 DOI: *https://doij.org/10.10000/IJLMH.111265*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 4

2021

Improving Albania's Internet Law to Achieve Growth in E-Commerce: Paving the Way Toward Membership in the European Union

STEPHEN ERROL BLYTHE[1]

ABSTRACT

In the digital age, the E-signature has replaced the handwritten signature. Since 1995, there have been three generations of E-signature law: the first mandated use of the digital signature, the second recognized the legal validity of all types of E-signatures, and the third recognizes all types of E-signatures, but gives preferred status to the digital signature. Albania's Electronic Signature Law (ESL) is third generation; it recognizes all types of E-signatures, but favors use of the digital signature. Accreditation requirements are specified for Certification Service Providers (CSP), the issuers of certificates and verifiers to third parties that a digital signature is that of a specific subscriber. The CSP is responsible for maintaining the security of information that it receives from its subscribers. The CSP must inform the subscriber of any limitations on the use of the certificate. If an accredited CSP issues a qualified certificate, it must meet more stringent security requirements which can only be achieved with a digital signature. CSPs must maintain a publicly-accessible repository of certificates and the public keys which relying third parties can use to decrypt a subscriber's message. A CSP may incur legal liability for publishing a certificate with inaccurate information or for not issuing a private key to the subscriber corresponding to the public key in the repository. The ESL allows certificates issued by CSPs in foreign countries to be recognized if they provide sufficient security. The author recommends that the following provisions be added to Albania's E-Signature Law: (1) consumer protections for E-commerce participants; (2) several new computer crimes; (3) information technology courts; (4) mandatory E-government; and (5) explicit long-arm jurisdiction.

Keywords: *Albania, E-Commerce, E-Signature, Law*

[1] Author is an Associate Professor of Accounting and Business Law at Tarleton State University, Fort Worth, Texas USA.

 [ISSN 2581-5369]

I. ALBANIA: THE ECONOMY AND INTERNET INFRASTRUCTURE

Albania ended 46 years of Communist rule and established a multiparty democracy in the early 1990s. Since then, it has been making the difficult transition from a centrally-planned economy to a more modern open-market economy. Albania, with a population of 3.1 million, is now on the brink of achieving membership in the European Union (EU) after implementing EU-mandated justice reforms in 2016.[2]

Albania's Gross Domestic Product (GDP) was almost $40 billion in 2019 and GDP per capita in 2019 was about $14,000. The sectors contributing to Albania's GDP are: agriculture, 21.7%; industry, 24.2%; and services, 54.1%. GDP grew at a rate of 2.24% in 2019.[3] The unemployment rate in 2019 was 5.83%. The value of Albanian exports is approximately $900 million per year; those goods are primarily leather footwear, iron alloys, crude oil, clothing, electricity and perfumes.[4]

Broadband services were initiated in 2005 and the country continues to support the improvement of broadband availability and access. Albania has 2.2 million internet users and 72% of the population use the internet. Internet cafes are popular in Tirana and have begun to spread to other parts of the country. As the internet infrastructure develops, E-commerce is becoming more and more popular.[5] In order to stimulate the growth of E-commerce, further development of Albania's E-commerce law is needed.

II. THREE GENERATIONS OF ELECTRONIC SIGNATURE LAW

(A) First Generation: Digital Signature Required

In 1995, the U.S. State of Utah became the first jurisdiction in the world to enact an electronic signature law.[6] In the Utah statute, digital signatures were required and other types of electronic signatures were not recognized.[7] The authors of the Utah statute believed, with some justification, that digital signatures provide the greatest degree of security for electronic transactions. Utah was not alone; other jurisdictions granting exclusive recognition to the

[2] U.S. Central Intelligence Agency, "Albania," THE WORLD FACTBOOK, 16 June 2021; https://www.cia.gov/the-world-factbook/countries/albania/ .
[3] U.S. Department of State, Bureau of European and Eurasian Affairs, BACKGROUND NOTE: ALBANIA, 23 November 2020; https://www.state.gov/countries-areas/albania/
[4] *Supra Note 2.*
[5] *Supra Note 2.*
[6] UTAH CODE ANN. 46-3-101 *et seq.*, 1995. This first-generation statute was repealed in 2000 and replaced with the Uniform Electronic Transactions Act, a second-generation model law. UTAH CODE ANN. 46-4-101 *et seq.* (2000).
[7] Id.

digital signature include Argentina,[8] Bangladesh,[9] India[10], Malaysia,[11] Nepal,[12] New Zealand[13] and Russia.[14]

