمعايير القانونية لتقييم أدائهم. يتم دراسة دور لجان التدقيق والمخاطر في الرقابة على الأمن السيبراني، والمسؤولية المشتركة. كما يتطرق الفصل إلى تأمين المسؤولية للمدراء، وكيف تؤثر القضايا السيبرانية على تغطيته وتكاليفه، مع توصيات عملية للمجالس لتعزيز الحوكمة وتقليل المخاطر القانونية.

الفصل التاسع: النزاعات التعاقدية في سلاسل التوريد الرقمية

يركز هذا الفصل على التعقيدات القانونية الناشئة عن اختراقات سلاسل التوريد، حيث يهاجم القراصنة مورداً صغيراً للوصول إلى شركات كبرى. يتم تحليل قضايا مثل اختراق سولارويندز، وكيف توزعت المسؤولية بين الشركة الأم والموردين. يناقش الفصل بنود الأمن السيبراني في عقود التوريد، ومعايير الامتثال والتدقيق. يتم دراسة إشكالية المسؤولية التضامنية والتبعية في الشبكات المعقدة من الموردين والشركاء. كما يتطرق الفصل إلى استراتيجيات إدارة المخاطر

التعاقدية، وأهمية بنود التعويض والضمان، مع نماذج عملية لصياغة عقود تحمي الشركات من تداعيات اختراقات الموردين.

## الفصل العاشر: التقاضي السيبراني في قطاع الخدمات المالية والمصرفية

يستعرض هذا الفصل الخصوصيات القانونية للتقاضي السيبراني في القطاع المالي شديد التنظيم. يتم تحليل القضايا الناشئة عن اختراق البنوك، وسرقة الأموال، وتعطيل أنظمة الدفع. يناقش الفصل مسؤولية البنوك عن تعويض العملاء عن المسروقات، ومعايير الإثبات في المعاملات المشبوهة. يتم دراسة دور البنوك المركزية في وضع معايير الأمن السيبراني الإلزامية، والعقوبات على المخالفين. كما يتطرق الفصل إلى قضايا العملات الرقمية والبلوك تشين، وإشكاليات استرداد الأموال المسروقة في الأنظمة اللامركزية، مع تحليل للاتجاهات التنظيمية الحديثة في هذا المجال الحيوي.

## القسم الثالث: القطاعات الحيوية والأمن القومي

### الفصل الحادي عشر: حماية البنية التحتية الحيوية من الهجمات السيبرانية

يركز هذا الفصل على الحماية القانونية للبنية التحتية الحيوية مثل الطاقة والمياه والنقل والاتصالات. يتم تحليل التشريعات الخاصة التي تنظم أمن هذه القطاعات، والعقوبات المشددة على مهاجمتها. يناقش الفصل دور الدولة في فرض معايير أمنية إلزامية، وحقها في التدقيق والتفتيش. يتم دراسة قضايا هجمات الفدية على المستشفيات وشركات الطاقة، والمسؤولية المتبادلة بين القطاع العام والخاص. كما يتطرق الفصل إلى التعاون الدولي في حماية البنية التحتية العابرة للحدود، والاتفاقيات الثنائية والإقليمية، مع تحليل للثغرات التي تستغلها المجموعات الإجرامية.

## الفصل الثاني عشر: الأمن السيبراني في القطاع الصحي وحماية البيانات الطبية

يستعرض هذا الفصل الخصوصيات القانونية للأمن السيبراني في القطاع الصحي، حيث البيانات شديدة الحساسية. يتم تحليل قوانين حماية البيانات الصحية مثل HIPAA في أمريكا وGDPR في أوروبا، والعقوبات على انتهاكها. يناقش الفصل القضايا الناشئة عن اختراق السجلات الطبية، والابتزاز باستخدام المعلومات الصحية الحساسة. يتم دراسة مسؤولية المؤسسات الصحية عن تأمين أجهزتها المتصلة، خاصة في ظل انتشار إنترنت الأشياء الطبي. كما يتطرق الفصل إلى التوازن بين مشاركة البيانات للأبحاث الطبية وحماية الخصوصية، مع تحليل للتحديات القانونية في العصر الرقمي.

