Dolores E. FERNÁNDEZ MUÑOZ

Respecto de las relaciones colectivas de trabajo, se pronuncia por: *a*) suprimir el registro de las organizaciones sindicales y la "toma de nota" de sus mesas directivas; *b*) la creación de comités de empresas elegidos democráticamente, por un tiempo determinado; sugiere tomar en cuenta el modelo español; *c*) la celebración de los pactos normativos de condiciones de trabajo con obligatoriedad para trabajadores y patrones; *d*) prohibir absolutamente las cláusulas de exclusión, y otros aspectos de carácter procesal, que según el autor deberían ser reformadas oyendo a las partes involucradas en el proceso productivo.

En lo tocante a las perspectivas, el autor no presagia buenos augurios, después de un análisis a los principios que inspiraron al derecho del trabajo y sus fines. La crisis de la economía mundial y las posibles soluciones a la misma, han llevado al derecho del trabajo a un visible cambio de tendencias. Habrá más cambios, sin duda alguna. Y será necesario hacer del viejo derecho nuevo, como se le llamaba a principios de siglo, un derecho renovado.

3. *Razón de Estado y justicia social*

En este estudio el autor hace notar que entre la justicia social y el Estado se ha interpuesto un personaje tenebroso: la economía, que condiciona las conductas y rompe violentamente con el espíritu social. De Buen observa que el estado social de derecho vive una época precaria, por la "nueva razón de Estado", que conduce al país por la senda del neoliberalismo, las viejas estructuras del derecho social declinan, por la vía de la reforma o de la "razón de Estado", lo que no se puede —concluye el autor— es volver al reino del egoísmo, idea con la cual coincidimos.

En suma, esta obra y su interesante contenido son un valioso aporte a la bibliografía laboral mexicana —que mantiene su fuerza y vigor— por medio de los autores que, como De Buen, prefieren estar, más que a la moda, a la última verdad...

José Manuel LASTRA LASTRA

CAMACHO, Luis, *El delito informático*, Madrid, Gráficas Cóndor, 1987, 162 pp.

La primera advertencia que nos hace el autor es que no se trata de un libro jurídico, sino de uno más de los largos informes que como consultor

informático ha venido escribiendo por años, y la segunda es que cuando habla de delitos informáticos lo hace en el sentido de lo que a su juicio debe tipificarse, ya que en España sobre esta materia aún no se ha legislado. También cabe hacer notar que el libro no está específicamente dirigido a los juristas, sino más bien a los hombres de empresa que hasta ahora han dejado todo el aspecto de la seguridad informática en manos de los informáticos, a los que el autor acusa de estar más ocupados de su comodidad que de la eficacia del sistema, y que a menudo abusan de sus clientes y su desconocimiento de lo que es posible o no hacer. No por ello es menos valioso para los interesados en el tema, por uno u otro motivos.

El autor divide los delitos informáticos en tres grandes bloques:

1) Aquellos en los que el uso indebido o la manipulación fraudulenta de elementos informáticos de cualquier tipo (*hardware, software,* líneas de comunicaciones, información mecanizada, etcétera) posibilitan un beneficio ilícito. Es el denominado fraude informático.

2) Las acciones físicas que atentan contra la integridad de los elementos informáticos, como son los casos de vandalismo, terrorismo, etcétera, cuya finalidad primaria es causar un perjuicio, destruyendo información, paralizando actividades; aunque la mayor parte de las veces tiene motivaciones de venganza, también pueden ser actos originados por grupos terroristas o por delincuentes comunes como parte de actos de extorsión.

3) Los delitos relacionados con la propiedad intelectual de los elementos informáticos, especialmente del *software.* Es lo que se ha dado en llamar "la piratería del *software*".

Los delitos informáticos se caracterizan porque para su realización o encubrimiento deben estar necesariamente involucrados (medio) dispositivos informáticos, y que son circunstancias accidentales las que originan el descubrimiento de los hechos, sin que nunca se llegue a saber cuántas personas y en cuántas ocasiones pudieron hacer lo mismo. En estos momentos la posibilidad de que el autor de un delito informático resulte condenado es de una entre veintisiete mil, y ello es debido a que confluyen tres circunstancias claves: la casi total ausencia de medidas de seguridad en las instalaciones; la falta de una legislación adecuada y la gran inexperiencia existente para investigar los fraudes informáticos, y las escasas posibilidades de reunir pruebas que puedan inculpar a sus autores. El monto unitario promedio de este tipo de delitos es de 25 a 50 veces superior al conseguido en cualquier otro tipo de delito.

Las diversas áreas en que encontramos el fraude informático, a manera de ejemplo, son las siguientes: *a*) sustracción de dinero o documen-

tos que lo sustituyan; *b*) sustracción de mercancías manipulando los inventarios; *c*) sustracción de servicios (agua, electricidad, teléfono); *d*) sustracción de *software; e*) sustracción de información. Este último es uno de los delitos menos desarrollados, pero al que se le augura una mayor tasa de crecimiento, y al mismo tiempo uno de los que pueden alcanzar mayor potencial de perjuicios para las empresas afectadas.

A la piratería de *software* dedica un capítulo, donde indica que las causas que dan origen a esta conducta son, en primer lugar, las personas que lo desarrollan y que sintiéndolo una obra propia se adueñan de él. La segunda es que al sacar una copia del mismo no se deteriora el original, lo que da la apariencia de ser una acción inofensiva. El tercer factor es el precio desproporcionado que tienen los programas que se comercializan. "El hecho de que los usuarios potenciales consideren desproporcionado e injustificado dicho precio hace que de forma inmediata se justifique moralmente la realización de copias ilícitas, no para comercializar con ellas, sino para uso personal."

La informática también aparece relacionada con el terrorismo y el sabotaje. Aquél ha puesto sus ojos en la parte más vulnerable de las empresas: los centros de procesamiento de datos. Los saboteadores (que suelen ser empleados resentidos) pueden causar daños de enorme consideración, sólo por afán de venganza, en los elementos físicos necesarios para desarrollar la actividad informática o con acciones tendentes a destruir la información o los programas. Basta con interrumpir el suministro de energía eléctrica durante la ejecución de un proceso para que se puedan producir pérdidas de información, roturas de cintas magnéticas, y uno de los incidentes más perjudiciales que se dan en los discos magnéticos, lo que se denomina un aterrizaje de cabezas, que no sólo daña el disco magnético y hace que se pierda la información contenida en los sectores del disco afectados, sino que al dañarse la cabeza de lectura/escritura cada nuevo disco que se introduzca en esa unidad quedará a su vez dañado y la información que contenga se habrá perdido.

El autor narra también las pocas probabilidades de detectar a tiempo este tipo de delitos; lamenta la falta de preparación de los cuerpos de seguridad del Estado en la mayoría de los países, y las dificultades para hacer comprender al tribunal la naturaleza y el peso de las pruebas aportadas. Todo ello unido a la falta de legislación al respecto. En el último de los capítulos ofrece una serie de recomendaciones prácticas para evitar, en lo posible, ser víctimas de este tipo de "delitos".

Dolores E. FERNÁNDEZ MUÑOZ