Unfortunately, these jurisdictions' decision to allow the utilization of only one form of technology is burdensome and overly-restrictive. Forcing users to employ digital signatures gives them more security, but this benefit may be outweighed by the digital signature's possible disadvantages: more expense because of the fee paid to the certification authority; lesser convenience due to being forced to use a certification authority; forcing users to use one type of technology to the exclusion of others when another type of technology might be better suited to a particular type of transaction; use of a more complicated technology which may be less adaptable to technologies used in other nations, or even by other persons within the same nation; inappropriate risk allocation between users if fraud occurs; and the potential disincentive to invest in development of alternative technologies.[15]

(B) Second Generation: All Types of E-Signatures Accepted

Jurisdictions in the Second Generation overcompensated. They did the complete reversal of the First Generation and did not include any technological restrictions whatsoever in their statutes. They did not insist upon the utilization of digital signatures, or any other form of technology, to the exclusion of other types of electronic signatures. These jurisdictions have been called "permissive" because they take a completely open-minded, liberal perspective on electronic signatures and do not contend that any one of them is necessarily better than the others. The United States of America[16] is a member of the second wave; the overriding majority of its jurisdictions (forty-five states, the District of Columbia, and the Territories of Puerto Rico and Virgin Islands) have enacted the Uniform Electronic Transactions Act (either in its entirety or with minor amendments), a permissive second-generation model law.[17] Australia has also

[8] Argentine Republic, DIGITAL SIGNATURE DECREE 2628/2002, 19 December 2002. The original act was amended by DIGITAL SIGNATURE DECREE 724/2006 on 8 June 2006.
[9] Bangladesh, INFORMATION TECHNOLOGY (ELECTRONIC TRANSACTION) ACT 2000 (Draft).
[10] Republic of India, THE INFORMATION TECHNOLOGY ACT, 9 June 2000.
[11] Republic of Malaysia, DIGITAL SIGNATURE ACT, 1997.
[12] Federal Democratic Republic of Nepal, ELECTRONIC TRANSACTIONS ORDINANCE NO. 32 OF THE YEAR 2061 B.S. (2005 A.D.), ss 60-71.
[13] New Zealand, ELECTRONIC TRANSACTIONS ACT 2000.
[14] Russian Federation, ELECTRONIC DIGITAL SIGNATURE LAW, Federal Law No. 1-FZ, 10 January 2002.
[15] Amelia H. Boss, "The Evolution of Commercial Law Norms: Lessons To Be Learned From Electronic Commerce," 34:3 BROOKLYN JOURNAL OF INTERNATIONAL LAW 673, 689-90 (2009).
[16] For analysis of American law, *see* Stephen E. Blythe, "E-Commerce and E-Signature Law of the United States of America," THE UKRAINIAN JOURNAL OF BUSINESS LAW, Kiev, Ukraine, November, 2008. For concise coverage of American, British, European Union and United Nations law, *see* Stephen E. Blythe, "Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce With Enhanced Security," 11: 2 RICHMOND JOURNAL OF LAW AND TECHNOLOGY 6 (2005).
[17] United States of America, National Conference of Commissioners on Uniform State Laws, UNIFORM ELECTRONIC TRANSACTIONS ACT, 7A U.L.A. 20 (Supp. 2000).

 [ISSN 2581-5369]

enacted a second-generation statute.[18]

The disadvantage of the permissive perspective is that it does not take into account that, in fact, some types of electronic signatures *are* better than others. A PIN number and a person's name typed at the end of an E-mail message are both forms of electronic signatures, but neither is able to even approach the degree of security that is provided by the digital signature.

(C) Third Generation: Acceptance of All E-Signatures, With Preference for Digital

Singapore led the Third Wave. In 1998, that country adopted a compromise, middle-of-the-road position with respect to the various types of electronic signatures. In terms of relative degree of technological neutrality, Singapore adopted a "hybrid" model—a preference for the digital signature in terms of greater legal presumption of reliability and security, but not to the exclusion of other forms of electronic signatures.[19] The digital signature is given more respect under the Singapore statute, but it is not granted a monopoly as in Utah. Singapore allows other types of electronic signatures to be employed. This technological open-mindedness is commensurate with a global perspective and allows parties to more easily consummate electronic transactions with parties from other nations.[20]

In recent years, more and more nations have joined the Third Generation. They recognize the security advantages afforded by the digital signature and indicate a preference for the digital signature over other forms of electronic signatures. This preference is exhibited in several ways: (1) utilization of a digital signature using a PKI system is explicitly required for authentication of an electronic record; (2) utilization of a digital signature with PKI seems to be necessary in order for an electronic record to comply with any statutory requirement that a record be in paper form; and (3) in order for a signature in electronic form to comply with a statutory requirement that a pen-and-paper signature be affixed, it must be a digital signature created with PKI. Nevertheless, the Third Generation jurisdictions do not appear to be as technologically-restrictive as those in the First Generation. They do not compel the E-commerce participant to use only the digital signature, *in lieu* of other forms of electronic signatures, as the State of Utah did in its original statute of 1995.

