

Estado Libre Asociado de Puerto Rico  
TRIBUNAL DE APELACIONES  
PANEL XII

AMÉRICA PÉREZ  
HERNÁNDEZ

Demandante-Apelada

Vs.

COOPERATIVA DE  
VIVIENDAS LOS  
ROBLES

Demandada-Apelante

KLAN201900089

APELACIÓN  
procedente del  
Tribunal de Primera  
Instancia, Sala  
Superior de San  
Juan

Civil. Núm.  
SJ2018CV03840

Sobre: COBRO DE  
DINERO  
(ORDINARIO),  
DAÑOS Y OTROS

Panel integrado por su presidente, el Juez Hernández Sánchez, la Juez Brignoni Mártir y la Juez Méndez Miró.

**Hernández Sánchez, Juez ponente**

**SENTENCIA**

En San Juan, Puerto Rico, a 22 de agosto de 2019.

Comparece ante nuestra consideración La Cooperativa Los Robles (en adelante, La Cooperativa o Apelante) y nos solicita que revoquemos la Sentencia Parcial emitida por el Tribunal de Primera Instancia, Sala Superior de San Juan, el 20 de diciembre de 2018, y notificada el 21 de diciembre de 2018, mediante la cual dicho foro desestimó la *Reconvención* incoada por La Cooperativa en contra de América Pérez Hernandez (en adelante, Pérez Hernández).

Por los fundamentos que expondremos a continuación, se *confirma* la Sentencia apelada.

I

Los hechos relevantes a esta controversia comenzaron cuando Pérez Hernández presentó una *demanda* por incumplimiento de contrato, cobro de dinero, despido injustificado, represalias, daños y perjuicios.<sup>1</sup> En esta, alegó que había trabajado por contrato como secretaria-recepcionista de La Cooperativa desde el 2011, aunque

<sup>1</sup> Véase, Sentencia Parcial en las págs. 96-127 del apéndice del recurso y Demanda en las págs. 1-7 Alegato de la Parte Apelada.

ejerció funciones propias de una administradora. Posteriormente, se le contrató como administradora. El último de los contratos fue terminado por La Cooperativa antes de culminar su vigencia, el 3 de agosto de 2017. Por su parte, La Cooperativa presentó su *Contestación a la demanda* el 16 de junio de 2018. De otra parte, el 13 de septiembre de 2018, La Cooperativa presentó una *Reconvencción* contra Pérez Hernández al amparo de varios estatutos federales, a saber: *The Computer Fraud and Abuse Act*, 18 USCA sec. 1030; *The Wire Froud*, 18 USCA sec. 1343 y *The Stored Communication Act* 18 USCA sec. 2501.<sup>2</sup> En particular, La Cooperativa alegó que Pérez Hernández impidió el acceso de La Cooperativa a sus propios sistemas de computadora y de seguridad. Además, advino en posesión de varios documentos de La Cooperativa exclusivamente, entre otros asuntos. Todo lo cual le provocó daños ascendentes a \$100,000.00, alegadamente.

A tenor con ello, Pérez Hernández presentó una *Moción de desestimación* contra la Reconvencción presentada por La Cooperativa.<sup>3</sup> Tras la correspondiente *Oposición*, el Tribunal de Primera Instancia celebró una *Vista* el 14 de noviembre de 2018, en la cual las partes arguyeron sus posturas respecto a esta reconvencción.<sup>4</sup> Así las cosas, el 20 de septiembre de 2018, el foro primario dictó la *Sentencia Parcial* que aquí se impugna. En esta, desestimó la Reconvencción presentada por La Cooperativa por no justificar la concesión de un remedio.<sup>5</sup>

Inconforme, La Cooperativa presentó este recurso junto a una solicitud de paralización de los procedimientos en auxilio de jurisdicción, e hizo el siguiente señalamiento de error:

ERRÓ EL TPI AL APLICAR LOS ESTATUTOS  
COMPRENDIDOS POR EL COMPUTER FRAUD AND  
ABUSE ACT, 18 U.S.C.A. § 1030, WIRE FRAUD, 18

<sup>2</sup> Véase pág. 1 del apéndice del recurso.