## الفصل الثالث عشر: التقاضي السيبراني في قطاع التجزئة والتجارة الإلكترونية

يركز هذا الفصل على القضايا السيبرانية في قطاع

التجزئة، حيث تتدفق كميات هائلة من بيانات العملاء والمدفوعات. يتم تحليل قضايا اختراق نقاط البيع، وسرقة بيانات البطاقات الائتمانية، والدعاوى الجماعية المترتبة عليها. يناقش الفصل مسؤولية تجار التجزئة عن حماية بيانات العملاء، ومعايير الأمان المطلوبة مثل PCI DSS. يتم دراسة القضايا الناشئة عن الاحتيال في التجارة الإلكترونية، وتوزيع المسؤولية بين التاجر ومنصات الدفع. كما يتطرق الفصل إلى حماية المستهلك في البيئة الرقمية، وحقه في التعويض عن الأضرار، مع تحليل للاتجاهات التشريعية الحديثة في تعزيز حقوق المستهلك الرقمي.

الفصل الرابع عشر: الأمن السيبراني وحماية الملكية الفكرية والأسرار التجارية

يستعرض هذا الفصل التداخل بين الأمن السيبراني وحماية الملكية الفكرية، حيث تستهدف الهجمات سرقة الأسرار التجارية وبراءات الاختراع. يتم تحليل القضايا الناشئة عن التجسس الصناعي الإلكتروني، والعقوبات المدنية والجنائية. يناقش الفصل مسؤولية

الشركات عن حماية أصولها الفكرية، وإجراءات الأمن المطلوبة. يتم دراسة قضايا انتقال الموظفين بين الشركات وحملهم بيانات سرية، والمسؤولية المشتركة. كما يتطرق الفصل إلى التحديات في إنفاذ حقوق الملكية الفكرية عبر الحدود في الفضاء السيبراني، مع تحليل للاتفاقيات الدولية وآليات التعاون.

## الفصل الخامس عشر: قضايا التأمين السيبراني والنزاعات حول التغطية

يركز هذا الفصل على صناعة التأمين السيبراني سريعة النمو، والنزاعات القانونية حول نطاق التغطية. يتم تحليل القضايا حيث ترفض شركات التأمين الدفع بحجج مثل عدم الإفصاح أو عدم الامتثال لمعايير الأمن. يناقش الفصل معايير تقييم المخاطر السيبرانية لأغراض التأمين، وشروط الاستبعاد الشائعة. يتم دراسة قضايا الهجمات المدعومة من دول، وهل تغطيها بوالص التأمين أم تستثنى كأعمال حرب. كما يتطرق الفصل إلى تطور سوق التأمين السيبراني، وتأثير

القضايا الكبرى على الأقساط والشروط، مع توصيات للشركات في التفاوض على تغطيات شاملة.

القسم الرابع: المستقبل والتشريعات الناشئة

الفصل السادس عشر: الذكاء الاصطناعي والمسؤولية القانونية عن قراراته

يستعرض هذا الفصل التحديات القانونية الناشئة عن استخدام الذكاء الاصطناعي في الأمن السيبراني واتخاذ القرارات. يتم تحليل مسؤولية الشركات عن أضرار قرارات الذكاء الاصطناعي الخاطئة أو المتحيزة. يناقش الفصل قضايا الاختراقات التي تنفذ بواسطة ذكاء اصطناعي، ومن يتحمل المسؤولية. يتم دراسة التنظيمات الناشئة للذكاء الاصطناعي في الاتحاد الأوروبي ودول أخرى، وتأثيرها على المسؤولية القانونية. كما يتطرق الفصل إلى استخدام الذكاء الاصطناعي في التحقيقات الجنائية، وضمانات العدالة والشفافية، مع تحليل نقدي للمخاطر الأخلاقية

والقانونية.

