NACIONES UNIDAS **A**

Asamblea General

Distr. GENERAL
A/CN.9/446
11 de febrero de 1998

ESPAÑOL
Original: INGLÉS

COMISIÓN DE LAS NACIONES UNIDAS PARA
EL DERECHO MERCANTIL INTERNACIONAL
31º período de sesiones
Nueva York, 1º a 12 de junio de 1998

INFORME DEL GRUPO DE TRABAJO SOBRE COMERCIO ELECTRÓNICO ACERCA DE LA LABOR DE SU 32º PERÍODO DE SESIONES
(Viena, 19 a 30 de enero de 1998)

ÍNDICE

V.98-50894

ÍNDICE (*continuación)*

INTRODUCCIÓN

1. En su 29º período de sesiones (1996), la Comisión decidió incluir en su programa las cuestiones de las firmas numéricas y las entidades certificadoras. Se pidió al Grupo de Trabajo sobre Comercio Electrónico que examinara la conveniencia y viabilidad de preparar un régimen uniforme sobre esos temas. Se convino en que la labor que había de llevar a cabo el Grupo de Trabajo en su 31º período de sesiones podía incluir la preparación de proyectos de disposición sobre ciertos aspectos de dichos temas. Se pidió al Grupo de Trabajo que proporcionara a la Comisión elementos suficientes para adoptar una decisión informada acerca del ámbito del régimen uniforme que había de elaborarse. Se convino además, como mandato más preciso para el Grupo de Trabajo, que el régimen uniforme que había de preparar se refirieran a cuestiones tales como: la base jurídica que sustentaba los procesos de certificación, incluida la tecnología incipiente de autenticación y certificación numéricas; la aplicabilidad del proceso de certificación; la asignación del riesgo y la responsabilidad de los usuarios, proveedores y terceros en el contexto del uso de técnicas de certificación; las cuestiones concretas de certificación mediante el uso de registros y la incorporación por remisión[1].

2. En su 30º período de sesiones (1997), la Comisión tuvo ante sí el informe del Grupo de Trabajo sobre Comercio Electrónico acerca de la labor de su 31º período de sesiones (A/CN.9/437). En cuanto a la conveniencia y la viabilidad de preparar un régimen uniforme sobre cuestiones relacionadas con las firmas numéricas y las entidades certificadoras, el Grupo de Trabajo señaló a la Comisión que había consenso entre sus miembros en cuanto a la importancia y la necesidad de lograr la armonización de la legislación en esa esfera. Si bien no había adoptado una decisión definitiva respecto de la forma y el contenido de esa labor, había llegado a la conclusión preliminar de que era viable emprender la preparación de un proyecto de régimen uniforme al menos sobre las cuestiones de las firmas numéricas y las entidades certificadoras, y posiblemente sobre cuestiones conexas. El Grupo de Trabajo recordó que, al margen de las cuestiones de las firmas numéricas y las entidades certificadoras, en el marco de la labor futura sobre el comercio electrónico también podría ser necesario abordar otras cuestiones como las alternativas técnicas de la criptografía de clave pública; las cuestiones generales relacionadas con las funciones de terceros que eran proveedores de servicios; y la contratación electrónica (A/CN.9/437, párrs. 156 y 157). En cuanto a la cuestión de la incorporación por remisión, el Grupo de Trabajo llegó a la conclusión de que no era necesario que la Secretaría realizara un nuevo estudio dado que las cuestiones fundamentales eran bien conocidas y quedaba claro que muchos aspectos de la cuestión de la batalla de los formularios y los contratos de adhesión tendrían que precisarse en el marco de la legislación nacional aplicable por razones relacionadas, entre otras cosas, con la protección del consumidor y otras consideraciones emanadas de la política oficial. El Grupo de Trabajo opinó que la cuestión debía examinarse como primer tema sustantivo de su programa al comienzo de su período de sesiones siguiente (A/CN.9/437, párr. 155).

3. La Comisión expresó su reconocimiento por la labor ya efectuada por el Grupo de Trabajo en su 31º período de sesiones, hizo suyas las conclusiones del Grupo de Trabajo y le encomendó la preparación de un régimen uniforme sobre las cuestiones jurídicas de la firma numérica y de las entidades certificadoras (a que de ahora en adelante nos referiremos como “Régimen Uniforme”).

4. Con respecto a la forma y al alcance exacto del Régimen Uniforme, la Comisión convino en general en que no era posible adoptar una decisión al respecto en una etapa tan temprana. Se opinó que, si bien el Grupo de Trabajo podría concentrar su atención en las cuestiones de la firma numérica, dada la función predominante que al parecer desempeñaba la criptografía de clave pública en la práctica más reciente en materia de comercio electrónico, el Régimen Uniforme debía atenerse al criterio de neutralidad respecto de los medios disponibles adoptado en la Ley Modelo de la CNUDMI sobre Comercio Electrónico (en adelante denominada “la Ley Modelo”). Por ello, el Régimen Uniforme no debía desalentar el recurso a otras técnicas de autenticación. Además, al ocuparse de la criptografía de clave pública, tal vez fuera preciso que el Régimen Uniforme acomodara diversos grados de seguridad y reconociera los distintos efectos jurídicos y grados de responsabilidad correspondientes a los diversos tipos de

servicios prestados en el contexto de las firmas numéricas. Respecto de las entidades certificadoras, si bien la Comisión reconoció el valor de las normas de fiabilidad o seguridad fijadas por el mercado, predominó el parecer de que sería apropiado que el Grupo de Trabajo considerase el establecimiento de un conjunto de normas mínimas que las entidades certificadoras habrían de respetar estrictamente, particularmente en casos en los que se solicitara una certificación de validez transfronteriza.

5. Como tema adicional que había de considerarse en el marco de la futura labor en materia de comercio electrónico, se sugirió que el Grupo de Trabajo tal vez necesitara examinar, en una etapa ulterior, las cuestiones de competencia jurisdiccional, ley aplicable y solución de controversias en el marco de la Internet[2].

6. El Grupo de Trabajo sobre Comercio Electrónico, integrado por todos los Estados Miembros de la Comisión, celebró su 32º período de sesiones en Viena del 19 al 30 de enero de 1998. Asistieron al período de sesiones representantes de los siguientes Estados miembros del Grupo de Trabajo: Alemania, Argelia, Australia, Austria, Brasil, Bulgaria, China, Egipto, Eslovaquia, España, Estados Unidos de América, Federación de Rusia, Finlandia, Francia, Hungría, India, Irán (República Islámica del), Italia, Japón, México, Nigeria, Polonia, Reino Unido de Gran Bretaña e Irlanda del Norte, Singapur, Sudán y Tailandia.

7. Asistieron al período de sesiones observadores de los siguientes Estados: Angola, Belarús, Bosnia y Herzegovina, Canadá, Colombia, Costa Rica, Dinamarca, Grecia, Guatemala, Indonesia, Iraq, Irlanda, Kuwait, Líbano, Malasia, Marruecos, Países Bajos, Pakistán, Paraguay, República Checa, República de Corea, Suecia, Suiza, Turquía y Ucrania.

8. Asistieron al período de sesiones observadores de las siguientes organizaciones internacionales: Centro de Comercio Internacional (UNCTAD/OMC), Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD), Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), Organización de las Naciones Unidas para el Desarrollo Industrial (ONUDI), Organización Mundial de la Propiedad Intelectual (OMPI), Comisión Europea, Organización de Cooperación y Desarrollo Económicos (OCDE), Organización Mundial del Comercio (OMC), Centro Regional de El Cairo de Arbitraje Comercial Internacional, Comité Marítimo Internacional (CMI), Asociación Internacional de Puertos (AIP), Asociación Internacional de Abogados, Cámara de Comercio Internacional (CCI), *Internet Law and Policy Forum (ILPF)* y Asociación Europea de Estudiantes de Derecho.

9. El Grupo de Trabajo eligió a los siguientes miembros de la Mesa:

Presidente: Sr. Mads Bryde ANDERSEN (Dinamarca);

Vicepresidente: Sr. PANG Khang Chau (Singapur);

Relator: Sr. Gritsana CHANGGOM (Tailandia).

10. El Grupo de Trabajo tuvo ante sí los siguientes documentos: programa provisional (A/CN.9/WG.IV/WP.72); una nota preparada por la Secretaría para el 31º período de sesiones del Grupo de Trabajo con el título: "Planificación de la labor futura sobre comercio electrónico: firmas digitales, autoridades certificadoras y asuntos jurídicos conexos" (A/CN.9/WG.IV/WP.71), en la que se resumen las deliberaciones previas del Grupo de Trabajo sobre la cuestión de la incorporación por remisión; una nota en la que figura el texto de un proyecto de disposición propuesto sobre incorporación por remisión y notas explicativas presentadas por el Reino Unido de Gran Bretaña e Irlanda del Norte (A/CN.9/WG.IV/WP.74); y una nota de la Secretaría que contiene el proyecto de régimen uniforme para las firmas numéricas, otras firmas electrónicas, autoridades certificadoras y cuestiones jurídicas conexas (A/CN.9/WG.IV/WP.73).

11. El Grupo de Trabajo aprobó el siguiente programa provisional:

1. Elección de la Mesa

2. Aprobación del programa

3. Aspectos jurídicos del comercio electrónico: la incorporación por remisión

4. Aspectos jurídicos del comercio electrónico: proyecto de régimen uniforme sobre firmas numéricas, otras firmas electrónicas, entidades certificadoras y cuestiones jurídicas conexas

5. Otros asuntos

6. Aprobación del informe

I. DELIBERACIONES Y DECISIONES

12. El Grupo de Trabajo debatió el tema de la incorporación por remisión tomando como base la nota preparada por la Secretaría (A/CN.9/WG.IV/WP.71) y la propuesta presentada por el Reino Unido de Gran Bretaña e Irlanda del Norte (A/CN.9/WG.IV/WP.74). Las deliberaciones y conclusiones del Grupo de Trabajo sobre este tema figuran en la sección II *infra*. Tras un debate, el Grupo de Trabajo aprobó el texto de un proyecto de artículo sobre incorporación por remisión. Se pidió a la Secretaría que preparase, tomando como base las deliberaciones y decisiones del Grupo de Trabajo, una breve guía para ayudar a los Estados a incorporar en su derecho interno y aplicar el proyecto de artículo. Se señaló que el proyecto de artículo, junto con la guía correspondiente para su incorporación al derecho interno, se presentarían a la Comisión en su 31º período de sesiones, que se celebraría en Nueva York del 1º al 12 de junio de 1998, para su examen final y su posible inclusión en la Ley Modelo y en su Guía para la incorporación al derecho interno.

13. El Grupo de Trabajo examinó también las cuestiones de las firmas numéricas, otras firmas electrónicas, las entidades certificadoras y cuestiones jurídicas conexas sobre la base de la nota preparada por la Secretaría (A/CN.9/WG.IV/WP.73). Las deliberaciones y conclusiones del Grupo de Trabajo en relación con esos temas figuran en la sección III *infra*. Se pidió a la Secretaría que preparase, basándose en dichas deliberaciones y conclusiones, un conjunto de disposiciones revisadas, con posibles variantes, para que el Grupo de Trabajo lo examinase en un futuro período de sesiones.

II. INCORPORACIÓN POR REMISIÓN

14. Habiendo recordado las deliberaciones celebradas previamente sobre la cuestión de la incorporación por remisión y los proyectos de texto propuestos en sus anteriores períodos de sesiones (A/CN.9/WG.IV/WP.71, párrs. 77 a 93), se invitó al Grupo de Trabajo a que examinara la cuestión de la incorporación por remisión en un contexto electrónico sobre la base de un proyecto de disposición propuesto (A/CN.9/WG.IV/WP.74, anexo), cuyo texto era el siguiente:

> "1) El presente artículo se aplicará cuando un mensaje de datos contenga una remisión o su significado sólo pueda determinarse plenamente mediante una remisión a información consignada en otra parte ("la información complementaria").

2) Con sujeción al párrafo 5), el mensaje de datos tendrá el mismo efecto que si la información complementaria se expresara íntegramente en el mensaje de datos, y toda remisión al mensaje de datos constituirá una remisión a dicho mensaje que incluirá la totalidad de la información complementaria, siempre y cuando se cumplan las condiciones estipuladas en el párrafo 3).

3) Las condiciones mencionadas en el párrafo 2) son que en el mensaje de datos:

a) Se identifique la información complementaria

i) mediante un nombre, descripción o código colectivo; y

ii) mediante una indicación precisa del registro y de las partes de ese registro que contienen la información complementaria y, cuando dicho registro no sea de dominio público, el lugar en que puede encontrarse y, si el modo de acceso no es obvio o está de alguna manera restringido, los medios por los cuales puede encontrarse; y

b) Se indique expresamente o se pueda deducir con claridad que el mensaje de datos tiene la finalidad de lograr el mismo efecto que si la información complementaria estuviera expresada íntegramente en el mensaje de datos.

4) La identificación a que se hace alusión en el inciso a) del párrafo 3) puede hacerse indirectamente mediante una remisión a información registrada en otra parte que contenga la identificación necesaria, siempre y cuando se cumplan las condiciones estipuladas en el párrafo 3) con respecto a dicha remisión.

5) Nada de lo expresado en el presente artículo menoscabará

a) Ninguna norma de derecho que requiera la debida notificación del contenido de la información complementaria, o del registro o lugar en que puede encontrarse dicha información, o los medios por los cuales ésta puede hallarse, o que exija que dicho lugar o registro sea accesible a otra persona;

b) Ninguna norma de derecho relativa a la validez de las condiciones para los fines de la formación del contrato, incluida la aceptación de una oferta;

c) Ninguna norma de derecho que disponga la incorporación efectiva de la información complementaria o la validez del proceso de incorporación."

15. Se observó que el proyecto de disposición se aplicaría cuando en un mensaje de datos se utilizara la incorporación por remisión (párr. 1); que el principio general consistía en que la información incorporada (que no se denominaba "términos o condiciones", dado que no toda la información creaba una obligación) había de tener el mismo efecto que si estuviese expresada íntegramente en un mensaje de datos (párr. 2); que las condiciones generales de la incorporación por remisión eran que se identificara en forma clara y precisa la información que había de incorporarse (lo que era especialmente importante para la protección del consumidor y de otros terceros), se identificara el lugar y la forma en que podía accederse a ella y se indicara la intención de incorporar dicha información (párr. 3); que la identificación indirecta de la fuente de información mediante una remisión a otra fuente debía ser aceptable con sujeción a las mismas condiciones (párr. 4); y que toda norma de derecho existente que se aplicara a la incorporación por remisión en las comunicaciones convencionales debía hacerse extensiva a las comunicaciones electrónicas (párr. 5).

16. Se convino en general en la necesidad de abordar la cuestión, dado que la incorporación por remisión era inherente a la utilización de las comunicaciones electrónicas. Se afirmó que en las comunicaciones electrónicas se incorporaba necesariamente por remisión un gran número de datos (por ejemplo, registros de comunicaciones, declaraciones de política, firmas numéricas en certificados). Además, se observó que la incorporación por remisión en un contexto electrónico podía realizarse satisfactoriamente mediante diversos métodos que, sin ser los únicos, incluían los localizadores de recursos uniformes, los identificadores de objetos u otros registros razonablemente disponibles en una determinada dirección.

17. Si bien se admitió que la incorporación por remisión presentaba ciertos riesgos, por ejemplo, para los consumidores, se adujo que al mismo tiempo esa práctica permitía a los consumidores aprovechar las oportunidades que se ofrecían únicamente por conducto de las redes de comunicación electrónicas. Se señaló que una disposición sobre incorporación por remisión debía tener como principal finalidad establecer un equilibrio entre las partes interesadas. Con miras a lograr ese objetivo, se invitó al Grupo de Trabajo a que examinara, paralelamente al proyecto de disposición antes citado, un proyecto de texto en los términos siguientes:

> "Variante A De no convenirse otra cosa entre las partes, se considerará que una información forma parte de un mensaje de datos si ello se indica expresamente o puede deducirse claramente [y si en ese mensaje de datos se indica un procedimiento mediante el cual puede accederse a esa información de manera razonable y oportuna]. Dicha información será efectiva en la medida en que lo permita la ley.
>
> Variante B No se negarán efectos jurídicos a la información por la sola razón de que se haya incorporado por remisión en un mensaje de datos."

18. Con respecto a la variante A, se observó que los factores materiales que determinaban si un término era o no razonablemente accesible incluían los siguientes: disponibilidad (horas de funcionamiento de la fuente de información, facilidad de acceso y niveles aceptables de redundancia); costo del acceso (excluidos los costos implícitos por concepto de servicios de comunicaciones; si los hubiere, los costos debían ser razonables y estar en proporción con el valor asociado con el contrato); formato (ampliamente utilizado en la comunidad interesada); integridad (verificación del contenido, autenticación del remitente, y mecanismo para corregir los errores de comunicación); y grado en que el término estaba sujeto a ulterior modificación (sin el derecho contractual de hacerlo; notificación de actualizaciones; notificación de la política de modificación). Se añadió que esos factores podían consignarse en una guía para incorporar las disposiciones sobre incorporación por remisión en el derecho interno (véanse los párrafos. 23 y 24 *infra*).

19. El Grupo de Trabajo continuó sus deliberaciones sobre la base de los citados proyectos de disposición propuestos como alternativas. Se observó que los proyectos de disposición tenían varias ventajas en común. Una de ellas consistía en que su propósito era facilitar la incorporación por remisión en un contexto electrónico eliminando la incertidumbre que imperaba en muchas jurisdicciones en cuanto a si las disposiciones relativas a la incorporación por remisión tradicional se aplicaban a la incorporación por remisión en un entorno electrónico. A ese respecto, se sugirió que se adoptara un criterio diferente, a saber que se desalentara la utilización generalizada de la incorporación por remisión en un entorno electrónico a fin de reducir el riesgo de duplicar la difícil situación conocida como la "batalla de los formularios" en el comercio tradicional basado en la documentación consignada sobre papel. En apoyo de esa sugerencia, se observó que, mientras que en el contexto de la documentación escrita la incorporación por remisión era necesaria por razones de tiempo, espacio y costo, en un contexto electrónico podía consignarse gran cantidad de información en un mensaje de datos de manera sencilla, rápida y poco costosa. Se rebatió esa sugerencia aduciendo que no sería apropiado que un régimen uniforme desempeñara el papel de código de conducta, con la consecuencia de desalentar el recurso a una práctica importante y ampliamente empleada, cuya utilización era inherente a las comunicaciones electrónicas.

20. Se dijo que otra ventaja de los proyectos de texto mencionados era que reconocían que no debía obstruirse la legislación relativa a la protección del consumidor u otras normas del derecho nacional o internacional de carácter obligatorio (por ejemplo, las normas destinadas a proteger a las partes más débiles en el contexto de los contratos de adhesión). Se señaló que el primer texto propuesto perseguía ese resultado enumerando las normas de derecho que no habrán de resultar menoscabadas (párr. 5)) y que el segundo proyecto de texto conseguía ese mismo resultado, pues estipulaba que la información sería efectiva en la medida en que lo permitiera la ley (variante A), o no impedía que se negasen efectos jurídicos a la información por la sola razón de que se hubiese incorporado por remisión (variante B). Con miras a aclarar inequívocamente que la legislación existente no resultaba menoscabada por ninguna de las formulaciones propuestas, se sugirió que toda disposición sobre incorporación por remisión se redactase en términos similares a los de la segunda nota del artículo 1 de la Ley Modelo, que afirmaba expresamente el principio de que la Ley Modelo no se proponía derogar las normas jurídicas destinadas a la protección del consumidor.

21. No obstante, se expresó la opinión de que el primer texto propuesto y la variante A del segundo texto propuesto presentaban varias desventajas. Una de ellas era que se corría el riesgo de trastornar prácticas bastante arraigadas o de reciente adopción al establecer una norma demasiado estricta. Se afirmó que en muchos casos prácticos sería imposible satisfacer los requisitos que exigían una indicación expresa o una posibilidad de deducción clara de la intención de que la información fuera incorporada por remisión o de que esa información fuera razonablemente accesible. Se citó el ejemplo de la incorporación por remisión de un contrato de fletamento principal en un conocimiento de embarque entregado con arreglo a un subcontrato de fletamento, práctica que, se adujo, se vería menoscabada por el requisito de indicación expresa o de posibilidad de deducción clara de la intención de que la información fuera incorporada por remisión o de que fuera razonablemente accesible. Otra desventaja era que tales disposiciones podrían obstruir involuntariamente la aplicación de normas jurídicas de carácter obligatorio y tener consecuencias injustas. A ese respecto, se señaló que además de las dos condiciones estipuladas en el primer proyecto de texto y en la variante A del segundo, debía incluirse un tercer elemento, a saber, que la incorporación por remisión debía estar sujeta a la aceptación por las partes. Se dijo en particular que en el contexto del intercambio electrónico de datos abierto la aceptación por las partes era fundamental.

22. En respuesta a ello, se observó que el párrafo 5) del primer proyecto de texto y la segunda oración de la variante A del segundo tenían por objeto abordar precisamente esas preocupaciones y velar por que la disposición sobre incorporación por remisión no obstruyese las prácticas establecidas o las normas obligatorias del derecho interno. Sin embargo, se estimó que esas disposiciones podrían suscitar problemas de interpretación. Se observó que la variante B no presentaba esa desventaja, dado que simplemente expresaba el principio general de no discriminación consagrado en el artículo 5 de la Ley Modelo. Se reconoció en general que la variante B implicaba que la incorporación por remisión sólo sería eficaz en la medida en que lo permitiera la ley. Sobre esa base, el Grupo de Trabajo convino en general en que la variante B era preferible.

23. Como cuestión de redacción, se sugirió que la variante B debía reflejar la terminología empleada en el artículo 5 de la Ley Modelo y referirse, por tanto, no sólo a los efectos jurídicos, sino también a la validez y la fuerza obligatoria. Con respecto a la ubicación de la disposición sobre incorporación por remisión, se sugirió que como la cuestión se relacionaba con el comercio electrónico en general y no sólo con las firmas numéricas, debía insertarse en la Ley Modelo como artículo 5 *bis*. A fin de ayudar a los usuarios de la Ley Modelo y a los legisladores a interpretar la disposición sobre incorporación por remisión, se sugirió asimismo que en la Guía para la incorporación de la Ley Modelo al derecho interno se incluyeran los antecedentes y explicaciones pertinentes con respecto a la disposición sobre incorporación por remisión. Se sugirió que en la Guía se indicasen los factores en que podían basarse los Estados para adoptar una versión ampliada de la disposición sobre incorporación por remisión. Esos factores podían derivarse del texto del primer proyecto de disposición propuesto y de la variante A del segundo. Esta sugerencia se consideró generalmente aceptable. Sin embargo, se hizo la advertencia de que ese criterio podría ser incoherente con el criterio adoptado en el artículo 5 de la Ley Modelo. Se expresó la opinión de que los mencionados

factores no debían figurar como alternativas a las disposiciones de la Ley Modelo. En general, se opinó que al redactar la parte de la Guía para incorporación de la Ley Modelo al derecho interno relativa a la incorporación por remisión debía velarse por evitar toda sugerencia involuntaria en el sentido de que se introdujeran restricciones a la incorporación por remisión con respecto al comercio electrónico además de las que ya pudiesen estar en vigor respecto del comercio basado en la documentación escrita.