The moderate position adopted by Singapore has now become the progressive trend in international electronic signature law. The hybrid approach is the one taken by the European

[18] Commonwealth of Australia, ELECTRONIC TRANSACTIONS ACT 1999.

[19] Singapore's lawmakers were influenced by the U.N. Model Law on E-Commerce. *See* United Nations Commission on International Trade Law ("UNCITRAL"), MODEL LAW ON ELECTRONIC COMMERCE WITH GUIDE TO ENACTMENT ("MLEC") G.A. Res. 51/162, U.N. GAOR, 51st Sess., Supp. No. 49, at 336, U.N. Doc. A/51/49 (1996).

[20] Republic of Singapore, ELECTRONIC TRANSACTIONS ACT (Cap. 88), 10 July 1998, amended in 2010.

 [ISSN 2581-5369]

Union's E-Signatures Directive,[21] Armenia,[22] Azerbaijan[23] Barbados,[24] Bermuda,[25] Bulgaria,[26] Burma,[27] China[28] Colombia,[29] Croatia,[30] Dubai,[31] Egypt,[32] Finland,[33] Hong Kong,[34] Germany,[35] Hungary,[36] Iran,[37] Jamaica,[38] Japan,[39] Jordan,[40] Lithuania,[41] Pakistan,[42] Peru,[43] Poland,[44] Slovenia,[45] South Korea,[46] Taiwan,[47] Tunisia,[48] Turkey,[49] United Arab Emirates,[50]