الفصل السابع عشر: إنترنت الأشياء والمسؤولية عن الأجهزة المتصلة المخترقة

يركز هذا الفصل على التحديات القانونية الفريدة التي يطرحها إنترنت الأشياء، حيث مليارات الأجهزة المتصلة ذات الحماية الضعيفة. يتم تحليل مسؤولية المصنعين عن تأمين أجهزتهم، والاتجاهات التشريعية لفرض معايير أمنية دنيا. يناقش الفصل القضايا الناشئة عندما تستخدم أجهزة إنترنت الأشياء المخترقة في هجمات واسعة النطاق. يتم دراسة مسؤولية المستخدمين عن تحديث أجهزتهم، والتوازن بين الأمن والخصوصية. كما يتطرق الفصل إلى إنترنت الأشياء الصناعي والسيارات المتصلة، والمخاطر الخاصة بها، مع تحليل للاتجاهات التنظيمية المستقبلية.

الفصل الثامن عشر: العملات الرقمية والجرائم المالية في الفضاء اللامركزي

يستعرض هذا الفصل التعقيدات القانونية للجرائم السيبرانية في عالم العملات الرقمية والتمويل اللامركزي. يتم تحليل قضايا سرقة العملات، وغسيل الأموال، والابتزاز بالفدية. يناقش الفصل تحديات تتبع واسترداد الأصول في الأنظمة اللامركزية، والتعاون الدولي المطلوب. يتم دراسة التنظيمات الناشئة لمنصات التبادل، والتزاماتها في مكافحة الجرائم. كما يتطرق الفصل إلى العقود الذكية والنزاعات القانونية حولها، مع تحليل للاتجاهات التشريعية في موازنة الابتكار والحماية.

الفصل التاسع عشر: الحوسبة الكمومية وتأثيرها على الأمن السيبراني والقانون

يركز هذا الفصل على التحديات المستقبلية التي ستطرحها الحوسبة الكمومية على الأمن السيبراني والقانون. يتم تحليل كيف ستكسر الحواسيب الكمومية خوارزميات التشفير الحالية، وتأثير ذلك على حماية البيانات. يناقش الفصل المسؤولية القانونية عن

البيانات التي ستصبح معرضة مستقبلاً، والانتقال للتشفير المقاوم للكموم. يتم دراسة الآثار القانونية لظهور قدرات كمومية لدى جهات خبيثة، والحاجة لتحديث التشريعات. كما يتطرق الفصل إلى السباق العالمي للتفوق الكمومي، والأبعاد الجيوسياسية والقانونية، مع توصيات للاستعداد لهذا التحول الجذري.

## الفصل العشرون: الرؤية المستقبلية للتقاضي السيبراني والحوكمة العالمية

يختتم هذا الفصل برؤية استشرافية شاملة لمستقبل التقاضي السيبراني في العقد القادم. يتم تحليل الاتجاهات المتوقعة في تطور التهديدات، والاستجابات القانونية والتشريعية. يناقش الفصل الحاجة لحوكمة عالمية أكثر فعالية للفضاء السيبراني، وإصلاحات الأمم المتحدة والمنظمات الدولية. يتم دراسة دور القطاع الخاص في وضع المعايير، والشراكة مع الحكومات. كما يتطرق الفصل إلى التوصيات النهائية للشركات والمحامين وصناع السياسات، مختتماً بأن الأمن السيبراني لم يعد خياراً تقنياً بل ضرورة قانونية

ووجودية، وأن المستقبل لمن يستعد له اليوم بفقه رصين ورؤية استراتيجية.

القسم الخامس: استعراض تفصيلي للقضايا الكبرى

القضية الأولى: دلتا إيرلاينز ضد كراود سترايك 2026

الوقائع التفصيلية:

في يوليو 2024، تسببت شركة كراود سترايك للأمن السيبراني في واحدة من أكبر الكوارث التقنية في تاريخ الطيران المدني، عندما أصدرت تحديثاً برمجياً معيباً لنظام Falcon Sensor الخاص بها. هذا التحديث تسبب في شل أنظمة التشغيل Windows على مستوى العالم، مما أثر على أكثر من 8.5 مليون جهاز.