24. Tras un debate, el Grupo de Trabajo aprobó la variante B, decidió presentarla a la Comisión para su examen y su posible inserción como artículo 5 *bis* de la Ley Modelo y pidió a la Secretaría que preparara una nota explicativa a fin de añadirla a la Guía para la incorporación de la Ley Modelo al derecho interno.

III. EXAMEN DEL PROYECTO DE RÉGIMEN UNIFORME PARA LAS FIRMAS ELECTRÓNICAS

CAPÍTULO I. ÁMBITO DE APLICACIÓN Y DISPOSICIONES GENERALES

25. Hubo acuerdo general en el Grupo de Trabajo en que más adelante sería preciso establecer la relación entre el Régimen Uniforme y la Ley Modelo (en particular, la cuestión de si el Régimen Uniforme para las firmas numéricas debía constituir un instrumento jurídico independiente o si se debía incorporar a una versión ampliada de la Ley Modelo). Si bien se convino en que no se podía tomar una decisión en ese momento, el Grupo de Trabajo confirmó su hipótesis de trabajo de que el Régimen Uniforme debería tener las siguientes características: se debía preparar como un proyecto de disposición legislativa; debía ser compatible con las disposiciones de la Ley Modelo en general; y de alguna forma debía incorporar disposiciones con arreglo al tenor del artículo 1 (Ámbito de aplicación), incisos a), c) y e) del artículo 2 (Definiciones de “mensaje de datos”, “iniciador” y “destinatario”), artículo 3 (Interpretación) y artículo 7 (Firma) de la Ley Modelo.

26. Por lo que se refiere a la esfera de aplicación del Régimen Uniforme, se expresó la opinión de que debía limitarse a las firmas numéricas, con exclusión de otras técnicas de autenticación. En respuesta a ello, se recordó que, al formular su conclusión preliminar de que era viable emprender la preparación de un proyecto de normas uniformes sobre cuestiones relacionadas con firmas numéricas, el Grupo de Trabajo, en su anterior período de sesiones, había convenido también en que, al margen de las cuestiones de las firmas numéricas y las entidades certificadoras, también podría ser necesario que se examinaran las cuestiones de las alternativas técnicas a la criptografía de clave pública en el ámbito del comercio electrónico (A/CN.9/437, párrs. 156 y 157). Se recordó también que, en el 30º período de sesiones de la Comisión, se opinó que, si bien tal vez procedería que el Grupo de Trabajo concentrara su atención en las cuestiones de las firmas numéricas habida cuenta del papel aparentemente predominante desempeñado por la criptografía de clave pública en la práctica emergente del comercio electrónico, el Régimen Uniforme debía ser compatible con el enfoque de neutralidad en cuanto a los medios adoptados en la Ley Modelo de la CNUDMI sobre Comercio Electrónico (véase *infra*, párr. ...). Tras un debate, el Grupo de Trabajo confirmó su decisión de que, además de concentrarse en la preparación de disposiciones específicas relativas a las técnicas de firma numérica, debía también extraer de esas disposiciones específicas normas de aplicación más general para dar cabida a otras técnicas de autenticación.

CAPÍTULO II. FIRMAS ELECTRÓNICAS

Sección I. **Firmas electrónicas seguras**

Artículo 1. **Definiciones**

27. El texto del proyecto de artículo 1 examinado por el Grupo de Trabajo era el siguiente:

"Para los fines del presente Régimen:

"a) por "firma" se entenderá cualquier símbolo utilizado, o cualquier procedimiento de seguridad adoptado, por una persona [o en su nombre] con la intención de identificar a esa persona e indicar que esa persona aprueba la información a la que esa firma está adherida;

b) por "firma electrónica" se entenderá [la firma] [los datos] en forma electrónica contenida (contenidos) en un mensaje de datos o adjunta (adjuntos) a él o lógicamente vinculada (vinculados) con él [y utilizada (utilizados) por una persona o [en su nombre] con la intención de identificar a esa persona e indicar su aprobación del contenido de ese mensaje de datos] [y utilizada (utilizados) para satisfacer las condiciones del [artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico]];

c) por "firma electrónica segura" se entenderá un firma electrónica que

i) sea una firma numérica conforme al artículo 4 y satisfaga los requisitos contenidos en el artículo 5; o

ii) desde el momento en que se consignó, pueda verificarse como la firma de una persona determinada mediante la aplicación de un procedimiento de seguridad que esté exclusivamente vinculado con la persona que la utiliza; sea capaz de identificar pronta, objetiva y automáticamente a esa persona; haya sido creada de manera o con unos medios bajos control exclusivo de la persona que la utilice; y esté vinculada con el mensaje de datos a que se refiera de modo que, si el mensaje es alterado, queda invalidada la firma electrónica; o

iii) sea comercialmente razonable, en las circunstancias previamente acordadas, y debidamente aplicadas, por las partes [entre las partes que participen en la generación, el envío, la recepción, el archivo u otra elaboración de mensajes de datos en el curso ordinario de sus actividades]."

Observación general

28. Se señaló que las disposiciones que figuraban en el proyecto de artículo 1 estaban concebidas no sólo como definiciones sino también como medio de delinear el alcance del Régimen Uniforme. Si bien se hizo notar que se había utilizado la misma técnica de redacción en el contexto de la Ley Modelo, muchos participantes opinaron que el Grupo de Trabajo tal vez tuviera que volver a examinar el proyecto de artículo 1 durante sus deliberaciones acerca del alcance del Régimen Uniforme.

Inciso a)

29. Muchos participantes opinaron que debía suprimirse el inciso a). Por más que la inclusión en el Régimen Uniforme de una definición de "firma" basada en el artículo 7 de la Ley Modelo tal vez brindara buena orientación en aquellos países en los que actualmente no existía una definición de "firma" se declaró que no era necesaria una definición de esa índole para los fines del Régimen Uniforme. Uno de los argumentos aducidos en pro de la supresión del inciso era que la inclusión en el texto de una definición de alcance general tal vez pondría en peligro la aceptabilidad del instrumento en aquellos países en que la disposición contenida en el inciso a) podría entrar en conflicto con las definiciones existentes.

Inciso b)

30. Muchos participantes opinaron que la redacción del inciso b) debería reflejar el texto del artículo 7 de la Ley Modelo. Ello podría lograrse ya fuere reproduciendo ese artículo en su totalidad en el inciso b) o mediante una referencia a "las condiciones enunciadas en el artículo 7 de la Ley Modelo". Tras un debate, el Grupo de Trabajo concluyó que esta última formulación era preferible. Como cuestión de redacción, hubo acuerdo general en que se utilizara la expresión "los datos" en lugar de la expresión "la firma".

Inciso c): observaciones generales

31. Se expresó la opinión de que tal vez fuera improcedente definir una firma electrónica con el calificativo de "segura". El hecho de que una técnica determinada fuera "segura" no era cuestión de definición sino cuestión de hecho que habría de ser determinada en relación con las circunstancias en las que se utilizara esa técnica. También se criticó la utilización de la palabra "segura" alegando que introducía un criterio subjetivo y que daba a entender que las firmas que no pertenecían a esa categoría eran inherentemente inseguras. Se declaró en respuesta que, si bien tal vez habría que sustituir la referencia a una firma "segura" por una mejor expresión, se utilizaba en el Régimen Uniforme únicamente como medio de delimitar una categoría de firmas electrónicas de una calidad tal que se les podría adscribir efectos jurídicos específicos. Respecto de si el empleo de la palabra "segura" podría establecer un criterio subjetivo, se declaró que las técnicas de autenticación no se desarrollaban en un vacío. Se dispondría de normas aplicadas ya sea por reglamentación o por prácticas voluntarias basadas en la industria para evaluar el grado de seguridad de cualquier técnica dada. Tras un debate, el Grupo de Trabajo decidió proseguir suponiendo que se utilizaría una categoría (provisionalmente denominada "segura") para abordar la gama de técnicas a las que el Régimen Uniforme adscribiría ciertos efectos jurídicos.

32. Se expresó la opinión de que tal vez fuera improcedente disponer que se adscribiría el mismo efecto jurídico a la utilización de una amplia variedad de técnicas de autenticación, que, según se afirmó, iban desde las inherentemente seguras (p.ej.: las firmas numéricas) a las inherentemente inseguras (p.ej.: determinadas técnicas de autenticación en la que puedan convenir las partes). En respuesta, se declaró que el inciso c) estaba encaminado precisamente a crear una categoría en la que las firmas más seguras de las firmas numéricas se podrían poner en pié de igualdad con otras técnicas, siempre que esas técnicas cumplieran el estricto criterio enunciado en el apartado ii) del inciso c). Por lo que se refiere al apartado iii) del inciso c), tal vez podría estudiarse la posibilidad de colocarlo en una disposición aparte que se ocupara de la autonomía de las partes. Se convino en que tal vez fuera necesario reanudar el debate sobre las definiciones una vez que se hubieran examinado las disposiciones relativas a los efectos jurídicos de esas definiciones.

Apartado i) del inciso c)

33. El contenido del apartado i) del inciso c) se consideró generalmente aceptable. No obstante, se expresó la opinión de que los requisitos del proyecto de artículo 5, mencionados en el apartado i) del inciso c), no garantizaban que las firmas numéricas fueran firmas electrónicas seguras. Se sugirió que esta cuestión volviera a tratarse en el contexto del proyecto de artículo 5.

Apartado ii) del inciso c)

34. Se expresó la inquietud de que la carga de la prueba en virtud de lo dispuesto en el apartado ii) del inciso c) era tan alta que las resoluciones que figuraban en el párrafo 1) del proyecto de artículo 2 tendrían escaso sentido en el caso en que se utilizaran firmas electrónicas no numéricas. En respuesta, se declaró que el apartado ii) del inciso c) y el proyecto de artículo 2 estaban concebidos para servir finalidades distintas. Hubo acuerdo general, no obstante,

en que tal vez se tendrían que esclarecer las relaciones entre el apartado ii) del inciso c) y el proyecto de artículo 2 en el proyecto revisado de Régimen Uniforme que había de preparar la Secretaría.

35. Muchos participantes opinaron que la sustancia del apartado ii) del inciso c) era importante para garantizar la neutralidad de la Ley Modelo en cuanto a los medios. Se expresó la opinión de que, puesto que la finalidad del apartado ii) del inciso c) era definir ciertos criterios que una determinada técnica debía cumplir para dar validez a las presunciones enunciadas en el proyecto de artículo 2, no hacía al caso el que la técnica se utilizara o no con la intención de firmar. Por lo tanto, se sugirió que se suprimieran las palabras “pueda verificarse como la firma de una persona determinada”.

36. Se hicieron otras sugerencias acerca de la formulación específica del apartado ii) del inciso c). Se sugirió que se suprimieran las palabras “pronta(mente)” y “automáticamente”. Se afirmó que la identificación “pronta” y “automática” de una persona no era inherente al uso de la mayoría de las técnicas de autenticación (incluidas determinadas técnicas de firma numérica) y no estaba claramente relacionada con la seguridad del procedimiento de autenticación y la integridad de los datos que se firmaban electrónicamente. También se sugirió que las palabras “de un procedimiento de seguridad” se complementaran con las palabras “o una combinación de procedimientos de seguridad”. Tras un debate, el Grupo de Trabajo adoptó esas sugerencias.

Apartado iii) del inciso b)

37. Se sugirió que se suprimiera el apartado iii). Se declaró que otorgar la condición de “firma electrónica segura” a cualquier procedimiento en el que las partes puedan convenir crearía el riesgo de que se pudiera utilizar cualquier procedimiento de bajo nivel de seguridad para surtir efectos jurídicos. A ese respecto, se expresó la opinión de que, en la actualidad, la única técnica de autenticación “segura” era la de la firma numérica. En respuesta, se observó que, como cuestión de libertad de contrato, las partes deberían ser libres de convenir en que, entre ellas, se fiarían de una técnica de autenticación que fuera menos segura que el tipo de firma electrónica descrito en el apartado ii) del inciso c), y que adscribirían las presunciones contenidas en el proyecto de artículo 2 a la utilización de esa técnica de autenticación. También se observó que la referencia al carácter “comercialmente razonable” de la técnica de firma tenía la finalidad de salvaguardar contra el reconocimiento ilimitado de técnicas de autenticación posiblemente inseguras a través de la autonomía de las partes. Se hizo una advertencia, no obstante, acerca del riesgo de depender de la idea de la “razonabilidad comercial” para aportar esa salvaguarda. En cierto número de países, el mero hecho de que unas partes “comerciales” hubieran convenido en un procedimiento bastaría para interpretar ese procedimiento como “comercialmente razonable”. Como cuestión de redacción, se planteó una cuestión acerca de la posible incompatibilidad entre el uso de las palabras “comercialmente razonable” y la redacción utilizada en el artículo 7 de la Ley Modelo. Si bien se recordó que las palabras “comercialmente razonable” se habían utilizado en el artículo 5 de la Ley Modelo de la CNUDMI sobre transferencias internacionales de crédito, el Grupo de Trabajo opinó que tal vez fuera necesario una nueva redacción idónea para evitar esa interpretación. Se sugirió que tal vez fuera necesario incluir en el apartado iii) del inciso c) una referencia a una estipulación expresa de las partes en el sentido de que la técnica convenida surtiría los efectos de una firma electrónica segura en virtud de lo dispuesto en el proyecto de artículo 2. También se sugirió que se mantuvieran las palabras “entre las partes” sin corchetes en el apartado iii) del inciso c).

38. Se trató la cuestión de si el apartado iii) del inciso c) podría ser utilizado por las partes para sustraerse a una normativa legal obligatoria relativa a la forma de ciertos actos legales. Se declaró que esa interpretación sería aceptable habida cuenta de que esa libertad de contrato no existía en un entorno basado en el papel. Si bien hubo acuerdo general en que, en virtud de la legislación de cierto número de países, el acuerdo privado no podía sustraerse de determinados requisitos de forma obligatorios, estos requisitos de forma obligatorios se aplicaban típicamente a una categoría muy estrecha de operaciones, de las que probablemente se podría dar cuenta mediante una exclusión expresa del alcance de una disposición general relativa a la autonomía de las partes.

39. El debate se centró en la forma en que el Régimen Uniforme abordaría la autonomía de las partes. Se recordó que la mera referencia al artículo 4 (Modificación mediante acuerdo) de la Ley Modelo tal vez no bastara para aportar una solución satisfactoria, habida cuenta de que el artículo 4 establecía una diferencia entre las disposiciones de la Ley Modelo que podían modificarse libremente por contrato y las disposiciones que debían considerarse obligatorias salvo que la modificación mediante acuerdo estuviera autorizada por la ley aplicable fuera del marco de la Ley Modelo. Con respecto a las firmas electrónicas, la importancia práctica de redes "cerradas" obligaba a otorgar un amplio reconocimiento a la autonomía de las partes. No obstante, tal vez también haya que tener en cuenta las restricciones de política pública de la libertad de contrato, comprendidas las leyes que protegen al consumidor contra contratos de adhesión demasiado amplios. Se sugirió que el Régimen Uniforme incluyera una disposición con arreglo al tenor del párrafo 1) del artículo 4 de la Ley Modelo a los efectos de que, salvo que el Régimen Uniforme u otra legislación aplicable lo dispusiera, las firmas electrónicas y los certificados emitidos, recibidos o hechos valer de conformidad con procedimientos convenidos entre las partes en una operación tendrían el efecto especificado en el acuerdo. Además, se sugirió que el Grupo de Trabajo examinase tal vez la posibilidad de establecer una regla de interpretación en el sentido de que, al determinar si un certificado, una firma electrónica o un mensaje de datos verificado por remisión a un certificado, era suficientemente fiable para una finalidad concreta, se tuvieran en cuenta todos los acuerdos pertinentes en que participaran las partes, toda línea de conducta entre ellas y todo uso comercial pertinente.

40. Como opción alternativa, se invitó al Grupo de Trabajo a que examinase el siguiente texto de un nuevo artículo propuesto:

> "1) Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho mediante una firma electrónica:
>
> a) Si las partes en la transacción convinieron en el uso de la firma electrónica, o
>
> b) Si la firma electrónica era tan fiable como procedente para la finalidad para la que se utilizaba la firma electrónica.
>
> 2) Al determinar si una firma electrónica es debidamente fiable para una finalidad concreta, se tendrán en cuenta toda línea de conducta entre las partes y todo uso comercial pertinente."

41. El debate continuó sobre la base del nuevo artículo propuesto. Se declaró que en el texto propuesto se proponía aprovechar y ampliar el enfoque adoptado en el artículo 7 de la Ley Modelo. En particular se declaró que: el inciso a) del párrafo 1 tenía la finalidad de permitir que las partes determinaran el tipo de firma electrónica que desearan usar en sus transacciones comerciales; el inciso a) del párrafo 1) se había inspirado en el inciso b) del párrafo 1) del artículo 7 de la Ley Modelo; y el párrafo 2) constituía un esfuerzo por explicar el inciso b) del párrafo 1). Se expresó la opinión de que, si se llegara a incluir el nuevo artículo en el Régimen Uniforme, el párrafo 2) del proyecto de artículo 2 del Régimen Uniforme no sería necesario y se podría suprimir.

42. Hubo objeciones generalizadas a la propuesta basándose en que era contraria al artículo 7 de la Ley Modelo en diversas maneras, comprendidas las siguientes: que no incluía los elementos de identificación y de aprobación, llamando de ese modo firma a algo que, a la luz de la Ley Modelo, no era una firma; que permitía que las partes se apartaran de las normas de ley obligatorias relativas a las firmas, invalidando de ese modo normas que, en virtud del párrafo 2) del artículo 7 de la Ley Modelo, podían establecer la obligación de una firma, o consecuencias jurídicas en caso de que no existiera una firma; y que no incluía una disposición del estilo del párrafo 3 del artículo 7 de la Ley Modelo, que permitía a los Estados excluir la aplicación del artículo 7 en determinados casos (por ejemplo, títulos negociables).

43. Muchos participantes opinaron que la principal desventaja del nuevo artículo propuesto radicaba en que, a diferencia del artículo 7 de la Ley Modelo y en contra las normas aplicables en un entorno basado en el papel, permitía que las partes se apartaran de normas de ley obligatorias. Así pues, el nuevo artículo 2 propuesto podía surtir inadvertidamente el efecto de socavar la Ley Modelo y la legislación nacional relativa a las firmas y afectar improcedentemente a los derechos de terceros. Además, se expresó amplio apoyo a la opinión de que el propuesto nuevo artículo repetía innecesariamente elementos ya enunciados en el proyecto de artículo 1 del Régimen Uniforme.

44. Con objeto de armonizar el nuevo artículo propuesto con el artículo 7 de la Ley Modelo y abordar las deficiencias antes citadas, se formuló una serie de sugerencias. Una de ellas consistía en incluir una referencia a las características esenciales de una firma, a saber, las relativas a la identificación de una persona y la aprobación y el contenido de un mensaje, insertando para ello al final del encabezamiento del párrafo 1) del nuevo artículo propuesto un texto que rezara con arreglo al siguiente tenor: "es la firma de esa persona y". También se sugirió que se diera precedencia a la ley aplicable introduciendo para ello al principio del inciso a) del párrafo 1) un texto que dijera lo siguiente: "Con sujeción a la ley pertinente". Otra sugerencia consistía en que, de conformidad con el artículo 7 de la Ley Modelo, la conjunción entre los incisos a) y b) debía ser "y", y no "o". Se sugirió asimismo que se debería permitir tener en cuenta la conducta de las partes y los usos comerciales pertinentes a que se hacía referencia en el párrafo 2) del nuevo artículo, en lugar de imponerlo, lo que podía conseguirse sustituyendo la palabra "tendrán" por la expresión "podrán tener". Se sugirió además que debían introducirse en el nuevo artículo propuesto los elementos esenciales de los párrafos 2) y 3) del artículo 7 de la Ley Modelo.

45. Muchos participantes opinaron que, en lugar de redactar nuevamente el nuevo artículo propuesto, el Grupo de Trabajo debería tratar de establecer principios básicos relativos a la medida en que el Régimen Uniforme debería dar cabida a la autonomía de las partes. Hubo acuerdo general en que el Régimen Uniforme no debería limitar normalmente la autonomía de las partes entre las propias partes. También se convino en que los esfuerzos del Grupo de Trabajo deberían encaminarse a concretar los tipos de operaciones (y, en el caso de las firmas numéricas, los tipos de certificados) que supondrían un alto nivel de seguridad y podrían por ello estar sujetos a normas obligatorias en virtud de la legislación vigente en cierto número de países. Respecto de los requisitos legales de forma que podrían interferir con la autonomía de las partes, muchos participantes opinaron que podría establecerse una distinción entre los requisitos de firma que tenían por objeto facilitar pruebas (que podrían supeditarse a la autonomía de las partes), y los requisitos de forma que se prescribieran a efectos de validez (que típicamente serían obligatorios).

46. Después de un debate, el Grupo de Trabajo pidió a la Secretaría que preparase un proyecto revisado del artículo 1 en el que se recogieran las deliberaciones y decisiones arriba citadas.

Artículo 2. **Presunciones**

47. El texto de proyecto de artículo 2 que examinó el Grupo de Trabajo era el siguiente:

> "1) Con respecto a los mensajes de datos autenticados mediante una firma electrónica segura, se presumirá, salvo prueba en contrario, que:
>
> a) el mensaje de datos no ha sido modificado desde el momento en que se consignó en él la firma electrónica segura;
>
> b) la firma electrónica segura es la firma de la persona a quien se refiere; y
>
> c) la firma electrónica segura fue consignada por esa persona con la intención de firmar el mensaje.

2) Con respecto a los mensajes de datos autenticados mediante una firma electrónica que no sea una firma electrónica segura, nada de lo dispuesto en el presente Régimen afectará las reglas sustantivas o probatorias acerca de la carga de la prueba de la autenticidad y la integridad de un mensaje de datos o una firma electrónica.

3) Lo dispuesto en el presente artículo no será aplicable a: [...]