[21] EUROPEAN UNION DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 13 DECEMBER 1999 ON A COMMUNITY FRAMEWORK FOR ELECTRONIC SIGNATURES, (1999/93/EC)—19 January 2000, OJ L OJ No L 13 p.12.
[22] Republic of Armenia, LAW ON ELECTRONIC DOCUMENT AND ELECTRONIC SIGNATURE, 2002.
[23] Republic of Azerbaijan, THE LAW OF THE AZERBAIJAN REPUBLIC ON DIGITAL ELECTRONIC SIGNATURE, 2003.
[24] Barbados, ELECTRONIC TRANSACTIONS ACT, CAP. 308B, 8 March 2001.
[25] Commonwealth of Bermuda, ELECTRONIC TRANSACTIONS ACT 1999.
[26] Republic of Bulgaria, LAW ON ELECTRONIC DOCUMENT AND ELECTRONIC SIGNATURE, 2001.
[27] The Union of Myanmar, ELECTRONIC TRANSACTIONS LAW, The State Peace and Development Council Law No. 5/2004, The 12 Waxing of Kason 1366 M.E., 30 April 2004.
[28] People's Republic of China, Order No. 18 of the President, LAW OF THE PEOPLE'S REPUBLIC OF CHINA ON ELECTRONIC SIGNATURE, Adopted at the 11th Meeting of the Standing Committee of the Tenth National People's Congress of the People's Republic of China, Promulgated 28 August 2004, Effective 1 April 2005.
[29] Republic of Colombia, LAW REGULATING DATA MESSAGES, ELECTRONIC TRADE, DIGITAL SIGNATURES AND CERTIFICATION ENTITIES, 13 January 1999.
[30] Republic of Croatia, ELECTRONIC SIGNATURE ACT, 17 January 2002.
[31] Emirate of Dubai, LAW OF ELECTRONIC TRANSACTIONS AND COMMERCE NO. 2/2002, 12 February 2002.
[32] Arab Republic of Egypt, LAW NO. 15/2004 ON E-SIGNATURE AND ESTABLISHMENT OF THE INFORMATION TECHNOLOGY INDUSTRY DEVELOPMENT AUTHORITY (ITIDA), 2004.
[33] Republic of Finland, Ministry of Justice, ACT ON ELECTRONIC SIGNATURES, 2003.
[34] Hong Kong Special Autonomous Region, People's Republic of China, ELECTRONIC TRANSACTIONS ORDINANCE, Ordinance No. 1 of 2000.
[35] Stephen E. Blythe, "A Critique of the German Electronic Signature Law and Recommendations for Improvement," a paper presented and published in the PROCEEDINGS OF THE ACADEMIC AND BUSINESS RESEARCH INSTITUTE INTERNATIONAL CONFERENCE, San Antonio, Texas USA, March 22-24, 2012.
[36] Republic of Hungary, ACT XXXV of 2001 ON ELECTRONIC SIGNATURE, 2001.
[37] Islamic Republic of Iran, ELECTRONIC COMMERCE LAW OF THE ISLAMIC REPUBLIC OF IRAN.
[38] Jamaica, ELECTRONIC TRANSACTIONS ACT, Act 15 of 2006..
[39] Japan, LAW CONCERNING ELECTRONIC SIGNATURES AND CERTIFICATION SERVICES, promulgated 24 May 2000, effective 1 April 2001.
[40] Hashemite Kingdom of Jordan, ELECTRONIC TRANSACTION LAW NO. 85 OF 2001.
[41] Republic of Lithuania, LAW ON ELECTRONIC SIGNATURE, No. VIII—1822 (July 11, 2000), As Amended, No. IX—934 (June 6, 2002).
[42]Islamic Republic of Pakistan, ELECTRONIC TRANSACTIONS ORDINANCE, 2002.
[43] Republic of Peru, LAW REGULATING DIGITAL SIGNATURES AND CERTIFICATES, 28 May 2000.
[44] Stephen E. Blythe, "Fine-Tuning Vietnam's Electronic Transactions Law In Order To Promote Growth of E-Commerce," a paper presented at the conference of the Eurasia Business and Economics Society, Warsaw, Poland, November 1-3, 2012.
[45] Republic of Slovenia, Centre for Informatics, ELECTRONIC COMMERCE AND ELECTRONIC SIGNATURE ACT, 2000.
[46] Korean Legislation Research Institute, DIGITAL SIGNATURE ACT NO. 5792, STATUTES OF THE REPUBLIC OF KOREA, Vol. 16 (II), pp. 1217-1220 (1999).
[47] Republic of China, ELECTRONIC SIGNATURES ACT, 2002.
[48] Republic of Tunisia, ELECTRONIC EXCHANGES AND ELECTRONIC COMMERCE LAW, 9 August 2000.
[49] Republic of Turkey, ELECTRONIC SIGNATURE LAW, 2004.
[50] United Arab Emirates, FEDERAL LAW NO. (1) OF 2006 ON ELECTRONIC COMMERCE ANDTRANSACTIONS, 30 January 2006.

 [ISSN 2581-5369]

Vanuatu[51] and in the proposed statute of Uganda.[52] Many other nations have adopted the hybrid approach; Albania is one of them.

III. ALBANIA'S E-SIGNATURE LAW

Albania enacted its Electronic Signature Law (hereinafter "ESL") in 2008.[53] The National Electronic Certification Authority ("Authority) is empowered to implement the ESL and may promulgate regulations to that effect.[54] The use of the electronic form is voluntary with respect to private transactions, but it may become mandatory with respect to government agencies.[55] In 2015, the ESL was amended to allow E-signatures and E-documents attested with a qualified certificate issued by a CSP to be used for all legal purposes.[56]

(A) Validity of E-Signatures

E-signatures and E-documents may be used in place of handwritten signatures and paper documents and have the same degree of legal validity.[57] In the case of a contract, a "qualified" E-signature (with relatively greater security features) must be used to sign the E-document.[58] A court of law presumes that an E-document signed by a qualified E-signature is accurate and unmodified, unless the contrary is proven.[59] A court of law will consider an E-signature to be invalid if the security requirements of the ESL are not complied with.[60] Foreign E-signatures and foreign E-signature products shall be recognized in accordance with treaties between the Republic of Albania and other jurisdictions.[61]

(B) The Authority's Regulation of Certification Service Providers

The Authority registers practicing Certification Service Providers ("CSP") and also keeps track of those who have discontinued CSP practice. The register is continually updated and published online.[62] In order to be registered, a prospective CSP must have: sufficient expertise; reliability; sufficient financial resources; high-quality technical products; and other qualifications