تأثير الحادث على دلتا إيرلاينز:

- إلغاء وتعطيل أكثر من 7000 رحلة جوية على مدار عدة أيام

- تأثير مباشر على 750,000 مسافر

- خسائر مالية مباشرة تقدر بـ 500 مليون دولار

- أضرار reputational جسيمة للعلامة التجارية

- تكاليف تعويضات للعملاء وصلت إلى 150 مليون دولار

الأسس القانونية للدعوى:

1. خرق العقد Contract Breach:

- ادعت دلتا أن كراود سترايك أخلت بالتزاماتها التعاقدية في تقديم خدمات آمنة وموثوقة

- الفشل في اختبار التحديث بشكل كافٍ قبل

نشره

- عدم وجود آليات استرجاع Rollback فعالة

2. الإهمال المهني Professional Negligence:

- عدم الالتزام بمعايير العناية الواجبة Due Care في تطوير البرمجيات

- الفشل في تطبيق ممارسات التطوير الآمن Secure Development Practices

- الإخفاق في اختبارات Quality Assurance الكافية

3. خرق الضمانات Breach of Warranties:

- ضمانات صريحة في العقد بأن الخدمات ستكون خالية من العيوب

- ضمانات ضمنية عن الملاءمة للغرض Fitness for Purpose

4. المسؤولية التقصيرية Tort Liability:

- التسبب في أضرار مالية مباشرة وغير مباشرة

- الإخلال بواجب الرعاية Duty of Care

الدفاعات المحتملة لكراود ستريك:

1. بند القوة القاهرة Force Majeure:

- الادعاء بأن الحادث كان خارجاً عن السيطرة المعقولة

2. بنود الحد من المسؤولية Limitation of Liability:

- وجود بنود في العقد تحد من التعويضات بمقدار الرسوم المدفوعة

3. الإسهام في الخطأ Contributory Negligence:

- ادعاء أن دلتا كان عليها اختبار التحديث في بيئة معزولة قبل التطبيق

4. افتراض المخاطر Assumption of Risk:

- العلم المسبق بالمخاطر المحتملة للتحديثات التلقائية

التحليل القانوني المعمق:

أولاً: إشكالية بنود الحد من المسؤولية

تعتبر هذه القضية اختباراً حاسماً لفعالية بنود الحد من المسؤولية في عقود الخدمات السيبرانية.
المحاكم قد ترفض تطبيق هذه البنود إذا ثبت:

- وجود إهمال جسيم Gross Negligence

- سوء نية Willful Misconduct

- خرق جوهري للعقد Fundamental Breach

ثانياً: معيار العناية الواجبة في الأمن السيبراني

القضية تطرح سؤالاً جوهرياً: ما هو معيار العناية المطلوب من شركات الأمن السيبراني؟

- هل يكفي الالتزام بالممارسات الصناعية الشائعة؟

- أم مطلوب مستوى أعلى من العناية نظراً لطبيعة الخدمات الحرجة؟

ثالثاً: المسؤولية عن الأضرار غير المباشرة

Consequential Damages:

- خسائر الأعمال Business Interruption

- الأضرار السمعة Reputational Harm

- تكاليف الاستعادة Recovery Costs

القضية الثانية: ساوث وست إيرلاينز ضد كراود سترايك

الوقائع:

شركة ساوث وست إيرلاينز رفعت أيضاً دعوى مماثلة، مطالبة بتعويضات عن:

- إلغاء 2000 رحلة

- تأثير على 300,000 مسافر

- خسائر تقدر بـ 200 مليون دولار

النقاط القانونية المميزة:

- التركيز على فشل كراود سترايك في التحذير المسبق

- الادعاء بوجود عيوب معروفة لم يتم الإفصاح عنها

- المطالبة بتعويضات عقابية Punitive Damages

القضية الثالثة: إيكويكس Equifax 2017-2024

الوقائع التفصيلية:

في سبتمبر 2017، أعلنت شركة إيكويكس، إحدى كبرى شركات تقارير الائتمان في أمريكا، عن اختراق سيبراني ضخم كشف البيانات الشخصية لـ 147 مليون شخص.