[4) Las presunciones del párrafo 1) podrán ser destruidas mediante:

a) pruebas que indiquen que un procedimiento de seguridad empleado para verificar una firma electrónica no es generalmente reconocido como fiable, debido a los adelantos en la tecnología, la manera como el procedimiento se hizo funcionar o por otras razones;

b) pruebas que indiquen que el procedimiento de seguridad convenido entre las partes conforme al apartado iii) del inciso c) del artículo 1 no se hizo funcionar de manera fidedigna; o

c) pruebas relativas a hechos de que la parte que aceptó la firma era consciente que sugerirían que la confianza en el procedimiento de seguridad no era razonable. La razonabilidad comercial de un procedimiento de seguridad convenido por las partes conforme al apartado iii) del inciso c) del artículo 1 se determinará a la luz de las finalidades del procedimiento y las circunstancias comerciales en el momento en que las partes convinieron en adoptar el procedimiento, inclusive en la naturaleza de la operación, el grado de avance tecnológico de las partes, el volumen de operaciones análogas en que ha intervenido una de las partes o ambas, la existencia de otras posibles soluciones ofrecidas a la parte pero rechazadas por ella, el costo de otros procedimientos posibles y los procedimientos de uso general para tipos de transacción análogos.]"

48. Si bien hubo acuerdo en que el principio de la neutralidad en cuanto a los medios debería quedar reflejado en el Régimen Uniforme con el reconocimiento de los efectos jurídicos que surtiría el uso de firmas electrónicas basadas en técnicas no numéricas, el Grupo de Trabajo decidió aplazar su examen del proyecto de artículo 2 hasta que hubiera terminado su examen de los restantes proyectos de artículos del Régimen Uniforme.

Artículo 3. **Atribución**

49. El texto del proyecto de artículo 3 que examinó el Grupo de Trabajo era el siguiente:

"1) **Variante A** Sin perjuicio de lo dispuesto en [el artículo 13 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico], el iniciador de un mensaje de datos en el que se ha consignado su firma electrónica segura [estará obligado por el contenido] [se considerará firmante] del mensaje de la misma manera que si el mensaje hubiera existido en forma [manualmente] firmada con arreglo a la ley aplicable al contenido del mensaje.

Variante B Entre el titular de una clave privada y todo tercero que se fíe de una firma numérica susceptible de ser [verificada] [autenticada] utilizando la correspondiente clave pública certificada, la firma numérica [se presumirá que pertenece al titular] [satisface las condiciones expuestas en [el párrafo 1 del artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico]].

2) El párrafo 1) no se aplicará cuando:

a) el [iniciador] [titular] pueda demostrar que la [firma electrónica segura] [clave privada] se utilizó sin permiso y que el [iniciador] [titular] no pudo evitar dicha utilización ejerciendo una diligencia razonable; o

b) la parte que se fió de la firma sabía o debió haber sabido, si hubiese pedido información [al iniciador] [a la autoridad certificadora] o hubiese de otra manera ejercido una diligencia razonable, que la firma [electrónica segura] [numérica] no pertenecía al [iniciador] [titular de la clave privada]."

Observaciones generales

50. El Grupo de Trabajo examinó en primer lugar la finalidad y el alcance del proyecto de artículo 3 y su relación con los artículos 7 y 13 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico.

51. Se expresaron opiniones divergentes con respecto a si el proyecto de artículo debía versar únicamente sobre la atribución de las firmas electrónicas seguras (o las firmas numéricas) o si también debía abordar la cuestión de la responsabilidad del supuesto firmante para con las partes que se hubiesen fiado de su firma. Según una opinión, el proyecto de artículo 3 debía tener por objeto vincular una firma con el supuesto firmante y garantizar la integridad de un mensaje de datos. De acuerdo con otra opinión, el propósito principal del proyecto de artículo 3 debía ser crear un aliciente para la utilización de las firmas numéricas mediante la debida asignación de responsabilidad por toda pérdida causada a la parte confiante por el hecho de que el supuesto firmante no hubiese ejercido una diligencia razonable, así como evitar el uso no autorizado de su firma (véase el párrafo 58 *infra*). La opinión mayoritaria era que debían abordarse ambas cuestiones. En ese contexto, se instó a ejercer cautela al tratar las cuestiones relativas a la responsabilidad, que podrían no estar en consonancia con el criterio adoptado en la Ley Modelo, según el cual las cuestiones contractuales habrían de precisarse en la legislación aplicable, al margen de la Ley Modelo. En respuesta, se observó que el Régimen Uniforme se basaba en un criterio algo diferente en el sentido de que en él ya se abordaba, entre otras cosas, la cuestión de la responsabilidad de las entidades certificadoras. Tras un debate, el Grupo de Trabajo acordó examinar la posibilidad de abordar ambas cuestiones, posiblemente en disposiciones separadas (véanse los párrafos 55 y 60 *infra*).

52. Con respecto al alcance del proyecto de artículo 3, se expresó la opinión de que debía limitarse a las firmas numéricas y trasladarse a la parte correspondiente. En apoyo de esa opinión, se afirmó que las firmas numéricas eran tan conocidas y ampliamente utilizadas que se justificaba darles prioridad. Además, se señaló que la cuestión de la atribución de las firmas numéricas era suficientemente importante como para tratarse por separado de la cuestión de la atribución de otros tipos de firmas electrónicas. Según otra opinión, las normas establecidas con arreglo al proyecto de artículo 3 debían aplicarse tanto a las firmas numéricas como a otras firmas electrónicas. Imperó la opinión de que, en la medida de lo posible, las cuestiones incluidas en el proyecto de artículo 3 debían tratarse con un criterio de neutralidad respecto de los medios utilizados a fin de abarcar una amplia gama de firmas electrónicas.

53. En cuanto a la relación entre el proyecto de artículo 3 y los artículos 7 y 13 de la Ley Modelo, se observó que el artículo 7 versaba sobre los requisitos para las firmas y el artículo 13 sobre la atribución de los mensajes. Se expresó preocupación por la posibilidad de que el proyecto de artículo 3 simplemente repitiese las disposiciones del artículo 13 de la Ley Modelo. En respuesta a ello, se afirmó que el proyecto de artículo 3 se refería a la atribución de una firma electrónica y no a la atribución del mensaje de datos y otorgaba protección específicamente al supuesto firmante en casos en que su firma se utilizase sin autorización y el supuesto firmante no hubiese podido evitar dicha utilización no autorizada, de haber ejercido una diligencia razonable.

Párrafo 1)

54. Se expresó apoyo respecto de ambas variantes. A favor de la variante A, se dijo que estaba basada en un criterio de neutralidad respecto de los medios disponibles y por tanto abarcaba distintos tipos de tecnologías utilizadas en el comercio internacional. A ese respecto, se señaló que debía garantizarse la neutralidad también en cuanto a la forma en que se aplicaba una determinada tecnología (por ejemplo, una firma numérica con o sin un certificado). Se observó que tal neutralidad en la aplicación podía lograrse mediante una regla general en el sentido de que el receptor del mensaje de datos que razonablemente confiara en una firma electrónica segura tendría derecho a considerar ese mensaje como perteneciente al supuesto firmante (véase A/CN.9/WG.IV/WP.73, párrs. 35 y 36). En apoyo de la variante B, se afirmó que centraba debidamente la atención en las firmas numéricas, las cuales, por oposición a otros tipos de firmas electrónicas, eran bastante conocidas y ampliamente utilizadas.

55. No obstante, se criticaron ambas variantes por mezclar indebidamente dos cuestiones diferentes, a saber, la cuestión de la atribución y la cuestión de la responsabilidad. Además, se expresaron inquietudes y se formularon observaciones con respecto a ambas variantes. En cuanto a la variante A, se observó que las palabras introductorias no eran suficientemente claras; el empleo del término "iniciador" no era adecuado por varias razones, entre ellas que el firmante de un mensaje de datos no tenía necesariamente que ser su iniciador; las palabras "estará obligado por el contenido" se referían a la ley general de obligaciones y no a la mera atribución de firmas electrónicas al supuesto firmante; y la referencia a la legislación aplicable debía relacionarse con la legislación aplicable al mensaje de datos en su conjunto y no su contenido.

56. Con respecto a la variante B, se observó que a fin de no hacer caso omiso de las excepciones estipuladas en otras disposiciones del Régimen Uniforme en relación, por ejemplo, con las claves privadas comprometidas, debía añadirse al principio de la variante B una frase como "a reserva de lo dispuesto en los artículos ..."; en consonancia con el criterio adoptado en el artículo 13 de la Ley Modelo, debía hacerse referencia a la verificación efectiva de la utilización autenticada de una firma numérica y no sólo a la capacidad del titular de la clave privada de verificar dicha utilización; a fin de evitar una situación en que la firma numérica pudiese atribuirse al supuesto firmante aunque éste hubiese revocado el certificado, debía incluirse una frase como "la clave privada contenida en un certificado válido"; y no debía hacerse referencia al artículo 7 de la Ley Modelo, dado que ese artículo versaba sobre el requisito de una firma y no sobre la atribución de una firma.

Párrafo 2)

57. Si bien hubo acuerdo en el Grupo de Trabajo en cuanto a que el párrafo 2) era en general aceptable, se expresó preocupación por la posibilidad de que el término "diligencia razonable" crease incertidumbre. Para paliar esa preocupación se hicieron varias sugerencias. Según una de ellas, la firma debía atribuirse al supuesto firmante si no lograba demostrar que la firma se había utilizado sin autorización. De acuerdo con otra sugerencia, la firma debía considerarse la del supuesto firmante si, además, éste no lograba demostrar que no había podido evitar dicha utilización no autorizada, sin hacer referencia a la noción de "diligencia razonable". Se criticaron ambas sugerencias aduciendo que aumentarían indebidamente el grado de responsabilidad del supuesto firmante.

Sugerencias relativas a un nuevo artículo 3

58. A fin de abordar las preocupaciones expresadas con respecto al proyecto de artículo 3, y en el supuesto de que la cuestión de la atribución de las firmas electrónicas seguras se había tratado suficientemente en el proyecto de artículo 2 del régimen uniforme, se sugirió que en el proyecto de artículo 3 se trasladase el centro de atención a la cuestión de la responsabilidad del supuesto firmante y que, por tanto, el artículo 3 se formulase en términos como los siguientes:

> "1) Entre el titular de una clave privada y toda persona que se fíe de una firma numérica, el titular no quedará vinculado por el mensaje si no lo ha firmado.

2) Si el titular de la clave no ha ejercido una diligencia razonable para impedir que la parte receptora se fíe de la utilización no autorizada de la firma numérica, tendrá la obligación de compensar a la parte confiante por todo daño o perjuicio que se le haya causado. La parte confiante sólo tendrá derecho a dicha compensación si había solicitado información a la entidad certificadora o había de otra manera ejercido una diligencia razonable para demostrar que la firma numérica no era la del titular."

59. Si bien se acordó en general que la formulación sugerida permitía distinguir efectivamente entre la atribución de una firma y la rendición de cuentas (o responsabilidad) por el daño o perjuicio como consecuencia de la utilización no autorizada de una firma, se observó que no tenía en cuenta en forma suficiente las preocupaciones expresadas con respecto a las variantes A y B. Además, se observó que esa formulación trasladaba la carga de la prueba a la parte confiante, la cual debía demostrar que había ejercido una diligencia razonable a fin de probar que la firma era la del supuesto firmante. Se acordó en general que sería preferible adoptar un criterio de neutralidad con respecto a los medios utilizados y que las cuestiones de la atribución y la responsabilidad debían tratarse por separado.

60. Con miras a reflejar dicho criterio, se invitó al Grupo de Trabajo a que examinara otra formulación del texto en los términos siguientes:

"**Atribución de firmas electrónicas seguras**

En las relaciones entre el supuesto firmante y la parte que haya de fiarse del mensaje, una firma electrónica segura será atribuible al supuesto firmante a menos que el supuesto firmante pueda demostrar que la firma electrónica segura se utilizó sin autorización.

Responsabilidad respecto de las firmas electrónicas seguras

Cuando la firma electrónica segura no haya sido autorizada y el supuesto firmante no haya ejercido una diligencia razonable para impedir que el destinatario confíe en el mensaje, el supuesto firmante tendrá la obligación de pagar daños y perjuicios para compensar a la parte que se fió del mensaje, a menos que la parte confiante no haya solicitado información a terceros pertinentes o haya sabido o debido saber de algún otro modo que la firma no era la del supuesto firmante."

61. Tras un debate, el Grupo de Trabajo pidió a la Secretaría que reflejara el texto sugerido como alternativa en un proyecto de régimen uniforme revisado para que el Grupo de Trabajo lo siguiera examinando en un futuro período de sesiones. Varias delegaciones expresaron la preocupación de que el texto sugerido pudiera interferir con la legislación nacional en materia de daños extracontractuales.

Sección II. **Firmas numéricas**

Artículo 4. **Definición**

62. El texto del proyecto de artículo 4 que examinó el Grupo de Trabajo era el siguiente:

"Para los fines del presente Régimen,

Variante A por "firma numérica" se entenderá un tipo de firma electrónica consistente en una transformación de un mensaje de datos gracias al empleo de una función de compendio de mensajes y un criptosistema asimétrico que permitan que una persona que disponga del

mensaje de datos sin transformar y de la clave pública del firmante pueda determinar con exactitud:

a) si la transformación se efectuó utilizando la clave privada del firmante que corresponde a su clave pública; y

b) si el mensaje de datos inicial fue modificado después de efectuada la transformación.

Variante B

a) por "firma numérica" se entenderá un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido vinculado a la clave criptográfica privada del iniciador, permite determinar que ese valor numérico se ha obtenido exclusivamente con la clave criptográfica privada del iniciador.

b) los procedimientos matemáticos utilizados para generar firmas numéricas autorizadas a tenor del presente Régimen se basan en la criptografía de clave pública. Aplicados a un mensaje de datos, esos procedimientos matemáticos transforman el mensaje de modo que permite que una persona que tenga el mensaje inicial y la clave pública del iniciador pueda determinar con exactitud:

i) si la transformación se efectuó utilizando la clave privada del firmante que corresponde a la clave pública del iniciador; y

ii) si el mensaje de datos inicial fue modificado después de efectuada la transformación."

63. Si bien se manifestó cierto apoyo respecto de ambas variantes, el Grupo de Trabajo no aprobó ninguna de las dos.

64. A favor de la variante A se dijo que, en la medida en que se centraba en la creación de una firma numérica sin referirse a ninguna tecnología concreta, era lo suficientemente flexible como para incluir diferentes tipos de firmas numéricas. No obstante, se expresó la inquietud en el sentido de que la variante A no reconocía las diferentes formas en que podía aplicarse una infraestructura de clave pública (por ejemplo, tomando o no tomando como base una función de compendio de mensajes), ni las diferentes funciones que podrían desempeñarse mediante la utilización de una firma numérica (por ejemplo, la función de identificación del firmante ("firmas seguras"), la función de establecer la integridad del mensaje de datos ("constancias seguras"), o una combinación de ambas funciones). A fin de garantizar el reconocimiento transfronterizo de los diferentes tipos de certificados y firmas numéricas, en el contexto de este debate se sugirió que el Grupo de Trabajo estudiase la idea de preparar una convención en lugar de una adición a la Ley Modelo (véase el párrafo 212 *infra*).

65. En respuesta a la mencionada inquietud, se señaló que la inclusión de los elementos de identificación del firmante y la verificación de la integridad del mensaje en una definición de "firma numérica" forman parte de un criterio establecido. Además, se indicó que dicho criterio, cuyo objetivo era establecer un equivalente funcional de una firma efectuada sobre papel, era coherente con el criterio adoptado en la Ley Modelo. Se afirmó asimismo que la tarea de abarcar todos los tipos de firmas numéricas sería excesivamente ambiciosa y demoraría los progresos en una esfera que había que reglamentar urgentemente a fin de evitar la falta de armonía entre las legislaciones al aplicar diferentes criterios en la legislación nacional. A este respecto, se observó que la variante A, al definir la firma numérica como un tipo de firma electrónica, limitaría este concepto a las aplicaciones de la criptografía de clave pública destinadas a servir de equivalente funcional de una firma sobre papel, en tanto que la variante B sería lo

suficientemente amplia para abarcar todas las manifestaciones de la tecnología de firmas numéricas, incluidas las que no estaban destinadas a servir de equivalentes funcionales de firmas.

66. A favor de la variante B, se observó que daba mayor seguridad en cuanto a su alcance, dado que estaba enunciada en términos más técnicos y se refería específicamente a la criptografía de clave pública que, según se afirmó, constituía una tecnología de uso generalizado. Al mismo tiempo, se expresó la preocupación de que la variante B fuera demasiado limitada en el sentido de que se basaba en un determinado procedimiento matemático para generar una firma numérica, lo que posiblemente excluía los futuros adelantos técnicos que podrían hacer obsoletos los procedimientos actualmente aceptados. Se sugirió que tal vez sería necesario hacer una referencia en el proyecto de disposición a "los procedimientos matemáticos más modernos".

67. Se objetaron las variantes A y B aduciendo que no definían de manera apropiada la "firma numérica" al referirse a "una transformación del mensaje de datos". Se explicó que lo que cambiaba como resultado del procesamiento del mensaje mediante la utilización de un algoritmo no era el mensaje en su conjunto sino únicamente su representación numérica. Para paliar ese problema se propuso la siguiente formulación:

> "La firma numérica es una transformación criptográfica (mediante una técnica criptográfica asimétrica) de la representación numérica de un mensaje de datos, de índole tal que cualquier persona que tenga el mensaje de datos y la clave pública pertinente pueda determinar:
>
> a) que la transformación se efectuó utilizando la clave privada correspondiente a la clave pública pertinente; y
>
> b) que el mensaje de datos no ha sido alterado desde que se efectuó la transformación criptográfica."

68. En apoyo del texto propuesto se dijo que, al evitar hacer referencia a la clave privada del firmante, se tenía en cuenta la necesidad de garantizar que las firmas numéricas utilizadas para diversos fines, aparte de la identificación del firmante, quedarían abarcadas en el Régimen Uniforme. Se afirmó asimismo que al evitar la referencia a una función de compendio de mensajes, el texto propuesto incluiría también las firmas numéricas generadas mediante un procedimiento diferente.

69. Durante el debate se sugirió que el Grupo de Trabajo estudiara, sólo con fines de comparación, el texto aprobado en 1988 por la Organización Internacional de Normalización (ISO), a saber: Mensaje de datos: datos anexos a una unidad de datos, o transformación criptográfica de ésta, que permiten al receptor de la unidad de datos comprobar la fuente y la integridad de dicha unidad y protegerla contra la falsificación, por ejemplo, por parte del receptor (ISO 7498/2). Otra sugerencia era que la definición de la ISO se incluyera en el Régimen Uniforme. Si bien se convino en que la definición de la ISO reflejaba un criterio técnico, la mayoría de los participantes en el Grupo de Trabajo se mostró escéptica en cuanto a la idoneidad de la definición para los fines del Régimen Uniforme.

70. Tras un debate, el Grupo de Trabajo acordó en general que debía reservarse su decisión con respecto a la definición de "firma numérica" hasta que hubiese finalizado el examen de las disposiciones sustantivas del Régimen Uniforme y llegado a una conclusión acerca del alcance de las disposiciones. En particular, la definición de "firma numérica" podría variar según si el Régimen Uniforme abarcaba únicamente las aplicaciones de técnicas informáticas cuyo objetivo era reproducir en un contexto electrónico las funciones que tradicionalmente se realizaban mediante firmas manuales en las operaciones comerciales internacionales, o si el alcance del Régimen Uniforme se hacía extensivo a otros usos de las "firmas numéricas". Se pidió a la Secretaría que preparase otros proyectos de texto basados en las variantes A y B y el proyecto de texto antes citado (véase el párrafo 67 *supra*)" teniendo en cuenta las observaciones formuladas, a fin de seguir examinando la cuestión en un futuro período de sesiones.

Artículo 5. **Efectos**

71. El texto del proyecto de artículo 5 que examinó el Grupo de Trabajo era el siguiente:

"1) Si un mensaje de datos está firmado en todo o en parte con una firma numérica, ésta se considerará como firma electrónica segura con respecto a la parte pertinente del mensaje cuando:

a) la firma numérica fue creada durante el período de vigencia de un certificado [válido] y ha sido verificada con referencia a la clave pública enunciada en el certificado; y

b) se estime que el certificado vincula con exactitud una clave pública con la identidad de una persona porque:

i) el certificado fue emitido por una entidad certificadora licenciada [acreditada] por ... *[el Estado promulgante especifica el órgano o la autoridad competente para licenciar a las entidades certificadoras y promulgar reglamentos para su funcionamiento]*; o

ii) el certificado fue de alguna otra manera emitido por una entidad certificadora de conformidad con las normas dictadas por ...*[el Estado promulgante especifica el órgano o la autoridad competente para establecer normas reconocidas sobre el funcionamiento de entidades certificadoras licenciadas]*.

2) Si un mensaje de datos está firmado en todo o en parte por una firma numérica que no satisface los requisitos contenidos en el párrafo 1), la firma numérica se considerará como firma electrónica segura con respecto a esa parte del mensaje si hay pruebas suficientes que indiquen que el certificado vincula con exactitud una clave pública con la identidad del titular.

3) Lo dispuesto en el presente artículo no será aplicable a: [...]."

Observaciones generales

72. Se reconoció ampliamente, en un principio, que el Grupo de Trabajo tendría que examinar nuevamente la sustancia del proyecto de artículo 5 a la luz de las decisiones que se adoptasen sobre el alcance del Régimen Uniforme. En particular, el proyecto de artículo 5 dependía directamente de que la noción de "firma electrónica segura" se utilizase en su momento en el Régimen Uniforme. Los efectos jurídicos que se derivaban del uso de certificados en el contexto de las firmas numéricas dependerían también de la definición de "certificado" en el marco del proyecto de artículo 8. Si el Régimen Uniforme se refiriera únicamente a los casos en que se utilizaban firmas numéricas a los efectos de operaciones comerciales internacionales con la intención de firmar (es decir, identificar al firmante y vincularlo con la información que se firma), tal vez resultara aceptable limitar la función del certificado a la de vincular un par de claves con la identidad de una persona. En tal caso, debería especificarse que el Régimen Uniforme se ocupaba únicamente de un tipo especial de certificados ("certificados de identidad"), sobre todo porque se pueden utilizar en el comercio electrónico otros tipos de certificados, por ejemplo, para acreditar el nivel de autoridad de una persona ("certificados de autoridad"). Se expresó la opinión de que el proyecto de artículo 5 debería abarcar los certificados de autoridad junto con los certificados de identidad. En el contexto de ese debate, se sugirió que en el proyecto de artículo 5 se hiciera alusión al certificado que verifica la integridad de la información contenida en el mensaje de datos. En respuesta a esa sugerencia, se declaró que, si bien la verificación de la integridad de los datos era una consecuencia importante del uso del certificado en el contexto de un proceso de firma numérica, no se trataba de un elemento característico del propio certificado.

73. Tras un debate, el Grupo de Trabajo decidió proseguir con su examen del proyecto de artículo 5. No obstante, hubo acuerdo general en que habría que reanudar el debate una vez que el Grupo de Trabajo hubiera terminado su examen de las disposiciones sustantivas del Régimen Uniforme.

Título

74. Se expresó la opinión ampliamente compartida de que el título del proyecto de artículo 5 no era suficientemente descriptivo y podría inducir a error. Se decidió que se redactara nuevamente el título de conformidad con el siguiente tenor: “Firmas numéricas respaldadas por certificados”.