[51] Republic of Vanuatu, ELECTRONIC TRANSACTIONS ACT (Act. 24 of 2000).
[52] Republic of Uganda, ELECTRONIC SIGNATURES ACT, Draft, 2004.
[53] Republic of Albania, LAW NO. 9880 OF 25 FEBRUARY 2008 ON ELECTRONIC SIGNATURE ("ESL"), 2008.
[54] ESL art. 10.
[55] ESL art. 2.
[56] Republic of Albania, Law No. 107/2015 ON ELECTRONIC IDENTIFICATION AND TRUST SERVICES; https://cesk.gov.al/publicAnglisht_html/wp-content/uploads/2016/04/ligji107.pdf .
[57] ESL art. 4.
[58] ESL art. 5.
[59] ESL art. 8.
[60] ESL art. 9.
[61] ESL art. 54.
[62] ESL art. 11 and 20.

pursuant to the ESL.[63] The technical products used by the CSP must be independently tested and certified by the Authority.[64] The Authority is empowered to invalidate a qualified certificate issued by a CSP if: they are not secure enough to counter forgery, or the private key has a security defect.[65] The Authority has the right to inspect the worksite of the CSP, and the CSP is required to cooperate during the inspection.[66] The Authority shall make recommendations to the Council of Ministers pertinent to the fees allowed to be charged by CSPs.[67]

(C) Business Practices of Certification Service Providers

CSP's must continuously be able to prove that they are qualified to operate pursuant to the ESL.[68] However, a CSP is allowed to operate without registering with the Authority.[69] A CSP must inform the Authority whenever it is unable to comply with the requirements of ESL art. 19, which mandates the CSP to have reliability, expertise and insurance.[70] The CSP may transfer some of its task to qualified third parties, and it must submit an annual report to the Authority by March 1 of each year.[71]

A CSP is allowed to issue a qualified certificate only after the subscriber has provided sufficient identification and other personal information,[72] but a pseudonym may be used.[73] The CSP is bound to maintain confidentiality of this information, but the CSP must divulge it to law enforcement authorities if they request it.[74] In order to prevent forgery, the CSP must ensure the security of the signature codes at all times and use only reputable personnel.[75] The subscriber will be given ownership of the private key and must be kept informed of the degree of security of the private key.[76] The CSP must also inform the subscriber that a qualified E-signature has the same degree of legal validity as a handwritten signature, and also the presence of any conditions that the subscriber must comply with pertinent to the issuance of a qualified certificate.[77]

[63] ESL art. 13.
[64] ESL art. 49-52.
[65] ESL art. 14.
[66] ESL art. 16 and 17.
[67] ESL art. 55.
[68] ESL art. 19.
[69] ESL art. 18.
[70] ESL art. 21,
[71] ESL art. 22 and 23.
[72] ESL art. 24.
[73] ESL art. 26.
[74] ESL art. 48.
[75] ESL art. 27 and 28.
[76] ESL art. 29 and 30.
[77] ESL art. 31 and 32.

 [ISSN 2581-5369]

The qualified certificate must contain: subscriber's name or pseudonym; signature-test code, and the related algorithms; certificate number; dates of validity; name of CSP and its location; any limitations on usage or monetary amount; statement it is a qualified certificate; and any special attributes of the subscriber.[78] The CSP is mandated to invalidate the qualified certificate if the requirements of the ESL are not complied with, and the subscriber also has the right to invalidate it.[79] The CSP is also authorized to issue time stamps, and the CSP is mandated to document all of its security procedures undertaken.[80] The subscriber has the right to access of his file kept by the CSP,[81] and the CSP is not allowed to use the subscriber's personal data for any purpose not related to the CSP's business.[82]

If the CSP fails to abide by the ESL, the CSP is liable to third parties incurring damages as a result thereof.[83] On the other hand, a CSP may avoid liability to third parties if it is able to prove it is not responsible for the damages.[84] The damages may not exceed any limitations on damages appearing on the face of the qualified certificate.[85] To ensure that it will be able to pay such damages, the CSP is responsible for procuring adequate insurance coverage or for the establishment of a monetary reserve for this purpose.[86]

A CSP planning to go out of business must inform the Authority. Those CSPs must inform their subscribers and must revoke all certificates that have been issued. Furthermore, they must find another CSP to assume their responsibilities.[87]

(D) Administrative Regulations to be Enforced with a Fine

The ESL does not contain computer crimes. However, it does contain two sets of administrative regulations. The first set provides for a maximum fine of 2 million Albanian Leke ("ALL") if the CSP fails: to report commencement of operations; to obtain adequate identification of the subscriber; fails to require proof of authorization to act on behalf of a third party, or get prior approval of a third party; or comply with the requirements for going out of business. The second set provides for a maximum fine of 1 million ALL if the CSP fails: to comply with the requirements for operation of a CSP business; to comply with its security requirements; to prepare and submit its annual report; or to cooperate with the Authority during an inspection

[78] ESL art. 33.
[79] ESL art. 35 and 36.
[80] ESL art. 38 and 39.
[81] ESL art. 40.
[82] ESL art. 47.
[83] ESL art.41.
[84] ESL art. 42.
[85] ESL art. 43.
[86] ESL art. 45.
[87] ESL art. 46.