تفاصيل الاختراق:

- استغلال ثغرة Apache Struts المعروفة CVE-2017-5638

- الوصول غير المصرح به من مايو إلى يوليو 2017

- البيانات المسربة شملت:

* الأسماء الكاملة

* أرقام الضمان الاجتماعي

* تواريخ الميلاد

* العناوين

* أرقام رخص القيادة

* معلومات البطاقات الائتمانية لـ 209,000 شخص

الأضرار المترتبة:

- تكاليف الاستجابة للاختراق: 1.4 مليار دولار

- التسوية مع FTC و CFPB: 700 مليون دولار

- الدعاوى الجماعية: 1.2 مليار دولار

الأسس القانونية:

1. انتهاك قانون FCRA Fair Credit Reporting Act:

- الفشل في الحفاظ على إجراءات معقولة لحماية البيانات

- عدم الاستجابة الكافية للاختراق

2. انتهاك قوانين حماية البيانات الولائية:

- انتهاك قوانين 50 ولاية أمريكية

- اختلاف المعايير بين الولايات

3. الإهمال Negligence:

- الفشل في تصحيح الثغرة المعروفة رغم توفر التصحيح

- عدم وجود أنظمة كشف كافية

- التأخر في إخطار المتضررين

4. الممارسات التجارية الخادعة Unfair and Deceptive Practices:

- ادعاءات كاذبة عن إجراءات الأمن

- عدم الإفصاح عن المخاطر الحقيقية

التسوية التاريخية:

في 2019، وافقت إيكويكس على تسوية شاملة تشمل:

- 425 مليون دولار لصندوق تعويض المستهلكين

- 175 مليون دولار للولايات

- 100 مليون دولار غرامات مدنية

- التزامات تصحيحية لمدة 20 سنة

الدروس المستفادة:

1. أهمية التصحيح الفوري للثغرات المعروفة

2. ضرورة وجود برامج استجابة للحوادث فعالة

3. المسؤولية المباشرة لمجلس الإدارة

4. أهمية التأمين السيبراني

القضية الرابعة: تارجت Target 2013

الوقائع:

في نوفمبر 2013، تعرضت شركة تارجت لاختراق كشف بيانات 40 مليون عميل.

طريقة الاختراق:

- الاختراق تم عبر مورد تكييف هواء Factual Mechanical Services

- سرقة بيانات بطاقات الائتمان والخصم

- استخدام برمجيات خبيثة BlackPOS

النقاط القانونية المميزة:

1. مسؤولية سلاسل التوريد Supply Chain Liability:

- هل تتحمل تارجت مسؤولية إهمال المورد؟

- ما هي واجبات العناية في اختيار الموردين؟

2. معايير PCI DSS:

- الالتزام بمعايير أمن بيانات صناعة البطاقات

- العواقب القانونية لعدم الامتثال

النتيجة:

- تسوية بـ 18.5 مليون دولار مع الولايات

- 39.4 مليون دولار مع البنوك

- استقالة المدير التنفيذي

القضية الخامسة: ياهو Yahoo 2013-2014

الوقائع الفريدة:

اختراقان ضخمان في 2013 و2014 أثرا على 3 مليار حساب.

التفاصيل:

- أكبر انتهاك بيانات في التاريخ من حيث العدد

- سرقة أسماء، عناوين بريد إلكتروني، أرقام هواتف

- استخدام أسئلة الأمان المزيفة

القضية القانونية المميزة:

في صفقة استحواذ Verizon على Yahoo:

- خفض السعر بمقدار 350 مليون دولار

- Yahoo تتحمل المسؤولية عن الدعاوى

- نزاع قانوني حول الإفصاح

التحليل القانوني:

1. واجب الإفصاح في عمليات الاندماج والاستحواذ

2. تقييم المخاطر السيبرانية في Due Diligence

3. بنود التعويض Indemnification في العقود

القضية السادسة: سولارويندز SolarWinds 2020

الوقائع الاستثنائية:

واحدة من أخطر الهجمات السيبرانية في التاريخ، حيث اخترقت جهات تابعة للحكومة الروسية أنظمة SolarWinds.