Párrafo 1)

Primera frase

75. Se expresó apoyo a la opinión de que la referencia a la noción de “firma numérica segura” no era necesaria en el proyecto de artículo 5 y debería sustituirse por una referencia a las condiciones enunciadas en el artículo 7 de la Ley Modelo. En respuesta, se declaró que una referencia de esa índole al artículo 7 de la Ley Modelo limitaría de forma improcedente el alcance del proyecto de artículo 5 al presuponer la existencia de requisitos legales de firma que tendrían que cumplirse en un entorno electrónico. El propósito del proyecto de artículo 5 era más extenso y apuntaba directamente a crear la certidumbre sobre los efectos jurídicos de las firmas numéricas, siempre que se cumplieran ciertos criterios técnicos, con independencia de que ya existiera un requisito específico de firma.

76. Tras un debate, el Grupo de Trabajo decidió que las referencias a una “firma electrónica segura” y a las condiciones enunciadas en el artículo 7 de la Ley Modelo se mantuvieran como redacción alternativa para su ulterior examen por el Grupo de Trabajo en un período de sesiones futuro. La primera frase del proyecto de artículo 5 debería rezar con arreglo al siguiente tenor: “Si el iniciador de un mensaje de datos en todo o en parte está identificado por una firma numérica, ésta [es una firma electrónica segura] [cumple las condiciones establecidas en el artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico] cuando:”.

Inciso a)

77. El contenido del inciso a) resultó generalmente aceptable. Con miras a mejor reflejar la necesaria fiabilidad del proceso de firma numérica, se decidió que se insertara la expresión “de forma segura” para calificar tanto la creación de la firma numérica como su verificación por referencia a la clave pública enumerada en el certificado. También se decidió que se mantuviera sin corchetes en el proyecto de disposición la referencia a la validez del certificado.

Inciso b)

78. Por lo que se refiere al inciso i) del párrafo b), se expresó la opinión generalizada de que las palabras “licenciada” o “registrada” eran preferibles a la palabra “acreditada” en una disposición que se ocupaba del caso en que los Estados adaptarían un planteamiento regulador de las infraestructuras de clave pública. Por lo que se refiere al inciso ii) del párrafo b), se expresó la opinión de que debería suprimirse la disposición, ya que el alcance del proyecto de artículo 5 debía limitarse a la utilización de certificados emitidos por entidades certificadoras licenciadas por el Estado promulgante. No obstante, la opinión dominante fue que debía hacerse alusión a normas industriales y a mecanismos que pudieran elaborar los profesionales para garantizar la fiabilidad de esas normas. Hubo acuerdo general en que una referencia de esa índole era necesaria para reflejar el “enfoque doble” de las firmas numéricas y las infraestructuras de clave pública adoptado por el Grupo de Trabajo en su período de sesiones anterior (A/CN.9/437, párr. 69). En virtud de ese enfoque, se reconocerían las normas industriales junto con la

reglamentación gubernamental. Se señaló que, en algunos países, las autoridades gubernamentales tal vez podían preferir no verse envueltas en el establecimiento de normas de seguridad para firmas numéricas. A ese respecto, se declaró que el proyecto de artículo 5 debería mencionar no sólo "normas de seguridad" sino abordar más ampliamente los diversos tipos de normas que podría elaborar la industria.

79. Por lo que se refiere a la referencia a normas industriales reconocidas, se sugirió que se podría tomar el texto del párrafo 2) del artículo 9 de la Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías, que aludía a "un uso del que [las partes] tenían o debían haber tenido conocimiento y que, en el comercio internacional, sea ampliamente conocido y regularmente observado por las partes en contratos del mismo tipo en el tráfico mercantil de que se trate". No obstante, hubo amplio acuerdo en que sería más procedente una referencia a "normas comercialmente apropiadas e internacionalmente reconocidas".

80. Teniendo en cuenta el debate arriba citado, se convino en que el inciso b) se redactara de nuevo, para los fines de ulteriores debates, con arreglo al siguiente tenor:

"b) el certificado vincula una clave pública con la identidad de una persona en virtud del hecho de que:

i) el certificado fue emitido por una entidad certificadora licenciada por ... [*el Estado promulgante especifica el órgano o la autoridad competente para licenciar a las entidades certificadoras y promulgar reglamentos para su funcionamiento]*; o

ii) el certificado fue emitido por una entidad certificadora acreditada por un órgano de acreditación competente aplicando normas comercialmente apropiadas e internacionalmente reconocidas relativas a la fiabilidad de la tecnología, las prácticas y otras características pertinentes de la entidad certificadora. Una lista no exclusiva de órganos o normas que cumplen con lo dispuesto en el presente párrafo podrá ser publicada por ... [*el Estado promulgante especifica el órgano o la autoridad competente para establecer normas reconocidas sobre el funcionamiento de entidades certificadoras licenciadas];* o

iii) el certificado fue de alguna otra manera emitido de conformidad con normas comercialmente apropiadas e internacionalmente reconocidas."

Párrafo 2)

81. Se expresó una serie de inquietudes en relación con el párrafo 2). Una de ellas consistía en que el párrafo 2) podía ser redundante a la luz del artículo 2, en el que se enunciaban las presunciones jurídicas que lleva consigo la condición de "firma electrónica segura". En respuesta, se declaró que el párrafo 2) era necesario para establecer el vínculo entre una firma numérica que pudiera ser reconocida (por ejemplo, por un tribunal de justicia) como el vínculo entre la clave pública y el titular, aunque no cumpliera formalmente los requisitos enunciados en el párrafo 1), y otras disposiciones del Régimen Uniforme (por ejemplo, el proyecto revisado de artículo 3 sobre "responsabilidad de la firma electrónica segura"). En ese contexto, se expresó la opinión de que tal vez habría que introducir en el proyecto de artículo 3 las palabras "No obstante lo dispuesto en el artículo 5".

82. Otra preocupación era que el párrafo 2) establecía una criterio excesivamente bajo para el reconocimiento de firmas numéricas que de otra manera no cumplían los requisitos enunciados en el párrafo 1). En su redacción actual, el párrafo 2) podría conducir a que se concediera la condición de "seguras" a firmas numéricas que dependían de procedimientos no seguros, por ejemplo, por falta de suficiente longitud de la clave. En respuesta, se declaró que, si bien podría ser necesario introducir otra referencia a la fiabilidad de los procedimientos técnicos en el proyecto de artículo 5 o en la definición de "firma electrónica segura", era necesaria una disposición del tenor del párrafo 2)

para conservar la posibilidad de que se pudiera permitir a las partes que determinaran ante un tribunal o un tribunal arbitral que la firma numérica que utilizaban era lo suficientemente fiable para que se le concediese valor jurídico aunque se utilizara fuera del contexto del párrafo 1). Sin embargo, se expresó la preocupación de que, al dar la calificación de "segura", se creaban presunciones y se asignaban responsabilidades extracontractuales en virtud de los artículos 2 y 3 del proyecto. Se afirmó que esas graves consecuencias habrían de ser demostrables por remisión a reglas y normas claras antes de utilizarse la firma, en vez de ser impuestas posteriormente por un tribunal a una parte que no sospechara nada.

83. Se formularon varias sugerencias sobre la forma en que se debía expresar la referencia a las reglas generales de prueba contenida en el párrafo 2). Una opinión era que el párrafo 2) debía tener un alcance más amplio para abarcar no sólo la situación en que se utilizara un certificado sino también cualquier otra situación en que se utilizara una firma numérica o cualquiera otra firma electrónica. Según esa opinión, debía suprimirse del párrafo 2) la referencia a "el certificado", que se debía colocar en una sección dedicada a las firmas electrónicas en general. Otra opinión sostuvo que el alcance del párrafo 2) debía ser más estrecho y que la disposición debería aplicarse únicamente cuando la firma numérica se creaba durante el período de vigencia de un certificado válido. Según esa opinión, la norma contenida en el párrafo 2) debería formar parte del inciso b) del párrafo 1) con el siguiente tenor:

> "iv) hay pruebas suficientes que indiquen que el certificado vincula con exactitud una clave pública con la identidad del titular."

84. Tras un debate, el Grupo de Trabajo no llegó a un consenso acerca del alcance y la colocación de la disposición contenida en el párrafo 2). Se pidió a la Secretaría que preparara un proyecto de disposición revisado, con variantes que reflejaran el debate, para su examen por el Grupo de Trabajo en un futuro período de sesiones.

Artículo 6. **Firma de personas jurídicas**

85. El texto del proyecto de artículo 6 que examinó el Grupo de Trabajo era el siguiente:

> "[Toda persona jurídica podrá identificar un mensaje de datos consignando en ese mensaje la clave criptográfica pública certificada para esa persona jurídica. Sólo se considerará que esa persona jurídica [es la iniciadora] [ha dado su aprobación al envío] de ese mensaje cuando el mensaje haya sido además firmado numéricamente por la persona física autorizada para actuar en nombre de dicha persona jurídica.]"

86. Se recordó que, en el anterior período de sesiones del Grupo de Trabajo, se había expresado la opinión generalizada de que el proyecto de artículo 6 debía suprimirse. Se había mantenido en corchetes como recordatorio de que el Grupo de Trabajo tal vez precisara examinar con más detalle el grado en que el Régimen Uniforme debía validar el funcionamiento de "agentes electrónicos" con fines de autenticar mensajes de datos automáticamente (véase A/CN.9/437, párrs. 115 a 117). El Grupo de Trabajo decidió que sería preciso examinar más tarde la cuestión de los "agentes electrónicos". Se decidió, no obstante, que se suprimiera el proyecto de artículo 6, puesto que podía considerarse que constituía una injerencia indebida en otros conjuntos normativos (por ejemplo: en la legislación sobre la representación y las disposiciones del derecho societario relativas a la representación de las sociedades por personas naturales).

Sección III. **Otras firmas electrónicas**

87. Hubo acuerdo general en que la sección III debía permanecer en el Régimen Uniforme hasta que se decidiera si el principio de no discriminación, enunciado en las definiciones de "firma" y de "firmas electrónicas seguras" (y expresado a través de la condición jurídica reconocida a toda técnica de autenticación que cumpla los requisitos de

firma electrónica “segura”), habría de expresarse en disposiciones más concretas relacionadas con las técnicas de autenticación distintas de las firmas digitales.

88. A fin de proporcionar más información al Grupo de Trabajo sobre el modo en que pueden funcionar las firmas digitales y otras técnicas de autenticación, se realizaron varias presentaciones de carácter técnico, que se resumen a continuación (párrs. 89 a 105).

89. Se recordó que el comercio electrónico seguro requería que las partes en una operación tuvieran capacidad para autenticarse recíprocamente. En muchos casos de interacción electrónica (por ejemplo, compras en Internet), los métodos tradicionales de autenticación no existían o no eran fiables. Esta necesidad de métodos fiables de autenticación electrónica va más allá de los requisitos del comercio y abarca a casi todos los tipos de interacción en un mundo digital.

90. Se observó que para hacer frente a estas necesidades existían actualmente muy diversas soluciones. Estas soluciones tenían componentes a la vez tecnológicos y metodológicos. Si bien se hacía hincapié en los distintos enfoques tecnológicos, no debía subestimarse el impacto de la metodología o del modelo comercial que implicaba la solución de autenticación electrónica. Además de los numerosos y distintos enfoques tecnológicos, el mercado había ofrecido también una gran diversidad de metodologías para la aplicación de esas tecnologías. La diversidad de soluciones reflejaba los distintos tipos de autenticación que se requerían en las numerosas situaciones que se daban en el mundo digital. A medida que se desarrollara este mundo, harían falta nuevas soluciones de autenticación.

91. Los métodos de autenticación podían dividirse en categorías en función de la característica que se autenticara. Las tres categorías básicas de características se describieron del modo siguiente: 1) “algo que usted sabe”; 2) “algo que usted es”; y 3) “algo que usted tiene”. En muchas soluciones se utilizaba una combinación de esas tres características.

92. La primera categoría (“algo que usted sabe”) era una de las características más comúnmente utilizadas para autenticar a personas. En esta categoría entraban las contraseñas, las frases en clave y los números de identificación personal (NIP). En la mayoría de los sistemas informáticos se ofrecían opciones con contraseña que permitían a los usuarios que dispusieran de una contraseña válida tener acceso a recursos. Por ejemplo, en el acceso automatizado a la información sobre cuentas bancarias, el usuario debe conocer el NIP correcto asociado a la cuenta sobre la que busca información. Otro tipo de autenticación en esta categoría se basaba en la información personal que sólo puede conocer una determinada persona. Por ejemplo, en algunas jurisdicciones los bancos acostumbran a pedir a la persona que abre una cuenta el apellido de su madre (antes de contraer matrimonio). Esta información podía utilizarse posteriormente para autenticar al titular de la cuenta. Si bien esta categoría de autenticación estaba muy difundida en la práctica, tenía varios inconvenientes. En primer lugar, se requería por lo general que la palabra utilizada fuera secreta o difícil de obtener. En segundo lugar, era necesario que las partes tuvieran una relación previa en que pudieran “compartir” la palabra o las palabras secretas (por ejemplo, la contraseña, el NIP o el apellido de soltera de la madre).

93. La segunda categoría de métodos de autenticación (“algo que usted es”) se refería a menudo a características físicas (biométrica). Para la autenticación se utilizaban cualidades innatas de las personas, como las huellas digitales, la retina, el iris, las huellas manuales, los registros de voz, y las firmas manuales. Dado que todas estas características eran únicas e irrepetibles, representaban un método excelente de autenticación. Si la información sobre esas características pudiera difundirse, este tipo de autenticación no requeriría una relación previa. Además, estos métodos podían ofrecer una autenticación muy sólida, dado lo difícil que era manipular o alterar esos sistemas. Estos métodos tenían el inconveniente de que su costo de realización era alto, ya que requerían algún tipo de equipo para obtener información sobre la característica de la persona. Otro problema que planteaban algunas aplicaciones de esta categoría era el aparato utilizado para recoger la información biométrica. En algunos casos, los aparatos eran

considerados muy molestos (por ejemplo, para el escáner de la retina había que colocar el ojo en un molde en forma de ojo con una luz roja que iluminaba la retina). En otros casos, la información obtenida con el aparato de autenticación podía revelar información médica que la persona no deseara divulgar (por ejemplo, podían diagnosticarse ciertas condiciones de salud mediante las irregularidades del iris; por consiguiente, si bien el examen del iris con escáner no resultaba físicamente molesto, se consideraba a veces como una violación de la intimidad). Por último, algunos de estos aparatos no eran siempre fiables en condiciones "anormales" (por ejemplo, la obtención de huellas dactilares de un dedo con un corte). No obstante, las soluciones biométricas se tenían por uno de los métodos más sólidos de autenticación y se utilizaban en la práctica. Se citó el ejemplo de un país cuyos servicios de inmigración y naturalización experimentaban una solución tecnológica con las huellas manuales para agilizar el control de pasaportes, y el de compañías de seguros que utilizaban datos biométricos para autenticar a personas en el procesamiento en solicitudes de pago.

94. La tercera categoría de métodos de autenticación ("algo que usted tiene") se consideraba como uno de los ámbitos más activos en la autenticación electrónica. El "algo" podía ser físico (por ejemplo, un aparato de respuesta) o podía ser información (por ejemplo, una clave criptográfica). El aparato de respuesta era similar al criterio del secreto compartido en la categoría de "algo que usted sabe", pero se llevaba a la práctica con métodos técnicos. Esta solución requería dar a las personas un aparato singular que se asignaba únicamente a esa persona. Cuando la persona trataba de tener acceso a un servicio, el sistema le pedía que se identificara (generalmente con el nombre del usuario) y a continuación el sistema generaba una combinación numérica basada en la información que el sistema tenía sobre el aparato asignado especialmente a esa persona. El usuario marcaba entonces ese número en el aparato, que generaba una respuesta numérica. Esa respuesta numérica podía introducirse en el sistema al que el titular del aparato intentaba tener acceso. El sistema "sabía" que sólo había una única respuesta aceptable al problema numérico presentado al usuario, y esa única respuesta aceptable sólo podía ser generada por el aparato asignado especialmente al usuario. Por consiguiente, cuando el usuario marcaba la respuesta numérica correcta, el sistema "sabía" que la persona que trataba de tener acceso a él era realmente la persona que decía ser. Ese tipo de aparato se utilizaba comúnmente para autenticar a personas que solicitaban acceso remoto a sistemas informáticos. También lo utilizaba un banco en un proyecto piloto de operaciones bancarias desde el domicilio particular, llamado operaciones de "*browser*", ya que permite a las personas tener acceso a una cuenta bancaria desde cualquier "*browser*" de cualquier máquina. Esta aplicación ponía en evidencia las ventajas del método, ya que si bien requería un componente de equipo, no requería una modificación del sistema como las tarjetas de chip.

95. La otra subcategoría de la tercera categoría abarcaba la utilización de firmas numéricas. El aspecto importante de la tecnología de las firmas numéricas era la utilización de una clave privada para generar una firma numérica y la utilización de una clave pública para autenticar la firma numérica. La clave privada utilizada para generar las firmas numéricas podía almacenarse en un disco duro o en una tarjeta *smart* y debía guardarse muy cuidadosamente ya que era estrictamente personal. La clave pública se difundía ampliamente. Había varios paradigmas para utilizar la tecnología de las firmas numéricas, cada uno de los cuales tenía un modo distinto de inspirar confianza al receptor de una firma numérica.

96. Uno de los primero métodos era la creación de una guía de personas y de claves públicas. Según este modelo, el receptor de un documento firmado numéricamente verificaba la clave pública del signatario del documento consultando la clave pública en una guía de confianza. Se tenía constancia de que actualmente se utilizaba este modelo en varias aplicaciones.

97. Otro método, históricamente nacido del método de la guía, se basaba en la utilización de certificados numéricos. Los certificados numéricos eran documentos electrónicos firmados numéricamente por una entidad de confianza. Cuando un documento estaba numéricamente firmado, se adjuntaba una copia del certificado numéricos del signatario, que contenía información sobre la persona y sobre su clave pública. Al recibir el mensaje y el certificado numérico, el receptor utilizaba la clave pública en el certificado numérico para autenticar el mensaje.

98. Los certificados numéricos se empleaban con una norma (ISO X.509) que permite una jerarquía de las entidades de confianza utilizadas para autenticar a las partes. Este método se denomina a menudo modelo de la tarjeta de crédito, ya que refleja el modelo comercial en que se basa la industria de tarjetas de crédito. Por ejemplo, un comerciante, aún no conociendo, podía estar dispuesto a aceptar una determinada tarjeta para el pago, ya que sabía que la tarjeta era emitida por un banco a nombre del consumidor (el nombre del banco figuraba siempre en la tarjeta) y ese banco estaba autorizado a emitir la tarjeta por la empresa de tarjetas de crédito. Aun cuando el comerciante no conociera el banco emisor de la tarjeta, podría confiar en el consumidor porque sabía que el consumidor había sido autenticado por el banco y el banco, a su vez, por la empresa de tarjetas de crédito. De modo similar, las jerarquías de confianza de la norma X.509 permitían autenticar certificados numéricos conforme a un orden jerárquico de entidades de confianza (denominadas "entidades certificadoras", así denominadas también en el presente informe) que podían ser verificadas por el receptor del certificado. La última autoridad certificadora en esta cadena era denominada la raíz. Por consiguiente, la firma digital de un documento conforme al método X.509 implicaba el envío del certificado digital del signatario y de todos los certificados digitales auxiliares relacionados con la jerarquía de entidades de confianza. Según ese modelo, el receptor podía verificar toda la cadena de entidades de confianza sin tener que consultar una guía en línea. Este método se consideró especialmente adecuado para facilitar las comunicaciones de confianza entre un gran número de personas que no han tenido apenas contactos previos entre sí. Una de las ventajas de este método, que era la posibilidad de relacionar muchos certificados con una raíz de confianza, constituía también su punto débil. Si esa raíz estaba en entredicho, todo lo que venía después de ella perdía credibilidad.

99. Otra variante de la utilización de los certificados digitales se denominaba comúnmente la malla del modelo de confianza. En este modelo no había entidades certificadoras. Los certificados numéricos eran generados por las personas. No había ninguna raíz de confianza. Las personas decidían en quién iban a confiar y hasta qué punto. Este modelo estaba concebido para pequeñas comunidades de usuarios con contactos regulares y era de difícil aplicación a más gran escala. No obstante, este modelo se utilizaba actualmente en muchos entornos.

100. Se afirmó que una importante consideración para comprender la utilización de los certificados numéricos X.509 era el sesgo histórico hacia la identidad. Dado que la norma X.509 nació de la guía X.500, trataba naturalmente de asociar las claves públicas con la identidad de las personas. Se sostuvo que esta predisposición con la identidad confundía muchas cuestiones de orden público en torno a la utilización de las firmas numéricas. Si bien estaba claro que ciertos certificados numéricos autenticaban la identidad de una persona, estaba claro también que los otros certificados numéricos tenían funciones distintas de la autenticación de la identidad. Los certificados numéricos también podían utilizarse para autenticar los derechos o relaciones de una persona sin especificar la identidad de la persona. En muchos casos, la identidad de la persona era innecesaria o incluso indeseable. Había muchos certificados con fines especiales que sólo podían utilizarse para ciertas funciones, al igual que la tarjeta de crédito de una persona sólo podía emplearse para autenticar la identidad de la persona y del mismo modo que un pasaporte no podía utilizarse para adquirir bienes. La tendencia a pensar ante todo en la identidad era lógica, pero podía limitar gravemente la utilización de la tecnología. Si toda aplicación que utilizara firmas numéricas tuviera que cumplir los requisitos estrictos de un certificado de identidad con fines generales, la tecnología tendría una utilización sumamente difícil y costosa. Era importante recordar que habría una amplia gama de requisitos de autenticación y que la tecnología era lo suficientemente flexible para cumplir todos estos requisitos.

101. Cuando varias empresas de tarjetas de crédito decidieron elaborar un método seguro para el comercio electrónico por redes públicas como Internet, se fijaron tres objetivos comerciales primordiales: la solución tenía que ser segura; la solución tenía que estar abierta a cualquier proveedor de tecnología interesado en elaborar un producto que cumpliera el protocolo definido; y todas las aplicaciones debían ser practicables entre sí. Para la industria de pagos, el término "seguro" tiene tres componentes: 1) el carácter reservado de la información sobre los pagos, incluido el número de cuenta del consumidor; 2) la integridad de la información sobre los pedidos; y 3) la autenticación de las partes en la operación. A fin de lograr el nivel deseado de "seguridad", se creó el protocolo de

Transacciones Electrónicas Seguras (“SET”). Este protocolo utilizaba firmas numéricas (basadas en el modelo X.509) para cumplir la función de integridad de los datos y autenticación de las partes.