<sup>3</sup> Véase pág. 27 del apéndice del recurso.

<sup>4</sup> Véase pág. 48 del apéndice del recurso.

<sup>5</sup> Véase, Sentencia Parcial en las págs. 96-127 del apéndice del recurso.

U.S.C.A. § 1343, Y STORED COMMUNICATIONS ACT,  
18 U.S.C.A. § 2501.

Con el recurso ante nuestra consideración, el 28 de enero de 2019, emitimos una *Resolución* en la cual concedimos un término a Pérez Hernández para que presentara su oposición al recurso. El 20 de febrero de 2019, recibimos la comparecencia de Pérez Hernandez. En esta, se incluyó una solicitud de imposición de sanciones por tratarse, a su juicio, de un recurso frívolo que no cumplió con las disposiciones de nuestro reglamento respecto al auxilio de jurisdicción.

## II

### *Computer Fraud and Abuse Act*

El *Computer Fraud and Abuse Act* 18 USC § 1030, crea una causa de acción a favor de aquellos que sufran daños o pérdidas por causa de un tercero que accede de manera intencional una computadora sin autorización o, abusando de dicha autorización, obtiene información de una computadora protegida.<sup>6</sup>

Las computadoras protegidas por dicho estatuto están definidas como aquellas utilizadas exclusivamente por una institución financiera o el gobierno de los Estados Unidos, o aquellas que, aunque no de manera exclusiva, sean utilizadas por una institución financiera o el gobierno de los Estados Unidos, y el acto afecta la utilización de la institución financiera o del gobierno. La ley también incluye aquellas computadoras que sean utilizadas por o para el comercio interestatal o comercio externo y que afecten el comercio o comunicación interestatal de los Estados Unidos.<sup>7</sup>

<sup>6</sup> *The Act creates a cause of action for persons “who suffer[ ] damage or loss” because, inter alia, a third party “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... information from any protected computer.”* 18 U.S.C. § 1030(a)(2)(C), (g). *In Re Google Inc. Cookie Placement Consumer Privacy Litigation*, 806 F.3d 125 (2015).

<sup>7</sup> (2) the term “protected computer” means a computer--

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

El estatuto federal dispone que la parte que haya sufrido pérdidas o daños a raíz de una violación a la ley podrá reclamar compensación.<sup>8</sup> El término prescriptivo de la acción civil es de dos años desde la violación o desde el conocimiento del daño.<sup>9</sup>

La jurisprudencia federal ha limitado la aplicación de la ley en casos de empleados que utilizan una computadora cuando el uso de dichos equipos está autorizado.<sup>10</sup> Se ha determinado que empleados que accedan información electrónica como parte de sus funciones no violan la prohibición del *Computer Fraud and Abuse Act* sobre el acceso no autorizado de una computadora protegida<sup>11</sup> aun cuando el empleado hace mal uso de la información.<sup>12</sup>

#### *The Stored Communications Act*

El *Stored Communications Act* fue aprobado por el congreso de los Estados Unidos en el 1986 como parte del *Electronic Communications Privacy Act*, con el propósito de atender preocupaciones sobre la seguridad de las operaciones de almacenaje

(B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States... 18 USC § 1030 (e)(2)(A)(B).

<sup>8</sup> (g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware. 18 USC § 1030 (g).

<sup>9</sup> 18 USC § 1030 (g).

<sup>10</sup> To prevail on a civil claim under the Computer Fraud and Abuse Act (CFAA), a plaintiff must show that defendant accessed its computer system without approval, and it is not enough to prove access to information beyond the scope of approval. 18 U.S.C.A. § 1030(a)(2)(C). *Fischkoff v. Iovance Biotherapeutics, Inc.*, 339 F. Supp. 3d 408, 2018 I.E.R. Cas. (BNA) 384119 (S.D. N.Y. 2018).