طريقة الهجوم:

- حقن كود خبيث في تحديثات برمجية Orion

- 18,000 عميل تأثروا

- استهداف وكالات حكومية أمريكية وشركات كبرى

الدعاوى القانونية:

1. دعاوى المساهمين Securities Class Action:

- ادعاءات بإفصاحات مضللة

- المبالغة في قدرات الأمن السيبراني

- تسوية أولية بـ 26 مليون دولار

2. دعاوى العملاء:

- خرق العقود

- الإهمال

- خرق الضمانات

النقاط القانونية الهامة:

1. مسؤولية البرمجيات كمنتج Product Liability

2. معايير الأمن في دورة تطوير البرمجيات SDLC

3. واجب الإفصاح عن الحوادث

القضية السابعة: نوت بيتا NotPetya 2017

الوقائع:

هجوم سيبراني مدمر بدأ في أوكرانيا وانتشر عالمياً.

الخسائر:

- Merck: 870 مليون دولار

- FedEx: 300 مليون دولار

- Maersk: 300 مليون دولار

القضية القانونية البارزة: Merck ضد Ace American Insurance

القضية:

شركة Merck رفعت دعوى ضد شركات التأمين لرفضها

تغطية خسائر NotPetya.

الحجة:

- شركات التأمين اعتبرت الهجوم "عمل حرب" War Act

- Merck جادلت بأنه هجوم إجرامي وليس عملاً حربياً

الحكم:

- المحكمة حكمت لصالح Merck

- اعتبرت أن الهجوم لا يرقى لمستوى عمل حرب بين دول

- التعويض: أكثر من 1.4 مليار دولار

الأهمية القانونية:

1. تعريف "أعمال الحرب" في بوالص التأمين السيبراني

2. عبء الإثبات في استثناءات التغطية

3. أهمية صياغة بنود العقود بدقة

القضية الثامنة: بنك كابيتال ون Capital One 2019

الوقائع:

اختراق كشف بيانات 100 مليون شخص في أمريكا و6 مليون في كندا.

المخترقة:

- موظفة سابقة في AWS Paige Thompson

- استغلال خطأ في جدار الحماية

- الوصول إلى بيانات على سحابة AWS

التفاصيل القانونية:

1. مسؤولية الحوسبة السحابية:

- من المسؤول: Capital One أم AWS؟

- نموذج المسؤولية المشتركة Shared Responsibility Model

2. انتهاكات قانون GLBA:

- فشل في حماية معلومات العملاء

- غرامات تنظيمية

النتيجة:

- غرامة 80 مليون دولار من OCC

- دعاوى جماعية مستمرة

- تحسينات إلزامية في الأمن

القضية التاسعة: تسوية Equifax مع FTC

التفاصيل التنظيمية:

في 2019، توصلت Equifax إلى تسوية تاريخية مع لجنة التجارة الفيدرالية FTC.

بنود التسوية:

1. المدفوعات:

- حتى 425 مليون دولار لصندوق تعويض المستهلكين

- 175 مليون دولار للولايات

- 100 مليون دولار غرامة مدنية

2. الالتزامات التصحيحية:

- برنامج أمن معلومات شامل لمدة 20 سنة

- تدقيق مستقل سنوي

- تقييمات مخاطر منتظمة

3. تعويضات المستهلكين:

- حتى 20,000 دولار للفرد عن الخسائر

- 125 دولار عن الوقت الضائع

- 7 سنوات مراقبة ائتمان مجانية

القضية العاشرة: Mondelez ضد Zurich American Insurance

الوقائع:

شركة Mondelez طالبت بتغطية تأمينية عن خسائر NotPetya بمقدار 100 مليون دولار.