102. Se hizo una breve descripción del protocolo SET. El consumidor que decidiera realizar comercio electrónico seguro con SET debía ante todo obtener material que cumpliera los procedimientos establecidos por la entidad certificadora básica de SET. Este material generaba un par de claves y una solicitud que el consumidor enviaba a la entidad que emitía la tarjeta de pago para su uso. El material ponía la clave pública en la solicitud del certificado e instaba al consumidor a proporcionar información de identificación a fin de que la institución financiera pudiera comprobar si la persona que solicitaba el certificado estaba autorizada a hacerlo. Esta solicitud se enviaba a la institución financiera a través de Internet. Si la solicitud era aceptada, la institución financiera firmaba numéricamente el certificado del consumidor y lo devolvía al consumidor por Internet. El material del consumidor almacenaba el certificado digital en su computadora. Este procedimiento de solicitud sólo se hacía una vez para obtener el certificado.

103. A continuación, el consumidor empezaba a comprar en línea y podía emprender operaciones seguras con comerciantes que utilizaran material ajustado a SET. En las primeras fases de la operación, el material del consumidor solicitaba al comerciante información de autenticación. El material autenticaba al comerciante comprobando todas las firmas numéricas y los certificados numéricos enviados por el comerciante. Si en algún momento del proceso de autenticación se producía un fallo, el consumidor quedaba avisado. A continuación, el consumidor especificaba los bienes o servicios que deseaba adquirir, seleccionaba el método de pago e iniciaba la operación. El material del consumidor separaba la información de pago de la del pedido. La información de pago estaba formulada en clave con una compleja criptografía, de modo que sólo la institución financiera del comerciante pudiera descifrarla. La información del pedido, en la que se especificaba lo que el consumidor quería adquirir y otros detalles de la operación y la información de pago formulada en clave se firmaba numéricamente y se enviaba al comerciante. Cuando el comerciante recibiera este mensaje, separaría la información de pago formulada en clave, firmaría numéricamente este nuevo mensaje y lo enviaría a su institución financiera. La institución financiera verificaría la firma digital del comerciante, descifraría la información sobre el pago y haría procesar esa información a través de la infraestructura existente para los pagos. La institución financiera firmaba numéricamente la respuesta de autorización y la enviaba al comerciante, que a su vez enviaba al consumidor una respuesta firmada numéricamente. Si la operación era autorizada, el comerciante cumplía el pedido.

104. Se afirmó que SET ilustraba la dependencia respecto de la tecnología de firmas numéricas en la autenticación de mensajes y de partes. No obstante, era importante señalar que los certificados SET no eran certificados de identidad. No autenticaban la identidad de nadie ni podían utilizarse con este fin, tal como se disponía expresamente en la declaración de política relativa a los certificados. Los certificados SET se limitaban a autenticar la relación de una clave pública con un número de cuenta. SET utilizaba tecnología de firmas numéricas para dar una mayor seguridad a la operación, no para identificar a una persona. Además, SET no utilizaba listas de revocación de certificados (“CRL”) para certificados de consumidores o comerciantes. En el contexto del modelo comercial SET, esas listas no eran necesarias. Las operaciones aún tenían que autorizarse a través de la infraestructura existente para los pagos, o sea que la agregación de una nueva CRL de titular de tarjeta no aportaría ningún beneficio y en cambio incrementaría notablemente los gastos de construcción y mantenimiento del sistema.

105. Se afirmó que SET ilustraba: 1) la utilización de firmas numéricas y certificados sin fines de identidad; 2) la emisión de certificados por entidades certificadoras sin licencia y basadas en el mercado; 3) la emisión de certificados en un sistema en que las partes habían definido sus derechos y responsabilidades mediante acuerdo; y 4) en algunos casos, una parte en la que se confiaba (el banco que realizaba el pago sobre la base de la información firmada numéricamente por el consumidor) podía ser el emisor del certificado. SET era sólo un ejemplo de aplicación de la tecnología de firmas numéricas. Se sostuvo que habría muchos más usos en los próximos años y que se basarían en tecnologías y modelos comerciales aún desconocidos.

106. El Grupo de Trabajo expresó su reconocimiento por las presentaciones efectuadas. Se consideró en general que las ilustraciones de las técnicas aplicadas o planeadas eran útiles para comprender mejor las cuestiones jurídicas que debían regularse en el Régimen Uniforme. El Grupo de Trabajo expresó la esperanza de que en el contexto de sus ulteriores períodos de sesiones pudieran efectuarse otras presentaciones sobre la evolución de las firmas numéricas y otras técnicas de autenticación.

CAPÍTULO III. ENTIDADES CERTIFICADORAS Y CUESTIONES CONEXAS

Artículo 7. **Entidad certificadora**

107. El texto del proyecto de artículo 7 que examinó el Grupo de Trabajo era el siguiente:

"1) Para los fines del presente Régimen, por "entidad certificadora" se entenderá:

a) toda persona o entidad licenciada [acreditada] por ... *[el Estado promulgante especifica el órgano o la autoridad competente para conceder licencias a las entidades certificadoras y promulgar reglamentos para su funcionamiento]* para actuar de conformidad con el presente Régimen; o

b) toda persona o entidad que, como parte ordinaria de sus actividades, se dedique a emitir certificados en relación con claves criptográficas utilizadas para firmas numéricas.

[2) Toda entidad certificadora autorizada podrá prestar o facilitar servicios de inscripción registral y de certificación cronológica de la transmisión y recepción de mensajes de datos, así como desempeñar otras funciones respecto de una comunicación protegida por medio de una firma numérica.]"

Párrafo 1)

108. Se expresó la opinión de que el párrafo 1) hacía demasiado hincapié en la situación en que un tercero independiente (a menudo denominado "tercero digno de confianza") desempeñaba la función de entidad certificadora, que no era la única situación imaginable. Se señaló que en la práctica de las firmas numéricas, las partes dependían cada vez más de sistemas de autocertificación (o de certificación mutua) en los que participaban solamente los iniciadores y destinatarios de mensajes firmados numéricamente. Por tanto, debía ampliarse la definición de "entidad certificadora" para que abarcase todo tipo de prácticas. Se sugirió que las palabras "como parte ordinaria de sus actividades", contenidas en el párrafo 1 b), se sustituyeran por "en el curso de sus actividades". Esa sugerencia se consideró generalmente aceptable.

109. Según otra sugerencia, además de la definición de "entidad certificadora", el Grupo de Trabajo tal vez tendría que examinar la definición "entidad de inscripción registral". Si bien no se expresó apoyo a esa sugerencia, en general se estimó que podría ser necesario examinar la cuestión en una etapa ulterior.

110. Otra sugerencia consistía en suprimir el inciso a) dado que se refería solamente a un subconjunto de la categoría que se abordaba en el inciso b) y en sustituir la frase "como parte ordinaria de sus actividades" del párrafo 1 b) por "en el curso de sus actividades" o "en el curso de sus operaciones". A favor de esa sugerencia se afirmó que cualquier referencia a "entidades certificadoras licenciadas" en el Régimen Uniforme podría interpretarse en el sentido de alentar a los Estados promulgantes a establecer sistemas de licencias, lo que podría entrar en conflicto con el "criterio dual" adoptado por el Grupo de Trabajo en su período de sesiones anterior. Se observó asimismo que la supresión del inciso a), a la vez que permitiría mantener la necesaria flexibilidad, concentraría debidamente

el del Régimen Uniforme en la utilización de firmas numéricas para fines de las operaciones comerciales internacionales, por oposición a la utilización de dichas firmas para fines administrativos. No obstante, la opinión que imperó fue que se mantuviera el contenido sustantivo del inciso a). Se afirmó que en ciertos contextos las "actividades" de las entidades certificadoras licenciadas podrían no ser de índole comercial. Además, la distinción entre las entidades certificadoras licenciadas y las entidades certificadoras que actuaban a título puramente privado era justificada a fin de reflejar los distintos regímenes jurídicos que podrían afectar a ambos tipos de entidades certificadoras. Como ejemplo de esa diferencia, se observó que la legislación antimonopolio que podría aplicarse a las entidades certificadoras privadas tal vez no se aplicase a las entidades certificadoras que desempeñaban funciones públicas. Por otra parte, incluso si la categoría abordada en el inciso a) quedase abarcada en la disposición contenida en el inciso b), el inciso a) seguiría teniendo utilidad dado que acomodaría las necesidades de los Estados que estimasen deseable depender de un sistema de licencias, con lo cual se preservaría la neutralidad del Régimen Uniforme.

111. Habida cuenta de las deliberaciones, se decidió que el párrafo 1) volviera a redactarse en los términos siguientes con miras a futuros debates:

> "1) Para los fines del presente Régimen, "por entidad certificadora" se entenderá toda persona o entidad que, en el curso de sus actividades, se dedique a emitir certificados en relación con claves criptográficas utilizadas para firmas numéricas.
>
> 2) El párrafo 1) estará sujeto a toda legislación aplicable que requiera que una entidad certificadora obtenga una licencia, esté acreditada o funcione de determinada manera estipulada en dicha legislación.

Párrafo 2)

112. Se expresaron algunas opiniones a favor de mantener el párrafo 2). Se opinó que las diversas funciones enumeradas en el párrafo 2) debían complementarse haciendo una referencia explícita a otras funciones, como la creación, administración, suspensión y revocación de certificados a fin de ilustrar mejor el vínculo entre los diversos servicios secundarios que ofrecían las entidades certificadoras y el funcionamiento de un sistema de firmas numéricas, que constituía la actividad principal de una entidad certificadora. Sin embargo, la opinión que predominó en general fue que se suprimiese el párrafo 2) y se examinase su contenido en una etapa ulterior para su posible inclusión en una guía para la incorporación al derecho interno, en la eventualidad de que el Grupo de Trabajo decidiera preparar dicha guía.

Artículo 8. **Certificado**

113. El texto del proyecto de artículo 8 examinado por el Grupo de Trabajo era el siguiente:

> "Para los fines del presente Régimen Uniforme, por "certificado" se entenderá un mensaje de datos [u otra constancia] que, por lo menos:
>
> a) identifique la entidad certificadora que lo emita;
>
> b) nombre o identifique a su titular o un dispositivo o agente electrónico bajo control del titular;
>
> c) contenga una clave pública que corresponda a una clave privada bajo el control del titular;
>
> d) especifique su período de vigencia [y las restricciones que haya, si las hay, respecto del ámbito de utilización de la clave pública]; y

e) esté firmado [numéricamente] por la entidad certificadora que lo emita."

Observaciones generales

114. Hubo acuerdo general en que el proyecto de artículo 8 debía dividirse en dos partes, o en dos artículos, a saber, una que contendría una definición general de los certificados que han de ser objeto del Régimen Uniforme y otra en la que se enumeraría el contenido mínimo de tales certificados con arreglo al tenor de los incisos a) a e). Se señaló que un enfoque de esa índole derivaría en una ampliación del alcance del Régimen Uniforme, que sería más limitado si todos los elementos contenidos en el proyecto de artículo 8 formaran parte de la definición de "certificado".

Definición de "certificado"

115. Al principio se convino en que tal vez no fuera procedente el empleo de definiciones técnicas de certificados, ya que era probable que se las sometiera a revisión para tener en cuenta la evolución de las necesidades y las tecnologías. El Grupo de Trabajo procedió a examinar una definición de "certificado", en función de una redacción ajustada al siguiente tenor: "Para los fines del presente Régimen Uniforme, por "certificado" se entenderá un mensaje de datos u otra constancia emitido por una entidad certificadora a los efectos de identificar a una persona o entidad que tiene en su poder una clave privada".

116. Se señaló que una definición de esa índole abarcaba únicamente los certificados de identidad y dejaba fuera del alcance del Régimen Uniforme una variedad de certificados que se utilizaban frecuentemente y que tal vez fuera necesario reconocer. A ese respecto se expresaron opiniones divergentes. Una opinión consistía en que el Régimen Uniforme debía incluir únicamente certificados de identidad. Otra opinión era que también debían incluirse otros tipos de certificados (por ejemplo, certificados de autoridad). Si bien se expresó cierto apoyo a favor de esta opinión, se manifestó la inquietud de que , si se fueran a incluir otros certificados, las disposiciones relativas a las declaraciones hechas por una entidad certificadora, y, en consecuencia, su responsabilidad, tendrían que establecer regímenes jurídicos distintos para abordar los distintos tipos de certificados emitidos, lo que podría desembocar en una tarea excesivamente ambiciosa para el Grupo de Trabajo.

117. Se sugirió que, a fin de abarcar diversos tipos de certificados, se podría preparar una definición general que incluyera todos los tipos de certificados, mientras que el contenido mínimo de cada tipo de certificado se enunciaría en disposiciones subsiguientes. A fin de recoger ese enfoque, se propuso una redacción del siguiente tenor: "Para los fines del presente Régimen Uniforme, por "certificado" se entenderá un mensaje de datos que permita la verificación de un mensaje de datos correspondiente a la clave pública contenida en el certificado". En ese caso, la finalidad de cada tipo de certificado se enunciaría con arreglo al siguiente tenor: "Un certificado de identidad tiene la finalidad de brindar pruebas de la identidad". Alternativamente, se sugirió que, para reflejar la idea de que los certificados pueden desempeñar varias funciones, sería preciso enmendar la definición para aludir a un mensaje de datos "... con la intención de verificar la identidad u otras características importantes de una persona". Se sugirió asimismo que la palabra "verificar", a la que en ocasiones se podría dar un significado técnico concreto, debería ser sustituida por la palaba "confirmar", "acreditar" u otra expresión análoga.

118. El debate se centró en la definición sugerida en último lugar. Se hizo una serie de sugerencias acerca de la formulación exacta de la definición de "certificados de identidad". Una sugerencia fue que se evitase la alusión a otras constancias. En apoyo de esa sugerencia se declaró que la referencia a "constancia" podría plantear problemas de interpretación del inciso a) del artículo 2 de la Ley Modelo. En respuesta, se observó que si se introdujera una referencia de esa índole a "constancia" en el Régimen Uniforme, se contribuiría a evitar que se plantease incertidumbre acerca de si un certificado extendido sobre papel quedaría incluido también en el Régimen Uniforme.

Otra sugerencia fue que, para evitar que se plantearan problemas de interpretación sobre las intenciones subjetivas de las partes, las palabras “a los efectos de identificar” debían sustituirse por las palabras “que identifica”.

119. Se formularon objeciones a la redacción sugerida basándose en que podría crear una situación en que la entidad certificadora podría sustraerse a su responsabilidad al no identificar a la persona a la que se emitiera el certificado. Por lo tanto, debería insertarse una frase del siguiente tenor “con la intención de certificar”. Otra sugerencia fue que la palabra “persona” se sustituyera por la expresión “sujeto”, que era una expresión técnica extensamente utilizada en la práctica y que sería procedente para abordar la situación en la que el sujeto del certificado no fuera una persona sino un “dispositivo o agente electrónico”. Se manifestó oposición a esa sugerencia por los siguientes motivos: que si se utilizara la expresión “sujeto” sería preciso definirla por referencia a una “persona”; que una persona controlaría, en todo caso, el “dispositivo o agente electrónico”; y que la expresión “sujeto” sería incompatible con la terminología utilizada en la Ley Modelo, así como en otros textos de la CNUDMI. Si bien la referencia a una “persona” resultó aceptable, se declaró que debía aclararse que significaba el sujeto de un certificado y se refería también a “entidad”. En lo tocante a la referencia a “entidad”, se convino en que se podría conservar mientras el Grupo de Trabajo tomaba una determinación definitiva acerca de la cuestión de si un “dispositivo o agente electrónico” podría ser sujeto de un certificado. Otra sugerencia fue que la expresión “una clave privada” fuera sustituida por la expresión “un par de claves”.

120. Tras un debate, el Grupo de Trabajo decidió que la definición se reformulara con arreglo al siguiente tenor:

> “Certificado [de identidad]
>
> Para los fines del presente Régimen Uniforme, por “certificado” [de identidad] se entenderá un mensaje de datos u otra constancia emitido por una entidad certificadora con la intención de confirmar la identidad [u otra característica importante] de una persona o entidad que tiene en su poder un determinado par de claves”.

121. Se convino en que la palabra “identidad” y las palabras “otra característica importante” que figuraban entre corchetes permitirían que el Grupo de Trabajo examinase más adelante la cuestión de si deberían incluirse otros tipos de certificados distintos de los certificados de identidad.

Disposición sobre el contenido mínimo de un certificado de identidad

122. Seguidamente, el Grupo de Trabajo dedicó su atención a los incisos a) a e), centrándose en la cuestión de si describían con exactitud el contenido mínimo de un certificado de identidad.

Observaciones generales

123. Hubo acuerdo general en que la finalidad práctica de una disposición en la que se enumerase el contenido mínimo de un certificado era la de establecer los criterios que una entidad certificadora tendría que satisfacer para poder desempeñar sus funciones y evitar la responsabilidad de los perjuicios causados a consecuencia de que la entidad certificadora no incluyera en el certificado todos los elementos necesarios. Se expresó la extendida opinión de que no podía tomarse una decisión definitiva en lo relativo al contenido mínimo de los certificados antes de que se hubiera esclarecido la cuestión de la responsabilidad de la entidad certificadora y la cuestión de los tipos de certificados que habrían de incluirse. El Grupo de Trabajo decidió proseguir con su examen de los incisos a) a e) en el supuesto de que un intercambio preliminar de opiniones podía facilitar la reanudación del debate más adelante.

124. Durante el debate se planteó la cuestión de si un certificado que no cumplía los requisitos mínimos enunciados en el proyecto de artículo 8 podría considerarse inválido o si el proyecto de artículo 8 debería servir de

norma supletoria, con el resultado de que un certificado de esa índole podría ser válido si así lo convenían las partes. En este último caso, se sugirió que se insertara en el proyecto de artículo 8 una norma con arreglo al tenor del párrafo 2) del proyecto de artículo 5.

Encabezamiento

125. Si bien se convino en que un certificado podía emitirse expedido sobre papel, se puso en tela de juicio la procedencia del empleo de la expresión "u otra constancia" (véase el párrafo 6 *supra*).

Inciso a)

126. El contenido del inciso a) resultó ser generalmente aceptable.

Inciso b)

127. Se observó que la utilización de la palabra " titular" planteaba la cuestión de si se refería a la persona a la que se había emitido el certificado o a la persona que tenía en su poder una copia del certificado y que dependía de él. Además, se declaró que la utilización de la expresión "titular" creaba incertidumbre, ya que se utilizaba en el proyecto de artículo 8 para referirse tanto a la persona en cuyo poder obraba el certificado como a la persona poseedora del par de claves pertinentes. Si bien se sugirió que era preferible la utilización de la expresión "sujeto", por las razones antes citadas, el Grupo de Trabajo expresó una preferencia general en favor de la expresión "persona" (véase el párrafo 7 *supra*). No obstante, se decidió que debían mantenerse los términos entre corchetes para un examen ulterior del asunto. En lo tocante a la referencia a un "dispositivo o agente electrónico", de cuyo uso se había afirmado que creaba incertidumbre, se decidió que la expresión se colocara entre corchetes mientras el Grupo de Trabajo examinaba la cuestión con más detalle (véase el párrafo 7 *supra*).

Inciso c)

128. El contenido del inciso c) resultó generalmente aceptable. Por lo que se refiere a la palabra "titular", se decidió que fuera sustituida por las palabras "sujeto" y "persona" entre corchetes (véase el párrafo 15 *supra*).

Inciso d)

129. Hubo acuerdo general en que el período de vigencia era uno de los elementos más esenciales de un certificado. Por lo que se refiere a la referencia al ámbito de utilización de un certificado y a las restricciones que en ese ámbito pudieran existir, se sugirió que debería suprimirse o al menos enmendarse para especificar que el ámbito y sus posibles restricciones, si las hubiere, podrían incorporarse al certificado por remisión. En apoyo de esta sugerencia, se declaró que tal vez fuera imposible incluir en un certificado una lista completa de todas las restricciones. Además, se observó que una referencia de esa índole podría derivar involuntariamente en que la entidad certificadora incurriera en responsabilidad por no haber incluido todas las posibles restricciones en el certificado. Se expresó oposición a esa sugerencia basándose en que el ámbito de utilización y sus posibles restricciones eran elementos críticos a tenor de los cuales se podían evaluar la función de la integridad del certificado. Además, se declaró que en una referencia al ámbito de utilización del certificado y a sus posibles restricciones podría abordase la necesidad de indicar qué certificados podían cumplir varias funciones. Así pues, se sugirió que se incluyera una referencia de esa índole en un nuevo inciso f) entre corchetes para el examen ulterior de la cuestión por el Grupo de Trabajo (véase el párrafo 18 *infra*). Con sujeción a dicho cambio, el Grupo de Trabajo aprobó el contenido del párrafo d).

Inciso e)

130. Si bien hubo acuerdo general en que la firma de la entidad certificadora era uno de los elementos esenciales de un certificado, se expresaron opiniones diferentes acerca de si esa firma tenía que ser numérica. Una opinión afirmó que la firma debería ser numérica para poder garantizar la integridad del certificado. Otra opinión sostuvo que, si la firma de la entidad certificadora fuera criptográfica, las partes que la hacían valer tal vez no podrían determinar que la firma de determinada entidad certificadora era lo que indicaría su intención de obligarse por el certificado. Además, se declaró que, si la firma de la entidad certificadora no era resultado de un procedimiento transparente, el certificado tal vez no fuera válido. El Grupo de Trabajo convino en que existía la necesidad de velar por que la firma de la entidad certificadora fuera segura y por que el proceso fuera transparente. En consecuencia, se decidió mantener la palabra "numéricamente" sin corchetes y que se añadiera la expresión "o hecho seguro por otros medios", con objeto de abordar las inquietudes expresadas respecto a la expresión "numéricamente".

Nuevo inciso f)

131. Se sugirió que se incluyeran los algoritmos aplicados por la entidad certificadora como uno de los elementos mínimo de un certificado. En apoyo de esa sugerencia, se declaró que los algoritmos eran esenciales para garantizar la identificación del firmante y la integridad del mensaje de datos. Se expresó oposición a la sugerencia basándose en que, si fuera necesaria una referencia a los algoritmos pertinentes para que el certificado fuera válido, la entidad certificadora podía sustraerse a la responsabilidad si no se incluían en el certificado. Se declaró que, si bien era necesario para velar por la integridad de los datos, ese resultado podría alcanzarse mejor incluyendo el elemento de integridad de los datos en la definición de la firma numérica. Una opinión contraria fue que, al incluir los algoritmos aplicados en el certificado, la entidad certificadora resultaría responsable por no haber emitido un certificado válido. Tras un debate, el Grupo de Trabajo decidió incluir en el proyecto de artículo 8 una referencia entre corchetes a los algoritmos aplicados para el ulterior examen de la cuestión en un período de sesiones futuro.

Artículo 9. **Declaración sobre prácticas de certificación**

132. El texto del proyecto de artículo 9 que examinó el Grupo de Trabajo era el siguiente:

> "Para los fines del presente Régimen Uniforme, por "declaración sobre prácticas de certificación" se entenderá una declaración publicada por una entidad certificadora en la que se especifiquen las prácticas que la entidad certificadora emplee en la emisión y demás manipulación de certificados."