<sup>11</sup> Employees who accessed employer's electronic information in ordinary course of their duties did not violate Computer Fraud and Abuse Act's (CFAA) prohibition against unauthorized access to protected computers, even if they subsequently misused or misappropriated that information after they left employer, where employer had granted them unfettered access to its computer system and information residing on it. 18 U.S.C.A. § 1030(a)(4); 18 U.S.C.(2006 Ed.) § 1030(a)(5)(A)(iii). *Orbit One Communications, Inc. v. Numerex Corp.*, 692 F. Supp. 2d 373 (S.D. N.Y. 2010).

<sup>12</sup> If an employer has given an employee access to a computer and to the relevant files, the employee's subsequent misuse of the information or misappropriation with the intent to compete with his employer is not sufficient to violate the Computer Fraud and Abuse Act (CFAA). 18 U.S.C.A. § 1030(a)(2)(C). *Apple Mortgage Corp. v. Barenblatt*, 162 F. Supp. 3d 270 (S.D. N.Y. 2016).

Formatted: Font: Italic, English (United States)

Formatted: English (United States)

Formatted: Font: Italic, English (United States)

Formatted: English (United States)

remoto de datos de computación y grandes bases de datos que almacenan correos electrónicos.<sup>13</sup>

Para presentar una acción al amparo de dicha ley, el demandante debe mostrar que el demandado (1) intencionalmente accedió sin autorización una facilidad a través de la cual se ofrecen servicios de comunicación electrónica, o (2) que de manera intencional abusó de la autorización para acceder la facilidad y obtener, alterar o impedir el acceso autorizado a comunicaciones electrónicas almacenadas en dicho sistema.<sup>14</sup> La jurisprudencia ha definido una facilidad de almacenaje como aquella que pertenece a un proveedor de servicios de red electrónica incluyendo proveedores de comunicación telefónica, de internet y de servicios de correo electrónico. La ley federal no protege equipos personales de computación pues dichos equipos no son considerados facilidades de almacenamiento o “*electronic storage*” conforme el *Stored Communications Act*.<sup>15</sup> Desde los orígenes de la medida es manifiesta la intención de proteger de manera específica información almacenada por proveedores de comunicación centralizada. No surge de la discusión para la creación de la ley la intención de proteger las computadoras de uso individual.<sup>16</sup>

#### *The Wiretap Act*

El *Wiretap Act* tipifica como delito la acción de interceptar comunicación electrónica de manera intencional.<sup>17</sup> Asimismo, dicha

<sup>13</sup> Congress passed the *Stored Communications Act* in 1986 as part of the *Electronic Communications Privacy Act* to address concerns that the advent of remote computing operations and large databanks of stored electronic communications would give rise to threats to individual privacy not addressed by the Fourth Amendment. The Act protects against the improper access and wrongful public disclosure of electronic communications by law enforcement authorities as well as unauthorized private parties. 1 A.L.R. Fed. 3d Art. 1

<sup>14</sup> To state a claim under the *Stored Communications Act*, a plaintiff must show that the defendant “(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system.” 18 U.S.C. § 2701(a); *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 806 F.3d 125 (2015) a la pág. 14.

<sup>15</sup> Véase, *García v. City of Laredo, Tex.*, 702 F.3d 788 (5to Cir.2012), a la pág. 793

<sup>16</sup> Véase, *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, supra a la pág. 15 y discusión del *Stored Communications Act* Sen. Rep. No. 99-541 (1986).

<sup>17</sup> Véase, *DIRECTV, Inc. v. Bennett*, 470 F.3d 565, 566-67 (5th Cir.2006); 18 U.S.C. §§ 2511(1); 2520(a).

disposición legal provee una causa de acción para que aquellas personas que fueron víctimas de la conducta criminal puedan reclamar por los daños sufridos.<sup>18</sup>

Para que prospere una acción al amparo del *Wiretap Act*, la parte demandante debe alegar que la parte demandada, de manera intencional, interceptó, divulgó o utilizó el contenido de una comunicación electrónica por medio de algún equipo.<sup>19</sup> La Ley establece una excepción a su aplicación pues no prohíbe el que una persona intercepte una comunicación electrónica si la persona participa en la comunicación o tiene la autorización de una de las partes en la comunicación.<sup>20</sup>