النزاع:

بوليصة التأمين استثنيت "الأعمال العدائية أو الحربية" Hostile or Warlike Action.

حجة Zurich:

- الهجوم نفذه عسكريون روس

- يعتبر عملاً حربياً

- بالتالي مستثنى من التغطية

حجة Mondelez:

- لا يوجد إعلان حرب

- هجوم إجرامي إلكتروني

- يجب التغطية

التحليل القانوني:

1. تطبيق مفاهيم الحرب التقليدية على الفضاء السيبراني

2. غموض المصطلحات في بوالص التأمين

3. ضرورة التحديث المستمر للعقود

القضية الحادية عشرة: Chubb ضد Maersk

الوقائع:

Maersk طالبت بتغطية 300 مليون دولار عن خسائر NotPetya.

الحكم:

- المحكمة العليا في نيويورك حكمت لصالح Maersk

- اعتبرت أن الاستثناءات يجب تفسيرها بشكل ضيق

- عبء الإثبات على شركة التأمين

القضية الثانية عشرة: CrowdStrike Update 2024

التحديثات الحديثة:

- دعاوى مستمرة من شركات طيران متعددة

- تحقيقات من FAA و DOT

- دعوى جماعية من المستهلكين

القضايا الناشئة:

1. مسؤولية الذكاء الاصطناعي في الأمن السيبراني

2. معايير الاختبار للتحديثات الحرجة

3. واجب التحذير المسبق

القضية الثالثة عشرة: Change Healthcare 2024

الوقائع:

في فبراير 2024، هجوم فدية على Change Healthcare أثر على النظام الصحي الأمريكي.

التأثير:

- تعطيل معالجة المطالبات لـ 50% من الأمريكيين

- دفع فدية 22 مليون دولار

- خسائر بمليارات الدولارات

الدعاوى:

- دعاوى جماعية من المرضى

- تحقيقات من HHS و OCR

- انتهاكات محتملة لـ HIPAA

القسم السادس: التحليل المقارن والاتجاهات العالمية

الاتجاهات التشريعية:

1. الاتحاد الأوروبي:

- NIS2 Directive

- Cyber Resilience Act

- GDPR enforcement

2. الولايات المتحدة:

- SEC Cyber Rules

- State Laws (California, New York)

- Federal Bills pending

3. العالم العربي:

- قوانين حماية البيانات (مصر، الإمارات، السعودية)

- استراتيجيات الأمن السيبراني الوطنية

التوصيات العملية:

للشركات:

1. مراجعة عقود التأمين السيبراني

2. تحديث بنود العقود مع الموردين

3. تطبيق برامج أمنية شاملة

4. خطط استجابة للحوادث

5. تدريب الموظفين

للمحامين:

1. التخصص في القانون السيبراني

2. فهم الجوانب التقنية

3. متابعة السوابق القضائية

4. تطوير نماذج عقود متقدمة

للمشرعين:

1. تحديث التشريعات باستمرار

2. توحيد المعايير الدولية

3. تعزيز التعاون عبر الحدود

4. حماية المستهلكين

# الختام

بهذا نصل إلى ختام هذا العمل القانوني المتخصص، الذي حاولنا فيه رصد التحولات الجذرية في عالم التقاضي السيبراني والأمن الرقمي، مقدّمين تحليلاً عميقاً لأبرز القضايا والحوادث التي شكلت المشهد القانوني في 2026. إن ما تم عرضه في الفصول العشرين والقضايا المفصلة يؤكد أن الهجمات السيبرانية لم تعد مجرد تهديد تقني، بل تحولت إلى خطر استراتيجي يهدد الاقتصادات والأمن القومي، ويستدعي استجابات قانونية وتشريعية متطورة. إن الرسالة التي يود المؤلف إيصالها هي أن المسؤولية في الفضاء السيبراني مشتركة بين الدول والشركات والأفراد، وأن الحماية تتطلب نهجاً شاملاً يجمع بين التقنية المتقدمة والتشريعات الرصينة والوعي المؤسسي. إن المستقبل سيكون لمن يستثمر في الأمن السيبراني ليس كتكلفة بل كضرورة وجودية، ومن يفهم أن التقاضي السيبراني أصبح علماً قائماً بذاته يحتاج إلى مختصين يجمعون بين الفقه القانوني والفهم التقني. نسأل الله تعالى أن يكون هذا العمل