133. El Grupo de Trabajo observó que el proyecto de artículo 9 se relacionaba con una serie de cuestiones abordadas en otras disposiciones del Régimen Uniforme, por ejemplo, la cuestión de las declaraciones al emitir un certificado (proyecto de artículo 10) y la cuestión de la responsabilidad de la entidad certificadora (proyecto de artículo 12) y decidió aplazar su examen del proyecto de artículo 9 hasta que hubiera terminado su examen del Régimen Uniforme.

Artículo 10. **Declaraciones al emitir un certificado**

134. El texto del proyecto de artículo 10 que examinó el Grupo de Trabajo era el siguiente:

> "Variante A
>
> 1) Al emitir un certificado, la entidad certificadora declara a toda persona que razonablemente se fíe del certificado, o de una firma numérica verificable por la clave pública indicada en él, que:
>
> a) la entidad certificadora ha cumplido con todos los requisitos aplicables a tenor del presente Régimen para la emisión del certificado y, caso de publicar el certificado o de ponerlo por cualquier

otro medio a disposición de alguna persona que razonablemente se fíe de su contenido, declara asimismo que el titular indicado en el certificado [y que sea titular legítimo de la clave privada correspondiente] ha aceptado que así se hiciera;

b) el titular designado en el certificado tiene [legítimamente] en su poder la clave privada correspondiente a la clave pública indicada en el certificado;

c) la clave pública y la clave privada del titular funcionan a modo de juego conjunto;

d) toda la información que figura en el certificado es exacta a la fecha en que se emitió, salvo que la entidad certificadora haya declarado en el certificado [o en otro lugar al que éste remita] que no confirma la exactitud del algún dato determinado; y

e) la entidad certificadora no tiene constancia de que en el certificado se hayan omitido datos sustanciales que, de conocerse, restarían fiabilidad a las declaraciones que anteceden.

2) Sin perjuicio de lo dispuesto en el párrafo 1), la entidad certificadora que emite un certificado declara a cualquier persona que razonablemente se fíe de él o de una firma numérica verificable por la clave pública indicada en el certificado que la entidad certificadora lo ha emitido con arreglo a cualquier declaración sobre prácticas de certificación aplicable [incorporada al certificado por vía de remisión o] de la cual esa persona tenga noticia.

Variante B

1) Al emitir un certificado, la entidad certificadora declara al titular y a toda persona que razonablemente se fíe de la información contenida en el certificado [,de buena fe y] durante su período de vigencia, que:

a) la entidad certificadora ha [procesado][aprobado][emitido] y gestionará y si es necesario revocará, el certificado de acuerdo con:

i) el presente Régimen;

ii) toda otra ley aplicable que rija la emisión del certificado; y

iii) toda declaración sobre prácticas de certificación formulada en el certificado o incorporada a él por vía de remisión, o de la cual esa persona tenga noticia, si la hubiere;

b) la entidad certificadora ha verificado la identidad del titular en la medida indicada en el certificado o en cualquier declaración sobre prácticas de certificación aplicable o, a falta de esa declaración, la ha verificado de manera [fiable][fidedigna];

c) la entidad certificadora ha verificado que la persona que solicita el certificado tiene en su poder la clave privada correspondiente a la clave pública indicada en el certificado;

d) salvo lo expresado en el certificado o en cualquier declaración sobre prácticas de certificación aplicable, por lo que le consta a la entidad certificadora, toda otra información que figure en el certificado es exacta a la fecha en que se emitió;

e) si la entidad certificadora ha publicado el certificado, el titular indicado en el certificado ha aceptado que así se hiciera.

[2) Si una entidad certificadora emitió el certificado con sujeción a las leyes de otra jurisdicción, esa entidad da también las garantías y hace las declaraciones por otra parte aplicables, en su caso, conforme a la ley que rigió su emisión.]"

135. Se sugirió que el título del proyecto de artículo se reformulara en términos como "proceso de emisión de un certificado". Se observó en un comienzo que el proyecto de artículo 10, que establecía una norma respecto de la cual había de medirse el grado de responsabilidad de la entidad certificadora, estaba estrechamente vinculado al proyecto de artículo 12, que preveía la sanción a dicha norma. Sobre la base de la variante A, el debate se centró en determinar si las declaraciones indicadas en los incisos a) a e) del párrafo 1) debían considerarse requisitos obligatorios (es decir, normas mínimas a las que las partes no podían sustraerse por acuerdo mutuo) o como normas "a defecto de otras" o "para llenar lagunas" (es decir, requisitos supletorios que sólo serían vinculantes a falta de un acuerdo en contrario).

136. A favor de que el párrafo 1) tuviese carácter de norma supletoria se afirmó que: se requería una norma flexible para poder acomodar futuros cambios en la tecnología; con imponer a las entidades certificadoras de una norma que estableciera un alto grado de responsabilidad sólo se lograría obstaculizar el desarrollo de la industria, a la vez que se alentaba a las entidades certificadoras menos fiables a entrar en el mercado; la imposición de reglas mínimas para los certificados de garantía relativamente baja podría limitar la utilización mundial de esos certificados en diversos contextos importantes- en general las expectativas del titular del certificado y las partes que se fiaran de él con respecto al contenido del certificado sólo debía determinarse remitiéndose a lo que la entidad certificadora se hubiese comprometido a declarar en el certificado tal como constaba en su declaración sobre prácticas de certificación o de alguna otra manera; con la adopción de reglas mínimas vinculantes para los certificados, el Régimen Uniforme podría quedar al margen de las practicas comerciales seguidas en los grandes mercados. Por consiguiente, la responsabilidad de la entidad certificadora sólo debía determinarse remitiéndose a las obligaciones que la entidad certificadora había aceptado asumir. Se dijo que ese criterio proporcionaría el grado de flexibilidad necesario para abarcar la amplia gama de certificados disponibles en el mercado. Se sugirió el siguiente texto como posible reformulación del proyecto de artículo 10, el cual podría refundirse con el proyecto de artículo 12:

"1) La entidad certificadora indicará explícitamente en el certificado el tipo de servicio que presta. Si la obligación de la entidad certificadora no está expresada en el certificado, se considerará que la entidad certificadora ha garantizado la identidad del titular de la clave.

2) Si una entidad certificadora no ha proporcionado los servicios estipulados en el certificado o ha garantizado la identidad del titular de la clave de manera negligente, será responsable por todo daño causado a la parte que se fió del certificado";

3) Una entidad certificadora podrá limitar su responsabilidad de pagar daños mediante la inclusión de salvedades explícitas en el certificado.

4) El presente artículo se aplicará a reserva de todo acuerdo contrario que exista entre la entidad certificadora y la parte que se haya fiado del certificado."

137. Se rebatió esa propuesta aduciendo que en algunos ordenamientos jurídicos habría incoherencia entre, por una parte, definir los criterios en los que podría basarse el reconocimiento de la condición jurídica de un certificado y, por otra, disponer que podía utilizarse una cláusula general de limitación de la responsabilidad para hacer caso omiso de los criterios esenciales. Se afirmó asimismo que típicamente no existiría una relación contractual entre la

parte confiante y la entidad certificadora. A ese respecto, se expresó la opinión de que podría ser útil aclarar si la noción de "parte confiante" debía abarcar al titular del juego de claves indicado en el certificado. Se opinó además que los certificados podrían tener un tamaño muy reducido, por lo que resultaría difícil incluir "salvedades explícitas" en ellos. Al respecto, se respondió que la fijación de una norma mínima en cuanto a lo que debía considerarse el contenido de un certificado estaba en consonancia con la necesidad de reducir el tamaño del certificado en sí.

138. A favor de mantener el párrafo 1) de la variante A como norma mínima que no debe permitirse que las partes modifiquen mediante un acuerdo privado, se recordó que el Grupo de Trabajo, en su período de sesiones anterior, había adoptado una decisión expresa con respecto a ese particular (A/CN.9/437, párrs. 70 y 71). Además, se indicó que el establecimiento de requisitos mínimos, a la vez que protegía al titular del certificado y a otras partes que se hubiesen fiado de él, también aumentaría la fiabilidad y la aceptabilidad comercial de los mecanismos basados en firmas numéricas, lo que a su vez beneficiaría asimismo a las entidades certificadoras. En respuesta a una objeción en el sentido de que la fijación de una norma mínima impondría considerables obligaciones a las entidades certificadoras, se señaló que el propósito del proyecto de artículo 10 no era imponer obligación alguna a la entidad certificadora sino simplemente definir un régimen jurídico específico para ciertos certificados que, al satisfacer ciertos requisitos, tenían las características necesarias para que se les otorgara una condición jurídica determinada. La entidad certificadora seguiría teniendo libertad para ofrecer certificados de menor calidad, aunque tales certificados no tendrían las mismas consecuencias jurídicas. En general, los partidarios de la adopción de una norma mínima convinieron en que los mecanismos destinados a limitar el grado de responsabilidad con arreglo al proyecto de artículo 12 proporcionarían un equilibrio apropiado con respecto a la aceptación por las entidades certificadoras de requisitos obligatorios conforme al proyecto de artículo 10. Se hizo un paralelo a ese respecto con el régimen de responsabilidad vigente en la industria de transportes marítimos, en la que el libre juego de las fuerzas del mercado históricamente había generado una incertidumbre generalizada de tal magnitud que desalentaba a las partes a entrar en operaciones marítimas, lo que había creado la necesidad de promulgar los primeros instrumentos internacionales en esa esfera, como las Reglas de La Haya.

139. Se sugirió que la limitación del alcance de la disposición mediante la definición de un tipo específico de certificados (por ejemplo, certificados de identidad emitidos para las operaciones de gran valor) a los que se aplicaría el proyecto de artículo 10 podrían hacer más aceptable la formulación de normas obligatorias. Como alternativa, se sugirió que la adopción de una norma obligatoria restringida podría contribuir a hacerla aceptable respecto de una categoría más amplia de certificados. Con miras a combinar esas dos sugerencias, se propuso mantener únicamente los incisos a), d) y e) del párrafo 1) como norma mínima. Si bien en general se apoyó la inclusión de esa propuesta en la continuación del debate, se estimó que habría que proporcionar mayores aclaraciones sobre varias cuestiones.

140. Una de las cuestiones que era necesario aclarar era la categoría exacta de certificados a los que se aplicaría esa norma obligatoria restringida. Según una opinión, la norma restringida debía aplicarse únicamente a una categoría limitada de certificados de identidad que requerían un alto grado de seguridad. Se apoyó la idea de que se requeriría una norma más estricta aún para los certificados a los que se asignase un alto grado de certeza jurídica. En particular, si el certificado tenía por objeto crear una firma jurídicamente vinculante, sería necesario proporcionar mayores seguridades en cuanto al vínculo entre el certificado y la identidad del titular del juego de claves. También se apoyó la opinión de que la norma mínima propuesta era tan restringida que podía hacerse aplicable a una amplia gama de certificados.

141. Otra cuestión que requería mayor aclaración era la coherencia del texto del párrafo 1) propuesto con otras disposiciones del Régimen Uniforme relacionadas con la función de identificación del certificado. Se recordó que, para fines de las firmas numéricas, la función principal del certificado era proporcionar identificación del titular del juego de claves, razón por la cual se había sugerido anteriormente que el Grupo de Trabajo centrase su atención en la noción de certificados de "identidad". Si se adoptase la norma restringida propuesta, la entidad certificadora ya

no haría declaración alguna en cuanto a la identidad del titular sino simplemente garantizaría que se había seguido el proceso definido por la propia entidad certificadora. Si bien se reconoció que ese proceso podría conducir indirectamente a la identificación del titular del juego de claves, se sugirió que podría examinarse más a fondo la posibilidad de mantener el contenido sustantivo de los incisos b) y c), relativos a la identificación directa (o "inequívoca") del titular, en el Régimen Uniforme, posiblemente como parte del proyecto de artículo 2.

142. Si bien se sostuvo que los incisos a), d) y e) fijaban una norma para los certificados de identificación, tras el debate se coincidió en general en que una norma tan limitada podría ser más aplicable a una amplia gama de certificados. También se convino en que debía seguirse examinando de qué forma debía reflejarse la función de identificación, ya fuese en el proyecto de artículo 10 o en una parte anterior del Régimen Uniforme, como función esencial de una categoría más pequeña de certificados, para la cual se requería un mayor grado de fiabilidad jurídica. Se acordó que sería necesario volver a examinar la cuestión en un futuro período de sesiones. Mientras tanto, se decidió mantener los incisos a), d) y c) en el párrafo 1) y poner entre corchetes los incisos b) y c). Se sugirió que tal vez sería necesario poner entre corchetes en el párrafo 1), como alternativa, otro texto extraído del inciso b) del párrafo 1) de la variante B para que el Grupo de Trabajo la examinara en un período de sesiones posterior. Con respecto al inciso d), en general se estimó que la referencia a una posible cláusula de limitación de la responsabilidad por parte de la entidad certificadora en cuanto a la exactitud de la información contenida en el certificado sería aceptable únicamente si los incisos b) y c) quedaran incluidos en el párrafo 1).

143. Con respecto al párrafo 2), hubo acuerdo general en cuanto a mantener el principio de que una entidad certificadora debe respetar los compromisos asumidos en su declaración sobre prácticas de certificación.

144. A fin de reflejar las deliberaciones anteriores, se sugirió la siguiente versión revisada del proyecto de artículo 10:

"Al emitir un certificado, se considerará que:

a) la persona o entidad que emite el certificado ha cumplido todos los requisitos aplicables a tenor del presente Régimen;

[b) en la fecha de emisión del certificado, la clave privada es la clave en poder del titular y corresponde a la clave pública indicada en el certificado;]

[c) la clave pública y la clave privada del titular funcionan a modo de juego conjunto;]

d) toda la información que figura en el certificado es exacta desde la fecha en que se emitió [, salvo que la entidad certificadora haya declarado en el certificado que no confirma la exactitud de algún dato determinado];

e) la entidad certificadora no tiene constancia de que en el certificado se hayan omitido datos sustanciales que, de conocerse, restarían fiabilidad a la información que figura en el certificado; y

[f) si la entidad certificadora ha publicado una declaración sobre prácticas de certificación, el certificado ha sido emitido por la entidad certificadora de conformidad con esa declaración de prácticas de certificación."

145. Tras un debate, el Grupo de Trabajo pidió a la Secretaría que preparara un proyecto de texto revisado del artículo 10, con posibles variantes, a fin de reflejar las deliberaciones anteriores.

Artículo 11. **Responsabilidad contractual**

146. El texto del proyecto de artículo 11 examinado por el Grupo de Trabajo era el siguiente:

> "1) Entre una entidad certificadora que emite un certificado y el titular de ese certificado [o toda otra parte ligada con la entidad certificadora por una relación contractual], el acuerdo celebrado entre ellas determinará los derechos y obligaciones de las partes.
>
> 2) Sin perjuicio de lo dispuesto en el artículo 10, la entidad certificadora podrá, mediante acuerdo, eximirse de la responsabilidad por cualquier pérdida causada por defectos en la información indicada en el certificado, averías técnicas o circunstancias análogas. No obstante, la cláusula que limite o excluya la responsabilidad de la entidad certificadora no podrá ser invocada cuando la exclusión o la limitación de la responsabilidad contractual falte gravemente a la equidad, habida cuenta de la finalidad del contrato.
>
> 3) La entidad certificadora no estará facultada para limitar su responsabilidad cuando se pruebe que la pérdida fue consecuencia de un acto o una omisión de esa autoridad con la intención de causar un daño o temerariamente y con conocimiento de que probablemente se ocasionaría un daño."

147. Se observó que el párrafo 1) reafirmaba el principio de la autonomía de la voluntad de las partes en relación con el régimen de la responsabilidad aplicable a la entidad certificadora. Se observó además que el párrafo 2) trataba de la cuestión de las cláusulas de exención, que en general eran aceptables, con dos excepciones. La primera procedía de una referencia al proyecto de artículo 10, que se proponía fijar una norma mínima de la que no se podía permitir que las entidades certificadoras se apartaran. La segunda excepción se inspiraba en los Principios de UNIDROIT relativos a los contratos mercantiles internacionales (artículo 7.1.6), como un intento de brindar una norma uniforme para evaluar la aceptabilidad de las cláusulas de exención. Además, se observó que el párrafo 3) se ocupaba de la situación en que se produjese una pérdida u otro perjuicio como resultado de un comportamiento incorrecto de la entidad certificadora o de sus representantes (regla inspirada en el artículo 18 de la Ley Modelo de la CNUDMI sobre transferencias internacionales de crédito).

148. El Grupo de Trabajo examinó en primer lugar la cuestión de si debía mantenerse en el Régimen Uniforme el proyecto de artículo 11. Se argumentó que debía suprimirse, ya que trataba de cuestiones que sería más adecuado que estuvieran reguladas por el contrato y la ley aplicable. En particular, se observó que: el párrafo 1) era superfluo, dado que se limitaba a enunciar el principio de la autonomía de la voluntad de las partes, ya tratado en el artículo 4 de la Ley Modelo; y que los párrafos 2) y 3) interferían con la ley nacional en asuntos tal vez no susceptibles de unificación. Además, se señaló que en el proyecto de artículo 10 ya se trataba suficientemente la cuestión. Si bien se estimó que era una opción aceptable dejar que la responsabilidad contractual se rigiera por el contrato y por la ley aplicable fuera del ámbito del Régimen Uniforme, prevaleció el criterio de que merecía la pena intentar lograr un cierto grado de unificación en esta importante cuestión.

149. Sobre el modo de lograr esos resultados se formularon varias sugerencias. Se sugirió mantener el texto actual del proyecto de artículo 11 con el argumento de que, si bien lo dispuesto en el párrafo 1) podía parecer obvio, el párrafo 2) introducía el importantísimo principio de que no podían eludirse las obligaciones fundamentales del contrato con cláusulas de exención. Además, se señaló que el párrafo 3) era esencial y abarcaba no sólo las relaciones contractuales sino también las extracontractuales.

150. Se sugirió también que en el párrafo 1) se dispusiera que las partes no podían acordar condiciones que supusieran una grave falta de equidad, y que se suprimieran los párrafos 2) y 3). Si bien se apoyó la supresión de los párrafos 2) y 3), se formularon diversas objeciones, concretamente que la utilización de la expresión "falta grave de equidad" no era apropiada, ya que era ajena a muchos ordenamientos jurídicos; que la protección de la parte más

débil, que era el objetivo de esas palabras, debía dejarse en manos de otra ley (por ejemplo, la ley de protección del consumidor); y que la supresión de los párrafos 2) y 3) podía dar sin querer a las partes la oportunidad de anular el efecto básico del contrato o de eximirlas de responsabilidad por comportamiento incorrecto.

151. Por otra parte, se sugirió insertar, después de las palabras "obligaciones de las partes" en el párrafo 1), las palabras "y sus eventuales limitaciones, a reserva de lo dispuesto en la ley aplicable", y suprimir los párrafos 2) y 3). Esta sugerencia se justificó argumentando que de este modo el texto contendría una declaración general aceptable basada en la autonomía de las partes y en el derecho aplicable. Sin embargo, se observó que esta enmienda no fomentaría la unificación.

152. Por otra parte, se sugirió sustituir el proyecto de artículo 11 por una disposición en virtud de la cual el límite hasta el que la entidad certificadora habría de ser considerada responsable fuera el límite enunciado en la declaración sobre prácticas de certificación. Esta sugerencia no recibió apoyo por considerarse que sustituiría a la vez al contrato y a las normas mínimas enunciadas en el proyecto de artículo 10 como punto de referencia para evaluar la responsabilidad de la entidad certificadora. Sin embargo, se expresó la opinión de que esa sugerencia podría ser una regla apropiada para los certificados de baja seguridad a los que no serían aplicables las normas mínimas del proyecto de artículo 10.

153. En las deliberaciones se sugirieron una serie de cambios de redacción. Con respecto al párrafo 1), se sostuvo que las palabras que figuraban entre corchetes ("o toda otra parte ligada con la entidad certificadora por una relación contractual") eran demasiado amplias y vagas y se sugirió su sustitución por las palabras "y toda otra parte que confíe en ella". Asimismo, se sugirió que se modificara el párrafo 1) para dejar claro que su finalidad no era supeditar la relación entre las partes exclusivamente al acuerdo entre ellas, ya que de este modo carecería de sentido la excepción al derecho de las partes a convenir en cláusulas de exención de responsabilidad, que figura en los párrafos 2) y 3). Con respecto al párrafo 2), se sugirió que después de la palabra "pérdida" se agregaran las palabras "relacionada con el certificado" y se suprimiera el resto de la primera frase del párrafo 2).

154. En las deliberaciones, el Grupo de Trabajo no logró llegar a un acuerdo sobre la formulación particular del proyecto de artículo 11 y pidió a la Secretaría que preparara opciones que reflejaran las diversas opiniones expresadas, a fin de que pudieran examinarse en un futuro período de sesiones.

Artículo 12. **Responsabilidad de la entidad certificadora frente a las partes que se fían de los certificados**

155. El texto del proyecto de artículo 12 examinado por el Grupo de Trabajo era el siguiente:

> "1) A falta de acuerdo en contrario, la entidad certificadora que emita un certificado responderá ante toda persona que razonablemente se fíe de él por:
>
> a) [incumplimiento de una garantía otorgada conforme al artículo 10] [negligencia al presentar como correcta información incorrecta ofrecida en el certificado];
>
> b) el pronto registro de la revocación de un certificado al recibir el aviso de su revocación; y
>
> c) [las consecuencias de no] [negligencia en] aplicar:
>
> i) un procedimiento expresado en la declaración sobre prácticas de certificación publicada por la entidad certificadora; o

ii) un procedimiento expresado a la ley aplicable.

2) No obstante lo dispuesto en el párrafo 1), la entidad certificadora no será responsable si puede demostrar que ella o sus representantes adoptaron todas las medidas necesarias para evitar errores en el certificado o que les fue imposible adoptarlas.

3) No obstante lo dispuesto en el párrafo 1), la entidad certificadora podrá, en el certificado [o de otra manera], limitar la finalidad para la que se pueda utilizar el certificado. No se tendrá por responsable a la entidad certificadora de los daños y perjuicios derivados de la utilización del certificado con otra finalidad.

4) No obstante lo dispuesto en el párrafo 1), la entidad certificadora podrá, en el certificado [o de otra manera], limitar el valor de las transacciones para las que es válido el certificado. No se tendrá por responsable a la entidad certificadora de los daños y perjuicios que excedan de ese límite."