### III

En el caso que tenemos ante nos, la parte Apelante alegó que el TPI erró al resolver descansando en lo establecido en *In Re Google Inc. Cookie Placement Consumer Privacy Litigation*, supra. Según la parte, dicho caso fue revocado en todo lo relevante al presente caso por un tribunal de mayor jerarquía en el caso *In Re Google Inc. Cookie Placement Consumer Privacy Litigation* 803 F.3d 125 (2015). El Apelante señala que, en el caso de autos, La Cooperativa como dueña de la información, reclama por la intervención ilegal de la apelada, América Pérez Hernández, pero que dicha información se encuentra en manos de un tercero proveedor de servicios de correo electrónico “Google”, quien alberga el sistema de mensajería “Gmail”. La parte expresa que, en el caso de *Google*, los usuarios reclaman

<sup>18</sup> Under the Wiretap Act, “any person whose wire, oral, or electronic communication is ... disclosed ... may in a civil action recover from the person or entity ... such relief as may be appropriate,” including damages and attorney’s fees, Id. § 2520(a) *In Re Zynga Privacy Litigation*, 750 F.3d 1098 (2014).

<sup>19</sup> A plaintiff pleads a prima facie case under the Wiretap Act by showing that the defendant “(1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication, (5) using a device.” *In re Pharmatrak, Inc. Privacy Litig.*, 329 F.3d 9, a la pag.18 (1st Cir.2003) y 18 USC § 2520(a).

<sup>20</sup> The Wiretap Act does not make it unlawful “for a person to ‘intercept ... electronic communication’ if the person ‘is [1] a party to the communication or [2] where one of the parties to the communication has given prior consent to such interception ....’ *In Re: Nickelodeon Consumer Privacy Litigation* 827 F.3d 262 (2016) a la pág. 274 citando el caso de *Nickelodeon I*, 2014 WL 3012873, a la pág. 13 citando el 18 U.S.C. § 2511(d)(2).

en contra de *Google Inc.*, como proveedor de servicios telemáticos por el uso dado por éste a cierta información de los usuarios.<sup>21</sup> La parte apelante también señaló que el término “*facility*” conforme al caso *In Re Google Inc.*, es definido como “*where network service providers store private communications*” lo cual, según dicha parte, comprende lo que fue alegado por la Cooperativa.

Al examinar la sentencia recurrida, es de notar que el Tribunal de Primera Instancia utilizó el caso de *In Re Google Inc.* en su aplicación del derecho, con respecto a la definición del término “*facility*”<sup>22</sup>. La decisión de *In Re Google* del Tercer Circuito del 2015, hace un análisis del historial legislativo de la medida y de la jurisprudencia interpretativa del término “*facility*”, para concluir que dicha definición no incluye computadoras personales sino facilidades de almacenamiento. El TPI señaló además que la parte demandante en dicho caso no citó jurisprudencia apelativa que determinara que una computadora personal está protegida por el *Stored Communications Act*.<sup>23</sup>

Coincidimos con dicha apreciación por lo cual concluimos que el TPI aplicó la ley federal correctamente al concluir que el término “*facility*” no incluye computadoras personales. Ello significa que dichos dispositivos electrónicos no están protegidos por la ley federal.

En relación con la causa de acción bajo el *Computer Fraud and Abuse Act*, el TPI determinó que en el recurso presentado no hay suficientes hechos específicos que establezcan que Pérez Hernández accedió intencionalmente una computadora de La Cooperativa sin la autorización para ello y que, como resultado de esa conducta, causó daños temerariamente.

---

<sup>21</sup> Véase, págs. 4-5 del recurso.

<sup>22</sup> Véase, pág. 109 del anejo del recurso.

<sup>23</sup> Véase, *In Re Google Inc. Cookie Placement Consumer Privacy Litigation*, supra, (2015) a las págs. 14-15.