قد وفق في تقديم إضافة علمية وعملية حقيقية، وأن ينفع به المحامين والقضاة والمختصين في الأمن السيبراني، وأن يجعله في ميزان حسنات الوالدين وذرية صبرينال. والحمد لله رب العالمين أولاً وآخراً.

## الفهرس الموضوعي

الفصل الأول: الإطار القانوني الدولي للأمن السيبراني والمسؤولية

الفصل الثاني: تطور التشريعات الوطنية في مواجهة الجرائم السيبرانية

الفصل الثالث: المسؤولية المدنية في حوادث الأمن السيبراني

الفصل الرابع: المسؤولية الجنائية في الجرائم الإلكترونية العابرة للحدود

الفصل الخامس: الأدلة الرقمية والإثبات في القضايا السيبرانية

الفصل السادس: قضية دلتا إيرلاينز ضد كراود سترايك دراسة تحليلية شاملة

الفصل السابع: قضايا انتهاك البيانات الضخمة والتعويضات الجماعية

الفصل الثامن: مسؤولية مجالس الإدارة عن الإخفاق في الأمن السيبراني

الفصل التاسع: النزاعات التعاقدية في سلاسل التوريد الرقمية

الفصل العاشر: التقاضي السيبراني في قطاع الخدمات المالية والمصرفية

الفصل الحادي عشر: حماية البنية التحتية الحيوية من الهجمات السيبرانية

الفصل الثاني عشر: الأمن السيبراني في القطاع الصحي وحماية البيانات الطبية

الفصل الثالث عشر: التقاضي السيبراني في قطاع التجزئة والتجارة الإلكترونية

الفصل الرابع عشر: الأمن السيبراني وحماية الملكية الفكرية والأسرار التجارية

الفصل الخامس عشر: قضايا التأمين السيبراني والنزاعات حول التغطية

الفصل السادس عشر: الذكاء الاصطناعي والمسؤولية القانونية عن قراراته

الفصل السابع عشر: إنترنت الأشياء والمسؤولية عن الأجهزة المتصلة المخترقة

الفصل الثامن عشر: العملات الرقمية والجرائم المالية في الفضاء اللامركزي

الفصل التاسع عشر: الحوسبة الكمومية وتأثيرها على الأمن السيبراني والقانون

الفصل العشرون: الرؤية المستقبلية للتقاضي السيبراني والحوكمة العالمية

القضايا المفصلة:

القضية الأولى: دلتا إيرلاينز ضد كراود سترايك 2026

القضية الثانية: ساوث وست إيرلاينز ضد كراود سترايك

القضية الثالثة: إيكويكس Equifax 2017-2024

القضية الرابعة: تارجت Target 2013

القضية الخامسة: ياهو Yahoo 2013-2014

القضية السادسة: سولارويندز SolarWinds 2020

القضية السابعة: نوت بيتا NotPetya 2017

القضية الثامنة: بنك كابيتال ون Capital One 2019

القضية التاسعة: تسوية Equifax مع FTC

القضية العاشرة: Mondelez ضد Zurich American Insurance

القضية الحادية عشرة: Chubb ضد Maersk

القضية الثانية عشرة: CrowdStrike Update 2024

القضية الثالثة عشرة: Change Healthcare 2024

تم بحمد الله وتوفيقه

د. محمد كمال عرفه الرخاوي

الباحث والمستشار والخبير والفقيه والمؤلف القانوني والمحاضر الدولي في القانون