Observaciones generales

156. Se expresó un amplio apoyo a favor de una disposición que abordara la cuestión de la responsabilidad de las entidades certificadoras respecto de las partes que hacen valer los certificados con arreglo al tenor del proyecto de artículo 12. No obstante, muchos participantes expresaron la opinión de que el alcance de una disposición de esa índole debía limitarse a casos en los que la entidad certificadora garantice la identidad del titular de la clave y la integridad de los mensajes de datos firmados por dicho titular. Un enfoque de esa índole podía facilitar ciertas prácticas en las que se exigieran elevadas normas de seguridad, sin afectar negativamente a otras prácticas en las que esas normas elevadas de seguridad y responsabilidad tal vez no fueran procedentes.

157. Se expresaron algunas dudas, no obstante, acerca de si se podría o debería establecer un régimen de responsabilidad específico. Se declaró que la implantación de un régimen de responsabilidad de esa índole podría obstaculizar la práctica de la certificación si no iba acompañado de una cuantificación razonable de los riesgos concomitantes a la prestación de servicios de certificación, ya que las entidades certificadoras estarían expuestas a riesgos para los que no podrían obtener cobertura de seguro. Además, se observó que tal vez no fuera necesario un régimen de responsabilidad de esa índole, ya que, a falta de un régimen específico, serían aplicables los principios generales del derecho relativo a la responsabilidad extracontractual. Se señaló, no obstante, que en algunas jurisdicciones en que no se había reglamentado específicamente la responsabilidad de las entidades certificadoras, no se tendría a éstas responsables, en principio, frente a las partes que hacían valer los certificados. Además, se dijo que no sería procedente dejar la cuestión en manos de la ley aplicable por varias razones, comprendidas las siguientes: que la incertidumbre reinante en muchas jurisdicciones podría afectar negativamente al desarrollo del comercio electrónico; que la ausencia de responsabilidad podría derivar involuntariamente en que las partes comerciales no pudieran aprovechar los servicios ofrecidos por las entidades certificadoras; y que la determinación del derecho aplicable planteaba cuestiones sumamente difíciles. Por lo que se refiere a la forma de trabajo, se expresó la opinión de que un régimen uniforme de responsabilidad podía aplicarse con mayor eficacia por medio de un convenio o convención que por una ley modelo (véase el párrafo 212 *supra*).

158. Tras un debate, el Grupo de Trabajo decidió que no se escatimaran esfuerzos por abordar la cuestión de la responsabilidad de las entidades certificadoras frente a las partes que se fían de los certificados en el Régimen Uniforme y pasó a examinar el proyecto de artículo 12 detalladamente. Se sugirió que tal vez el Grupo de Trabajo podría incluir en futuras deliberaciones sobre el proyecto de artículo 12 el tema de la naturaleza y la previsibilidad de los daños sufridos por la parte que se fía del certificado.

Párrafo 1)

Encabezamiento

159. Se expresaron diferentes opiniones acerca de si debería mantenerse la primera oración del encabezamiento. Una opinión mantuvo que, si en el proyecto de artículo 10 se establecían reglas mínimas que la entidad certificadora tenía que cumplir, debería suprimirse la primera oración. Otra opinión era que la primera oración era útil, en la medida en que permitía que las partes negociaran su responsabilidad. En respuesta, se declaró que las partes no podían negociar, ya que el proyecto de artículo 12 se ocupaba de la responsabilidad extracontractual en casos en los que, típicamente, no había acuerdo. Se observó, no obstante, que las partes que hacían valer los certificados en sistemas cerrados de comunicación tendrían normalmente algún tipo de acuerdo con las entidades certificadoras. Además, se observó que podrían incorporarse a los contratos entre titulares de claves y partes que hacían valer los certificados condiciones de responsabilidad negociadas entre las entidades certificadoras y los titulares de claves.

160. Prevaleció la opinión de que los casos citados eran excepcionales y no se debería permitir que dieran al traste con la finalidad principal del proyecto de artículo 12, que era la de reglamentar la responsabilidad extracontractual de las entidades certificadoras frente a terceros. Así pues, se sugirió que la necesidad residual de abordar acuerdos en contrario entre las entidades certificadoras y sus clientes o las partes que hacían valer los certificados, siempre que existieran tales acuerdos, podría resolverse incluyendo un texto pertinente al final del proyecto de artículo 12.

Incisos a) a c)

161. Se observó que el segundo grupo de texto entre corchetes en los incisos a) y c) reflejaba al parecer el principio de la responsabilidad estricta y debería ser suprimido. Se expresó la inquietud de que la utilización de la noción de "presentar como correcta información incorrecta", o "declaración falsa", podría dar lugar a incertidumbre, ya que, si bien tenía un significado concreto en algunos ordenamientos jurídicos, era desconocida en otros. Se sugirió la expresión "presentación no veraz".

Párrafo 2)

162. Se expresaron opiniones diferentes acerca de si la carga de la prueba de negligencia debería corresponder a la entidad certificadora o a la parte que hacía valer el certificado. Se opinó que la carga de la prueba debería recaer en la parte que se fiaba del certificado. En apoyo de esa opinión, se afirmó que la parte que hacía valer el certificado podía demostrar negligencia, ya que la prueba acerca de si la entidad certificadora había cumplido el criterio de cuidado enunciado en el proyecto de artículo 10 estaría fácilmente a disposición de esa parte. Además, se señaló que hacer recaer la carga de la prueba en la entidad certificadora sería procedente únicamente si el Grupo de Trabajo hubiera adoptado el principio de la responsabilidad estricta. También se opinó que, si bien la responsabilidad debía basarse en la negligencia, la carga de la prueba debería recaer en la entidad certificadora, ya que toda prueba pertinente estaría bajo control de esa entidad. Se observó que así ocurriría en particular, si el certificado se refería, no a la identidad del titular de la clave, sino al procedimiento aplicado por la entidad certificadora para determinar la identidad de ese titular de la clave.

Párrafos 3) y 4)

163. Contó con apoyo el principio de limitación de la responsabilidad de la entidad certificadora consagrado en los párrafos 3) y 4). No obstante, se expresó la opinión de que los límites de la responsabilidad serían procedentes únicamente en caso de un régimen basado en la responsabilidad estricta de la entidad certificadora, por contraposición a un régimen de responsabilidad basado en la negligencia.

164. Por lo que se refiere a los tipos de límites que se podrían introducir, se declaró que un límite por operación no protegía adecuadamente a las entidades certificadoras, particularmente en el contexto de los certificados de identidad, ya que, con independencia del límite de responsabilidad, se podían utilizar varias veces en un plazo muy corto, sin que hubiera ningún medio de determinar si se había rebasado el límite de responsabilidad. Por lo tanto, se sugirió que en el proyecto de artículo 12 se incluyera una disposición que introdujera un límite global de responsabilidad y que podría rezar con arreglo al siguiente tenor: "La entidad certificadora podrá, en el certificado o de otra manera, implantar un límite de responsabilidad para el período de vigencia de certificado para todos los casos de confianza por la suma de un valor global del certificado. No se tendrá por responsable a la entidad certificadora de los daños y perjuicios que excedan de ese límite global con independencia del número de reclamaciones presentadas contra ese certificado". No obstante, se expresó la opinión de que los límites globales de responsabilidad no podían funcionar, ya que la persona que se fiaba del certificado no tendría medios de saber si se había alcanzado un determinado límite.

Propuestas acerca de un nuevo proyecto de artículo 12

165. Con objeto de abordar las inquietudes expresadas anteriormente, se presentó una serie de propuestas acerca de una formulación alternativa del proyecto de artículo 12. Una propuesta fue que el proyecto de artículo 12 rezara con arreglo al siguiente tenor:

> "1) Cuando una entidad certificadora emita un certificado, responderá ante toda persona que razonablemente se fíe de él, si es negligente [al]:
>
> "a) facilitar información contradictoria en el certificado;
>
> b) no [notificar o] publicar la revocación [o la suspensión] del certificado prontamente en el momento de tener conocimiento de la necesidad de revocarlo [o suspenderlo] [; o
>
> c) no adoptar un procedimiento en una declaración de prácticas de certificación que haya sido publicada por la entidad certificadora y del que tiene conocimiento la persona que se fíe del certificado].
>
> 2) La entidad certificadora podrá declarar en el certificado [o en otro documento] una restricción de la finalidad o finalidades para las que se pueda utilizar el certificado y no se tendrá responsable a la entidad certificadora de los daños y perjuicios derivados del uso del certificado para cualquier otra finalidad.
>
> 3) La entidad certificadora podrá declarar en el certificado [o en otro documento] un límite del valor de las operaciones para las que es válido el certificado y no se tendrá responsable a la entidad certificadora de los daños y perjuicios que excedan de ese límite.
>
> [4) El párrafo 1) del presente artículo no se aplicará si existen condiciones contrarias en un acuerdo entre la entidad certificadora y la persona que se fía del certificado, y en la medida en que esas condiciones existan.]"

166. Se formuló otra propuesta consistente en que se enmendara el proyecto de artículo 12 para que rezara como sigue:

> "1) Salvo que la entidad certificadora demuestre que ella o sus representantes adoptaron todas las medidas razonables para evitar errores en el certificado, será responsable frente a toda persona que razonablemente se fíe de un certificado emitido por esa entidad certificadora por:

[insértense los incisos a) a c)]

2) No obstante lo dispuesto en el párrafo 1), la confianza en un certificado no será razonable en la medida en que sea contraria a la información contenida en el certificado."

167. Si bien es cierto que la primera propuesta fue recibida con cierto interés, el Grupo de Trabajo concentró su debate en la segunda propuesta. Se declaró que el párrafo 1) tenía por finalidad establecer la responsabilidad de errores en el certificado con sujeción al principio de la confianza razonable, evitando toda referencia a las declaraciones y a la negligencia. Además, se observó que el párrafo 2) tenía por objeto permitir que la entidad certificadora enunciara en el certificado las normas con arreglo a las cuales se juzgaría el carácter razonable de la confianza en el certificado. Se explicó que el párrafo 2) no se proponía facilitar una lista exhaustiva de todas las situaciones en las que la confianza en el certificado no sería razonable. Si bien los párrafos 1) y 2) resultaron generalmente aceptables como base para un debate futuro, se expresó una serie de inquietudes y se formularon sugerencias.

Nuevo párrafo 1)

168. Una de las inquietudes manifestadas era que, en la práctica, sería casi imposible que las entidades certificadoras adoptaran "todas las medidas razonables" de forma rentable y sin invertir un tiempo excesivo. Para salir al paso de esa inquietud se formularon varias sugerencias. Una de ellas consistía en que se suprimiera la palabra "todas" y se insertara la palabra "comercialmente" antes de la palabra "razonables". En apoyo de esa sugerencia se declaró que una referencia a "las medidas comercialmente razonables" reflejaría lo que resultaba viable en las circunstancias concretas. Además, se observó que una referencia de esa índole concordaría con la terminología empleada en otros textos de la CNUDMI (por ejemplo, en el inciso a) del párrafo 2) del artículo 5 de la Ley Modelo de la CNUDMI sobre transferencias internacionales de crédito). Se expresó oposición a esa sugerencia basándose en que introduciría incertidumbre, habida cuenta del hecho de que no existía un acuerdo universal de lo que era "comercialmente razonable". Se sugirió por otra parte que simplemente se suprimiera la expresión "todas". También se manifestó oposición contra esa sugerencia basándose en que podría dar lugar inadvertidamente a una disminución improcedente del criterio de cuidado que había de cumplir la entidad certificadora. Asimismo se sugirió que se empleara la redacción utilizada en el inciso a) del párrafo 1) del artículo 7 de la Ley Modelo.

169. Otra inquietud expresada era que el nuevo párrafo 1) no abordaba los errores cometidos por la entidad certificadora al emitir un certificado. Para poder atender a esa inquietud, se sugirió que se añadieran las palabras "o al emitirlo" después de "certificado" en el nuevo párrafo 1). Se declaró que también debía abordarse en el nuevo párrafo 2) la información contenida en una lista de revocación de certificados (LRC) o en una lista análoga.

170. Se convino en que, en tanto se determinaba la cuestión de la función de las declaraciones de prácticas de certificación, el inciso c) se colocara entre corchetes.

Nuevo párrafo 2)

171. Como cuestión de redacción, se sugirió que la primera oración se suprimiera y se insertaran las palabras "con sujeción a lo dispuesto en el párrafo 2)" al principio del nuevo párrafo 1). Se expresó la preocupación de que el nuevo párrafo 2) podría surtir el efecto fortuito de limitar excesivamente los motivos por los que se podría poner en tela de juicio el carácter razonable de la confianza en el certificado. Otra inquietud era que el nuevo párrafo 2) tal vez no preveía una situación en la que tal vez se hiciera valer el certificado en una operación de un valor excesivo, ya que la expresión "información" tal vez no abarcara el valor. Para poder salir al paso de todas esas preocupaciones, se sugirió que los párrafos 3) y 4) del proyecto de artículo 12 se enumeraran como ejemplo de situaciones en las que no sería razonable confiar en el certificado. En el mismo orden de ideas se sugirió que podrían darse otros ejemplos

análogos relativos, por ejemplo, a situaciones en que la entidad certificadora pudiera declarar en el certificado qué partes o tipos de partes designadas pueden hacer valer ese certificado. Además, se sugirió que la entidad certificadora no debería poder hacer valer límites de responsabilidad si la pérdida se derivaba del comportamiento intencionado o temerario de la entidad certificadora.

172. Se expresó además la preocupación de que, al referirse a la información "contenida" en el certificado, el nuevo párrafo 2) podría inadvertidamente tener la consecuencia de aumentar improcedentemente la cantidad de información que sería preciso incluir en el certificado. Para poder atender a esa inquietud, se hizo la sugerencia de que se permitiera incorporar esa información en el certificado por remisión. Se expresó oposición a esa sugerencia basándose en que sería injusto someter los derechos de terceros a condiciones incluidas en un acuerdo entre la entidad certificadora y el titular de la clave, condiciones que puede incluso que no sean fácilmente disponibles para terceros.

173. Tras un debate, el Grupo de Trabajo decidió que el proyecto de artículo 12 se reformulara con arreglo al siguiente tenor:

> "1) A reserva de lo dispuesto en el párrafo 2), salvo que una entidad certificadora demuestre que ella o sus representantes adoptaron [todas] las medidas [razonables] [comercialmente razonables] [que eran procedentes para la finalidad para la que se emitió el certificado, a la luz de todas las circunstancias] para evitar errores en el certificado [o al emitirlo], se la tendrá por responsable ante toda persona que razonablemente se fíe de un certificado emitido por esa entidad certificadora por:
>
> a) errores en el certificado; [o]
>
> b) el pronto registro de la revocación de un certificado al recibir el aviso de su revocación [; o
>
> c) las consecuencias de no aplicar:
>
> i) un procedimiento enunciado en la declaración sobre prácticas de certificación publicada por la entidad certificadora; o
>
> ii) un procedimiento enunciado en la ley aplicable].
>
> 2) La confianza en un certificado no será razonable en la medida en que sea contraria a la información contenida [o incorporada por remisión] en el certificado [o en una lista de revocación] [o en la información sobre la revocación]. [La confianza no será razonable, en particular, cuando:
>
> a) sea contraria a la finalidad para la que se emitió el certificado;
>
> b) exceda del valor para el que es válido el certificado; o
>
> c) [...].]"

Se expresó la opinión de que el proyecto de artículo 12 sólo habría de ser aplicable a las entidades certificadoras que expidan certificados de identificación.

Artículos 13 a 16

174. Por falta de tiempo, el Grupo de Trabajo decidió aplazar su examen de los artículos 13 a 16 del proyecto hasta un futuro período de sesiones. Se expresó la opinión de que esos artículos sólo deberían ser aplicables a las

entidades certificadoras que expiden certificados de identificación. También se sostuvo que el Grupo de Trabajo debería estudiar si el Régimen Uniforme debía aplicarse únicamente a los certificados de identificación o a cualquier otro tipo de certificado.

CAPÍTULO IV. RECONOCIMIENTO DE FIRMAS ELECTRÓNICAS EXTRANJERAS

Artículo 17. **Entidades certificadoras extranjeras que ofrecen servicios conforme al presente Régimen**

175. El texto del proyecto de artículo 17 que examinó el Grupo de Trabajo era el siguiente:

"Variante A 1) Las [personas] [autoridades] extranjeras podrán establecerse como entidades certificadoras locales o prestar servicios de certificación desde otro país sin un establecimiento local si satisfacen las mismas normas objetivas y aplican los mismos procedimientos que las entidades y personas nacionales que puedan convertirse en entidades certificadoras.

2) Variante X La norma formulada en el párrafo 1) no será aplicable a: [...].

Variante Y Podrán hacerse excepciones a la norma formulada en el párrafo 1) en la medida en que lo requiera la seguridad nacional.

Variante B El (La) ... *[el Estado promulgante designa el órgano o la autoridad competente para reglamentar la aprobación de certificados extranjeros]* queda autorizada para aprobar certificados extranjeros y dictar normas concretas por las que se rija dicha aprobación."

Observaciones generales

176. Con respecto al título del capítulo IV, se observó que la referencia al reconocimiento de firmas electrónicas extranjeras no era apropiada dado que el capítulo versaba sobre la prestación de servicios por entidades certificadoras extranjeras (en particular, el proyecto de artículo 17), la homologación de certificados extranjeros por entidades certificadoras nacionales (en particular, el proyecto de artículo 18) y el reconocimiento de certificados extranjeros por entidades certificadoras nacionales (en particular, el proyecto de artículo 19). El Grupo de Trabajo examinó brevemente varias sugerencias tendientes a reflejar más claramente en el encabezamiento del capítulo el tema tratado en éste (por ejemplo, "reconocimiento transfronterizo de certificados", "reconocimiento de firmas electrónicas y certificados", "reconocimiento de entidades certificadoras y certificados extranjeros"). No obstante, se acordó en general que el examen de un encabezamiento apropiado para el capítulo IV debía aplazarse hasta que el Grupo de Trabajo hubiese analizado más detalladamente los efectos jurídicos de los certificados.

177. Con respecto a las dos variantes propuestas en el proyecto de artículo 17, se estimó en general que la variante B, conforme a la cual un determinado órgano del Estado promulgante se encargaría de establecer normas para la aprobación de los certificados extranjeros, no proporcionaba una base apropiada para la elaboración de un régimen uniforme. Se acordó que el Grupo de Trabajo suprimiera la variante B y centrara sus deliberaciones en la variante A.

Ámbito de aplicación del proyecto de artículo 17

178. Se señaló que los objetivos del proyecto de artículo 17 eran duales: en primer lugar, reconocía el derecho de las entidades certificadoras extranjeras a establecerse localmente con arreglo a las condiciones estipuladas en el proyecto de artículo; en segundo lugar, otorgaba a las entidades certificadoras extranjeras derecho a prestar servicios en el Estado promulgante sin tener un establecimiento local. Como tal, el proyecto de artículo 17 abordaba cuestiones de política comercial, concretamente la medida en que el Estado promulgante dejaría sin efecto toda restricción respecto del establecimiento de entidades certificadoras extranjeras y de la prestación de servicios por éstas. Se sugirió que el Grupo de Trabajo tratase en cambio de centrar su labor en la elaboración de disposiciones modelo sobre los efectos jurídicos de los certificados extranjeros y la relación entre los titulares de certificados y las entidades certificadoras. Hubo varias intervenciones a favor de esa opinión. Se estimó que las cuestiones relativas a la política comercial competían a otros foros y que no sería aconsejable abordarlas en el Régimen Uniforme.

179. En respuesta a esas opiniones se observó que, al permitir que entidades extranjeras se establecieran como entidades certificadoras, el proyecto de artículo 17 simplemente afirmaba el principio de que no debía existir discriminación alguna contra las entidades extranjeras, siempre y cuando satisficieran las normas aplicables a las entidades certificadoras nacionales. Se consideró que ese principio era especialmente pertinente con respecto a las entidades certificadoras, dado que podría esperarse que éstas funcionaran sin tener necesariamente un establecimiento físico u otro local para la prestación de servicios en el país en que realizaban sus actividades. Se afirmó asimismo que la propia Ley Modelo abordaba una serie de asuntos de carácter transfronterizo que podrían considerarse susceptibles de plantear cuestiones de política comercial.

180. Habiendo escuchado las diversas opiniones expresadas, y a fin de llevar adelante su examen del Régimen Uniforme, el Grupo de Trabajo pasó a examinar varias enmiendas al proyecto de artículo 17, sin perjuicio de las reservas que se habían formulado en relación con el contenido sustantivo del proyecto de artículo 17.

Párrafo 1)

181. Se preguntó si el párrafo 1) abarcaba sólo el reconocimiento de las entidades certificadoras que funcionaban conforme a una aprobación emitida por un órgano u organismo gubernamental del Estado extranjero. En respuesta a esa pregunta se observó que, en su formulación actual, el párrafo 1) no abordaba la cuestión de si las entidades certificadoras estaban sujetas a aprobación gubernamental en el Estado extranjero. No obstante, también opinó que una disposición como el proyecto de artículo 17 había de basarse en un régimen de licencias con arreglo a requisitos legislativos.

182. Se expresó la opinión de que algunas de las dificultades que había suscitado el párrafo 1) se debían a que la disposición parecía hacer demasiado hincapié en el reconocimiento de las entidades certificadoras propiamente tales y no en la capacidad de las entidades certificadoras de emitir certificados que se utilizarían en el Estado promulgante. Además, la frase “satisfacen las mismas normas objetivas y aplican los mismos procedimientos que las entidades y personas nacionales que puedan convertirse en entidades certificadoras”, podría constituir un obstáculo para la aplicación de nuevas tecnologías, pues se estimaba que la disposición podía interpretarse en el sentido de que proporcionaba una justificación para prohibir el reconocimiento de entidades certificadoras extranjeras que aplicaran procedimientos tecnológicamente más avanzados que los que se utilizaban en el Estado promulgante. En lugar de la formulación actual, se sugirió que sería preferible a hacer referencia a “requisitos objetivos” que habían de satisfacer las entidades certificadoras en el Estado promulgante. Como alternativa, se sugirió poner entre corchetes las palabras “y aplican los mismos procedimientos”.

183. En relación con las condiciones que han de satisfacer las entidades certificadoras extranjeras, se observó que el propósito del proyecto de párrafo 1) era garantizar que esas condiciones fuesen esencialmente las mismas que se aplicaban a las entidades certificadoras nacionales. Por tanto, se propuso reformular el párrafo 1) a los efectos de que el reconocimiento de las entidades certificadoras extranjeras estuviese sujeto a las leyes del Estado

promulgante. El Grupo de Trabajo podía examinar en una etapa ulterior las cuestiones relativas a la definición de las normas que habían de satisfacer la entidades certificadoras extranjeras. Esa enmienda permitiría aclarar además que el reconocimiento también estaba sujeto a toda exclusión vigente en el Estado promulgante, lo que haría innecesarias ambas variantes del párrafo 2). Se propuso el texto siguiente:

> "A reserva de lo dispuesto en las leyes del Estado promulgante, las [personas] [entidades] extranjeras podrán:
>
> a) establecerse como entidades certificadoras locales; o
>
> b) prestar servicios de certificación sin un establecimiento local si satisfacen las mismas normas objetivas y aplican los mismos procedimientos que las entidades y personas nacionales que puedan convertirse en entidades certificadoras."