El TPI también señaló lo siguiente respecto al uso de los equipos por parte de Pérez Hernández:

Por un lado, la parte demandada-reconveniente alega en la reconvencción que la demandante accedió los mismos sin autorización durante el tiempo en que estuvo vigente el contrato en virtud del cual fungía como Administradora de La Cooperativa. Sin embargo, esa parte también alega que Pérez Hernandez realizaba sus funciones y deberes a través de los equipos de oficina y computación pertenecientes a La Cooperativa, a través de los sistemas y aplicativos de computación e informática pertenecientes a La Cooperativa, a través del alambrado de telecomunicaciones de La Cooperativa, a través de los dispositivos de telecomunicaciones de La Cooperativa, y a través de la suscripción de servicios en cuentas a nombre de La Cooperativa para fines de resguardo, telecomunicaciones, mensajería, y cualquier otro servicio o asunto telemático, informático y de computación.<sup>24</sup>

A raíz de dichas alegaciones concluyó el TPI que:

De lo anterior se desprende que, para ejercer sus funciones y deberes, la demandante debía utilizar dichos equipos, sistemas, aplicaciones, alambrados y dispositivos, por lo que se desprende igualmente que tenía autorización para ello.<sup>25</sup>

Al examinar el recurso de *Reconvencción* que tenía ante sí el TPI, coincidimos con la conclusión a la cual llegó dicho foro conforme las alegaciones de la parte apelante. El foro inferior actuó correctamente al determinar que no se cumple con los requisitos para una causa de acción bajo el *Computer Fraud and Abuse Act*.

Como ya hemos expuesto anteriormente, el *Stored Communications Act* protege aquella información almacenada en una facilidad de algún proveedor de servicios de comunicación electrónica. El TPI señaló que, en la reconvencción, no hay alegación alguna que establezca que Pérez Hernández accedió las facilidades de un proveedor de servicios de comunicación electrónica o que ella es un proveedor de servicios de comunicación que divulgó comunicaciones transmitidas o almacenadas en las facilidades.

<sup>24</sup> Véase, anejo del recurso a la pág. 121.

<sup>25</sup> *Id.*



Debido a ello, el TPI actuó correctamente al concluir que no se configuraron los elementos para una acción bajo el *Stored Communications Act* al no alegarse acceso a alguna facilidad de algún proveedor de comunicación electrónica. Luego de un examen de la Reconvención presentada ante dicho foro, coincidimos con que dicho documento no contiene alegaciones a tales efectos.

Finalmente, para que proceda una causa de acción al amparo del *Wiretap Act* se debe alegar que la parte demandada de manera intencional interceptó el contenido de una comunicación electrónica por medio de algún equipo y que dicha información fue divulgada o utilizada. **Según expusimos anteriormente, la jurisprudencia ha interpretado que cuando una persona tiene autorización para acceder a la comunicación o es parte de dicha comunicación protegida por la ley no viola el estatuto.** En el caso de autos, el TPI expresó que la parte apelante alega de manera conclusoria que la apelada interceptó comunicaciones electrónicas dirigidas a La Cooperativa. Dicho foro señaló que la Reconvención carece de hechos específicos sobre las circunstancias, frecuencia, lugar y tiempo en que la apelada interceptó las comunicaciones de La Cooperativa. El foro primario indicó que la Reconvención presentada no contiene hechos que apunten a que la apelada divulgó comunicaciones interceptadas o que ella no fuese parte en dichas comunicaciones.<sup>26</sup> Conforme los hechos del caso, Perez Hernández utilizaba el sistema de computación propiedad de La Cooperativa como parte de sus funciones de administración, por lo cual estaba autorizada para acceder a dichos equipos. En razón de ello, no se violó el *Wiretap Act*. Concluimos, pues, que el foro de instancia concluyó correctamente que una persona autorizada a acceder la

---

<sup>26</sup> Véase pág. 121 anejo del recurso.

comunicación electrónica o que es parte en la comunicación protegida no infringe el *Wiretap Act*.

IV

Por los fundamentos que anteceden, este tribunal *confirma* la determinación del TPI. Respecto a la solicitud de auxilio presentada en la nomenclatura del recurso de apelación, la declaramos sin lugar, sobre todo, tomando en consideración que la parte no detalló en qué consistía su reclamo urgente ni hizo súplica alguna al respecto.

Lo acordó y manda el Tribunal y lo certifica la Secretaria del Tribunal de Apelaciones.

Lcda. Lilia M. Oquendo Solís  
Secretaria del Tribunal de Apelaciones