184. En respuesta a esa propuesta, se afirmó que la referencia a la legislación nacional no era una solución satisfactoria, dado que las leyes del Estado promulgante podrían contener disposiciones discriminatorias susceptibles de menoscabar el espíritu del proyecto de artículo 17. Además, la enmienda propuesta suscitaba preguntas en cuanto a quién en el Estado promulgante determinaría que la entidad certificadora extranjera satisfacía las normas objetivas y aplicaba los mismos procedimientos que las entidades y personas nacionales y por qué medios se haría tal determinación.

185. Se expresó la opinión de que, en su formulación actual, el párrafo 1) parecía sugerir que las entidades certificadoras extranjeras debían no sólo estar aprobadas con arreglo a su propia legislación, sino además satisfacer los requisitos del Estado promulgante. Se estimó que esa regla podría tener efectos restrictivos indeseables y no contribuiría a promover el comercio electrónico. En relación con esta última observación, se sugirió que el significado del párrafo 1) podría aclararse si el texto se reformulaba como regla de no discriminación en los términos siguientes:

> "1) No se negará a las [personas] [entidades] extranjeras el derecho a establecerse localmente o a prestar servicios de certificación únicamente por el solo hecho de que sean extranjeras si satisfacen las mismas normas objetivas y aplican los mismos procedimientos que las entidades o personas nacionales que puedan convertirse en entidades certificadoras."

186. Se objetó esa propuesta aduciendo que la regla de no discriminación propuesta suscitaba el mismo tipo de preocupaciones generales que se habían expresado en las observaciones generales con respecto al ámbito de aplicación del proyecto de artículo 17 (véanse los párrafos 178 a 180 *supra*).

187. Habiendo examinado las diversas propuestas, y teniendo en cuenta las diferentes opiniones expresadas, el Grupo de Trabajo estimó que se necesitaba más tiempo para celebrar consultas sobre las cuestiones tratadas en relación con el párrafo 1). Se pidió a la Secretaría que propusiera una versión revisada del párrafo 1), con posibles variantes que reflejaran las deliberaciones anteriores, para que el Grupo de Trabajo la examinara en una etapa ulterior.

Párrafo 2)

188. En relación con las dos variantes de exclusiones propuestas en el párrafo 2), se expresó la opinión de que la variante X debería suprimirse, ya que podría proporcionar un mecanismo abierto para limitar el alcance del párrafo 1). Según esa opinión, si había de permitirse alguna exclusión, debía ser únicamente por motivos de seguridad nacional, como estipulaba la variante Y. Sin embargo, en general se expresó preferencia por mantener la variante

X, según la cual correspondería al Estado promulgante formular las excepciones a la regla general enunciada en el párrafo 1). Si bien la variante Y tenía el mérito de limitar toda posible exclusión a las relacionadas con la seguridad nacional, se estimó que los Estados tal vez deseasen incluir en su legislación otros posibles motivos de exclusión por consideraciones de orden público. Tras el debate, se decidió mantener ambas variantes entre corchetes para volverlas a examinar ulteriormente.

Artículo 18. **Homologación de certificados extranjeros por entidades certificadoras nacionales**

189. El texto del proyecto de artículo 18 examinado por el Grupo de Trabajo era el siguiente:

> "Los certificados emitidos por entidades certificadoras extranjeras podrán ser utilizados para los fines de una firma numérica en las mismas condiciones que los certificados sujetos al presente Régimen, de ser reconocidos por una entidad certificadora nacional que funcione conforme a .... *[la ley del Estado promulgante]*, y de garantizar esta autoridad, en la misma medida que respecto de sus propios certificados, la regularidad de los detalles del certificado, así como su validez y vigencia".

190. Como observación general se dijo que la inclusión de disposiciones relativas a la cuestión del reconocimiento recíproco transfronterizo suponía un notable avance para reforzar la fiabilidad de los certificados. Se señaló que en la práctica comercial se utilizaban cada vez más los certificados y que podría fomentarse la confianza en esta nueva tecnología mediante la adhesión a las normas internacionales. Se invitó al Grupo de Trabajo a que examinase los mecanismos internacionales de acreditación de las entidades certificadoras que se utilizaban conforme a las normas internacionales. Se apoyó la idea de incluir el tema propuesto entre las cuestiones que el Grupo de Trabajo debatiría ulteriormente. No obstante, se señaló que el tema propuesto no estaba relacionado únicamente con las cuestiones que se planteaban en el proyecto de artículo 18, y que el Grupo de Trabajo podría examinarlas, por ejemplo, cuando reanudase el examen de la cuestión del registro de los certificados.

191. En cuanto al proyecto de artículo 18, se señaló que el objetivo de la disposición que contenía era simplemente permitir a la entidad nacional certificadora que garantizase, en la misma medida que respecto de sus propios certificados, la veracidad de los detalles del certificado extranjero, así como su validez y vigencia. En virtud del proyecto de artículo 18, la responsabilidad en el supuesto de que el certificado extranjero se juzgara defectuoso correspondía a la entidad nacional certificadora que concedía dicha garantía. No obstante, la existencia de una garantía conforme al proyecto de artículo 18 no era una condición necesaria para el reconocimiento de un certificado emitido por entidades certificadoras extranjeras que, por lo demás, cumplían las condiciones establecidas en el proyecto de artículo 19. Puesto que la presentación de una garantía conforme al proyecto de artículo 18 era simplemente voluntaria, se sostuvo que el proyecto de artículo 18 no era necesario y podía suprimirse. Se sugirió asimismo que el Régimen Uniforme debería permitir que el Estado promulgante decidiera si las entidades certificadoras nacionales podían otorgar dicha garantía con respecto a los certificados emitidos por entidades certificadoras extranjeras, y en qué condiciones. Podría hacerse referencia a la concesión de garantías del tipo recogido en el proyecto de artículo 18 en una guía para la incorporación al derecho interno o en notas explicativas adjuntas, dependiendo de la naturaleza del instrumento que finalmente se aprobase.

192. Se recordaron al Grupo de Trabajo debates anteriores, celebrados durante su 31º período de sesiones, acerca de los diferentes grados de fiabilidad que podía proporcionar una entidad certificadora nacional con respecto a una extranjera, que oscilaban desde el nivel máximo, en el que la entidad certificadora nacional, a petición de la parte que invocara un certificado extranjero, garantizaría el contenido de ese certificado de acuerdo con su conocimiento declarado de los procedimientos que hubieran llevado a la expedición del certificado, asumiendo así plena responsabilidad por los errores u otras irregularidades del certificado, hasta el nivel más bajo de fiabilidad, en que la entidad certificadora nacional sólo garantizaría la identidad de la entidad certificadora extranjera, basada en la verificación de su clave pública y de su firma numérica (véase A/CN.9/437, párrs. 81 y 82). Se sostuvo que esos

diferentes niveles de fiabilidad no se reflejaban de forma adecuada en el proyecto de artículo 18 y que, si se mantenía la disposición, debería quedar claro que no excluía más acuerdo que una plena garantía de la regularidad y validez de un certificado emitido por una entidad certificadora extranjera.

193. En respuesta a esas observaciones se dijo que el proyecto de artículo 18 era de utilidad, ya que permitía la circulación y la utilización recíproca de certificados sin necesidad de acuerdos internacionales bilaterales ni multilaterales en materia de reconocimiento de certificados que algunos Estados podrían considerar necesarios para conceder el reconocimiento conforme al proyecto de artículo 19. Además, a la vista de la decisión adoptada por el Grupo de Trabajo de incluir en el Régimen Uniforme no sólo a las entidades certificadoras titulares de licencias concedidas por organismos públicos sino también a las entidades certificadoras que actuasen fuera sistema de oficial de concesión de licencias (véase A/CN.9/437, párrs. 48 a 50), el proyecto de artículo 18 contaba con la ventaja adicional de permitir una solución comercial para aquellas situaciones en las que el reconocimiento conforme al proyecto de artículo 19 no se concedería automáticamente. En relación con ese punto, se sugirió que el alcance del proyecto de artículo 18 quedaría más claro con la siguiente redacción:

> "Los certificados emitidos por entidades certificadoras extranjeras podrán ser utilizados para los fines de una firma numérica en las mismas condiciones que los certificados sujetos al presente Régimen siempre que exista la correspondiente garantía emitida por una entidad certificadora que funcione conforme a ... *[la ley del Estado promulgante]*."

194. Hubo manifestaciones a favor de mantener en el Régimen Uniforme una disposición que autorizase a una entidad certificadora nacional a otorgar garantías a certificados emitidos por entidades certificadoras extranjeras. Dicha disposición podría basarse en el proyecto de artículo 18, teniendo en cuenta las propuestas formuladas en el Grupo de Trabajo. No obstante, se sugirió que era inadecuada la inclusión actual del proyecto de artículo 18 en el capítulo IV, ya que dicha disposición no se refería al reconocimiento de certificados emitidos en el extranjero.

195. Tras el debate, el Grupo de Trabajo acordó mantener el proyecto de artículo 18 entre corchetes, con las enmiendas propuestas, y pidió a la Secretaría que preparase otras versiones de dicha disposición que tuvieran en cuenta las opiniones expresadas, para ser examinadas más adelante por el Grupo de Trabajo.

Artículo 19. **Reconocimiento de certificados extranjeros por entidades certificadoras nacionales**

196. El texto del proyecto de artículo 19 examinado por el Grupo de Trabajo era el siguiente:

> "1) Los certificados emitidos por una entidad certificadora extranjera se reconocerán como jurídicamente equivalentes a los emitidos por las entidades certificadoras que funcionen conforme a *[la ley del Estado promulgante]* cuando las prácticas de la autoridad extranjera ofrezcan un grado de fiabilidad por lo menos equivalente al requerido de las entidades certificadoras de conformidad con el presente Régimen. [Ese reconocimiento podrá hacerse mediante una determinación publicada del Estado o mediante un acuerdo bilateral o multilateral entre los Estados interesados.]
>
> 2) Las firmas y las constancias que cumplan con las leyes de otro Estado relativas a las firmas numéricas u otras firmas electrónicas se reconocerán como jurídicamente equivalentes a las firmas y constancias que cumplen con el presente Régimen cuando las leyes del otro Estado requieran un grado de fiabilidad por lo menos equivalente al requerido para esas constancias y firmas conforme a ... *[la ley del Estado promulgante]*. [Ese reconocimiento podrá hacerse mediante una determinación publicada del Estado o mediante un acuerdo bilateral o multilateral entre los Estados interesados.]

3) Se admitirá [por parte de los tribunales y otras autoridades encargadas de averiguar los hechos] la eficacia de las firmas numéricas verificadas con referencia a un certificado emitido por una entidad certificadora extranjera cuando el certificado sea tan fiable como corresponda a la finalidad para la cual se emitió el certificado, a la luz de todas las circunstancias.

4) Sin perjuicio de lo dispuesto en el párrafo anterior, los órganos públicos podrán hacer constar [mediante publicación] que se debe autorizar una entidad certificadora, una clase de entidades certificadoras o una clase de certificados en relación con los mensajes o las firmas presentados a esos órganos."

Párrafos 1) y 2)

197. Se señaló que los párrafos 1) y 2) se referían a la forma en la que debía establecerse la fiabilidad de los certificados y firmas extranjeros previamente a la realización de cualquier operación (y de cualquier controversia que surgiera con respecto al grado de fiabilidad de la firma). A ese fin, los párrafos 1) y 2) establecían las pruebas que podían realizarse en el Estado promulgante para reconocer los certificados emitidos por las entidades certificadoras extranjeras, así como las firmas y constancias que cumplían con la legislación de otro Estado.

198. Se plantearon varias cuestiones relativas al alcance del reconocimiento conforme a los párrafos 1) y 2). Con respecto al párrafo 1), se expresó la opinión de que no quedaba suficientemente clara la noción de equivalencia jurídica entre certificados emitidos por entidades certificadoras extranjeras y certificados emitidos por entidades certificadoras que actuasen conforme a las disposiciones del Estado promulgante. Se indicó que el término "reconocimiento", en el sentido generalmente utilizado en derecho internacional privado, suponía la concesión de efectos jurídicos a actos realizados en otra jurisdicción. No obstante, dicha noción no era aplicable en el contexto del párrafo 1), ya que un certificado era un instrumento que recogía declaraciones de hecho que cumplían meramente una función declarativa. Además, tanto en el párrafo 1) como en el párrafo 2) se sobreentendía que el Estado promulgante debería aplicar su propia legislación para asegurarse de la fiabilidad de los certificados emitidos por entidades certificadoras extranjeras, así como de que las firmas y constancias se adecuaban a la legislación del otro Estado. Por tanto, se dijo que los párrafos 1) y 2) no se correspondían con los principios generales del derecho internacional privado según los cuales la validez de los actos realizados en el extranjero tenía que establecerse de acuerdo con el derecho aplicable en la jurisdicción en la que se habían realizado. Se señaló además que el artículo 13 de la Ley Modelo y los proyectos de artículo 3 y 5 del Régimen Uniforme ya establecían normas para la atribución de mensajes de datos y para la verificación de la fiabilidad de una firma electrónica.

199. En respuesta a esas observaciones, se señaló que los párrafos 1) y 2) eran de utilidad en relación con los regímenes normativos nacionales que exigían la utilización de tipos específicos de certificados que proporcionaban un alto nivel de fiabilidad para la realización de determinadas operaciones. En los Estados promulgantes que contaban con dichos regímenes normativos, el párrafo 1) establecía las normas mínimas de reconocimiento de certificados emitidos por entidades certificadoras extranjeras que se utilizaban en relación con operaciones que no fueran aquellas para las que se exigía una clase determinada de certificados. Por la misma razón, el párrafo 2) proporcionaba a esos Estados promulgantes una norma supletoria que establecía una presunción de validez de las firmas y constancias que cumplían con la legislación de otro Estado que se consideraba que proporcionaban un grado de seguridad razonable para todas aquellas situaciones en las que no se exigían mayores requisitos conforme a la legislación del Estado promulgante. Se instó al Grupo de Trabajo a que no dejase que la cuestión de las normas mínimas aplicables a un certificado extranjero se determinase totalmente conforme a las normas del Estado promulgante en materia de conflictos de leyes.

200. El Grupo de Trabajo debatió posibles enmiendas de los párrafos 1) y 2) con miras a tener en cuenta las inquietudes expresadas. Se sugirió en particular que los párrafos 1) y 2) podrían reagruparse y volverse a redactar como una disposición no discriminatoria en los siguientes términos:

> "No podrá privarse a los certificados emitidos por entidades certificadoras extranjeras del mismo reconocimiento que los certificados emitidos por entidades certificadoras nacionales en razón de haber sido emitidos por entidades certificadoras extranjeras".

201. No obstante, se hicieron objeciones a la formulación negativa propuesta, ya que no establecía las normas conforme a las que debía concederse el reconocimiento. Asimismo se señaló que la disposición no discriminatoria propuesta podría dar lugar a las mismas reservas que se plantearon en relación con el proyecto de artículo 17 (véanse los párrafos 185 y 186 *supra*).

202. Tras el debate, la opinión general fue que sería deseable formular una disposición sustantiva que recogiese un método para establecer la fiabilidad de las firmas y los certificados extranjeros antes de cualquier operación. Se pidió a la Secretaría que preparase una versión revisada de los párrafos 1) y 2), incluyendo una que unificase ambos párrafos, con posibles variantes que tuvieran en cuenta las opiniones expresadas.

Párrafo 3)

203. Se señaló que la finalidad del párrafo 3) era establecer el criterio conforme al que podrían comprobarse las firmas y certificados extranjeros en ausencia de cualquier determinación previa de su fiabilidad. No obstante, se sugirió que, conforme a la formulación actual, la disposición podía no ser necesaria, ya que se limitaba a reformular el principio de que, en caso de que surgiese una controversia acerca de la autenticidad de una firma y de la fiabilidad de un certificado emitido por una entidad certificadora extranjera, los tribunales del Estado promulgante tenían que conceder a dicha firma o a dicho certificado la importancia probatoria que considerasen adecuada en esas circunstancias.

204. En respuesta a esas observaciones se señaló que el párrafo 3), inspirado en el artículo 7 de la Ley Modelo, proporcionaba una orientación útil para los tribunales del Estado promulgante a la hora de evaluar la fiabilidad de un certificado extranjero. Era conveniente destacar ese importante principio en el Régimen Uniforme teniendo en cuenta que el Estado que aprobase el Régimen Uniforme podía no haber incorporado necesariamente en su derecho interno el artículo 7 de la Ley Modelo. Con el objetivo de que su finalidad quedase más clara, se propuso que el párrafo 3) volviese a formularse de la siguiente forma:

> "No se privará de su eficacia [por parte de los tribunales y otras autoridades encargadas de averiguar los hechos] a las firmas numéricas verificadas con referencia a un certificado emitido por una entidad certificadora extranjera cuando el certificado sea tan fiable como corresponda a la finalidad para la cual se emitió el certificado, a la luz de todas las circunstancias."

205. Tras el debate, el Grupo de Trabajo decidió que debía mantenerse el contenido del párrafo 3) para que el Grupo de Trabajo lo examinase ulteriormente.

Párrafo 4)

206. Se formularon preguntas acerca de la necesidad de una disposición como la del párrafo 4), que recogía el derecho de los órganos públicos a determinar los procedimientos que debían utilizarse en la comunicación electrónica con ellos. Por una parte, se expresó la inquietud de que el párrafo 4) pudiera tener consecuencias restrictivas no deseadas y pudiera interpretarse en el sentido de que aquellas personas o entidades que no fuesen órganos públicos no tenían derecho a elegir la entidad certificadora, la clase de entidades certificadoras ni la clase de certificados que deseaban utilizar específicamente para los mensajes o firmas que recibieran. Se consideró que dicha situación no sería coherente con el principio de autonomía de la voluntad de las partes consagrado en varias disposiciones de Ley Modelo. Por otra parte, si la finalidad del párrafo 4) era establecer una prerrogativa especial para los órganos

públicos, tal vez fuera necesario perfeccionar de la disposición, puesto que podría interpretarse en el sentido de que, en caso de que un órgano público no indicase claramente la entidad certificadora, la clase de entidad certificadora o la clase de certificado que deseaba utilizar específicamente para los mensajes o las firmas que le presentasen, el órgano público tenía la obligación de aceptar cualquier clase de certificado o entidad certificadora.

207. La opinión general fue que debía reconocerse a las partes en las operaciones, comerciales o de otro tipo, y no únicamente a los órganos públicos, el derecho a elegir la entidad certificadora, la clase de entidad certificadora o la clase de certificado que desearan utilizar específicamente para los mensajes o firmas que recibieran. El Grupo de Trabajo pidió a la Secretaría que volviese a formular el párrafo 4) con el fin de reflejar dicha idea y decidió estudiar con posterioridad el lugar adecuado para la disposición una vez revisada.

IV. COORDINACIÓN DE LOS TRABAJOS

208. El Grupo de Trabajo oyó declaraciones relativas a la labor realizada por la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) y por la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD) en el ámbito del comercio electrónico.

209. Se dijo que, en su 29ª Conferencia General, la UNESCO había recibido el mandato de iniciar los preparativos de un instrumento jurídico internacional relativo a la utilización del ciberespacio. En relación con ese punto, se expresó la opinión de que era necesario que la UNESCO y la CNUDMI aunaran esfuerzos en el ámbito del comercio electrónico. Se señaló que dicha labor debería estar guiada por la necesidad de fomentar el comercio electrónico de forma que beneficiara tanto a los países desarrollados como a los países en desarrollo y que, al mismo tiempo, garantizara los derechos humanos fundamentales, incluido el derecho a la intimidad. Se subrayó que las cuestiones de la atribución de mensajes de datos al iniciador, la integridad de los mensajes de datos y la responsabilidad de las partes que participan en el comercio electrónico deberían constituir el centro de la labor del Grupo de Trabajo sobre firmas numéricas y otras firmas electrónicas.

210. En una declaración relativa a la labor de la UNCTAD, se señaló que se había establecido la *"Global Trade Point Network"* con el fin de prestar asistencia a los países en desarrollo en sus intentos por aprovechar los avances realizados en el ámbito de las comunicaciones electrónicas. Además, se anunció que la UNCTAD estaba organizando una exposición de fabricantes de equipo, creadores de programas informáticos y empresas de servicios en el ámbito del comercio electrónico (Lyon, 8 a 13 de noviembre de 1998) y que la exposición incluiría una serie de presentaciones sobre una amplia gama de temas relacionados con el comercio electrónico.

211. El Grupo de Trabajo tomó nota de las declaraciones y acogió con satisfacción la participación de organizaciones interesadas en su labor. Se pidió a la Secretaría que continuase supervisando los avances de otras organizaciones internacionales en cuestiones jurídicas del comercio electrónico y que informase al Grupo de Trabajo de dichos avances.

V. LABOR FUTURA

212. Al término del período de sesiones, se hizo una propuesta en el sentido de que el Grupo de Trabajo tal vez deseara examinar de forma preliminar la posibilidad de iniciar los preparativos de una convención internacional sobre la base de las disposiciones de la Ley Modelo y del Régimen Uniforme. Se acordó que podía ser necesario incluir esta cuestión como tema del programa en el próximo período de sesiones del Grupo de Trabajo tomando como base propuestas más detalladas que pudieran realizar las delegaciones interesadas. No obstante, la conclusión preliminar del Grupo de Trabajo fue que los preparativos de una convención deberían considerarse en cualquier caso como un proyecto independiente tanto de los preparativos del Régimen Uniforme como de cualquier otro texto que pudiera agregarse a la Ley Modelo. Hasta que se adoptara una decisión definitiva acerca de la forma del Régimen Uniforme,

la sugerencia de preparar una convención en una etapa posterior no debería apartar al Grupo de Trabajo de su labor actual, que era ante todo la preparación de un proyecto de Régimen Uniforme sobre firmas numéricas y otras firmas electrónicas, ni de su hipótesis de trabajo actual de que el Régimen Uniforme revestiría la forma la de un proyecto de disposiciones legislativas. Se consideró en general que la posible preparación de un proyecto de convención no debería utilizarse como un medio para volver a plantear cuestiones ya resueltas en la Ley Modelo, lo cual podría frenar la creciente utilización de tan fructífero instrumento.

213. Se indicó que estaba previsto que el próximo período de sesiones del Grupo de Trabajo se celebrara en Nueva York del 29 de junio al 10 de julio de 1998, fechas que estaban pendientes de confirmación por la Comisión en su 32º período de sesiones (Nueva York, 1º a 12 de junio de 1998).

Notas

[1] *Documentos Oficiales de la Asamblea General, quincuagésimo primer período de sesiones, Suplemento Nº 17* (A/51/17), párrs. 223 y 224.

[2] *Ibid.,quincuagésimo segundo período de sesiones, Suplemento Nº 17* (A/52/17), párrs. 249 a 251.