 [ISSN 2581-5369]

or to divulge the identity of a subscriber to law enforcement authorities.[88]

In addition to the sanctions mentioned above, the Authority is empowered to shut down a CSP whenever it engages in violations of the ESL which are sufficient to "pose a threat to the integrity and reliability" of the CSP.[89]

An appeal may be made to the Council of Ministers in reference to the above sanctions.[90]

IV. RECOMMENDATIONS FOR IMPROVEMENT OF THE E-SIGNATURE LAW

Add: Consumer Protections in E-Commerce Contracts

Albania has created good consumer protections for recipients of service providers. However, consumer protections for other types of E-commerce contracts seem to have been overlooked. As a model, Albania can look to Tunisia for an example of a nation with good consumer protections for E-commerce buyers. All of Tunisia's E-commerce consumer protections are commendable: (1) buyers have a "last chance" to review the order before it is entered into; (2) they have a 10-day window of opportunity to withdraw from the agreement after it has been made; (3) they have the right to a refund if the goods are late or if they do not conform to the specifications; and (4) the risk remaining on the seller during the 10-day trial period after the goods have been received.[91]

Add: Several New Computer Crimes

The following computer crimes should be recognized: (a) Unauthorized Access to Computer Material; (b) Unauthorized Tampering with Computer Information; (c) Unauthorized Use of a Computer Service; (d) Unauthorized Interference in the Operation of a Computer; and (e) Unauthorized Dissemination of Computer Access Codes or Passwords. The Singapore Computer Misuse Act can be used as a model.[92]

Add: Information Technology Courts

Because of the specialized knowledge often required in the adjudication of E-commerce disputes, Information Technology Courts should be established as a court-of- first-instance for them. The I.T. Courts would be tribunals consisting of three experts. The chairperson would be an attorney versed in E-commerce law, and the other two persons would be an I.T. expert and a business management expert. The attorney would be required to hold a law degree and

[88] ESL art. 56.
[89] ESL art. 57.
[90] ESL art. 58.
[91] Republic of Tunisia, ELECTRONIC EXCHANGES AND ELECTRONIC COMMERCE LAW, 2000.
[92] Republic of Singapore, COMPUTER MISUSE ACT (Cap. 50A), 30 August 1993.

 [ISSN 2581-5369]

be a member of the bar with relevant legal experience; the I.T. person would be required to hold a graduate degree in an I.T.-related field and have experience in that field; and the business management expert would be required to hold a graduate degree in business administration and have managerial experience. The E-commerce law of Nepal can be used as a model.[93]

Add: Mandatory E-Government

In order to reduce cost and to make governmental functions more convenient for citizens, E-government needs to be emphasized and mandated. By established deadlines, governmental departments should begin to convert to provision of online services if possible. The best example for Albania to follow in implementation of mandatory E-Government is Puerto Rico; its Electronic Government Act is exemplary.[94]

Add: Explicit Long-Arm Jurisdiction

Because so many of the E-transactions will occur between Albanians and parties outside the borders of the nation, it would be prudent for Albania to formally state its claim of "long arm" jurisdiction against any party who is a resident or citizen of a foreign country, so long as that party has established "minimum contacts" with Albania.[95] Minimum contacts will exist, for example, if a cyber-seller outside of Albania makes a sale to a party living within Albania. In that situation, the cyber laws of Albania should be applicable to the foreign person or entity outside of Albania because that person or firm has had an effect upon Albania through the transmission of a message that was received in Albania. The foreign party should not be allowed to evade the jurisdiction of the Albanian courts merely because they are not physically present in the country. After all, E-commerce is an inherently international phenomenon.

V. CONCLUSIONS

Albania's E-Signature Law is third generation; it distinguishes "E-signatures" and "qualified E-signatures." However, too much of the statute is devoted to the regulation and required business practices of Certification Service Providers and not enough attention is devoted to other important issues. The following provisions are recommended to be added: (1) consumer

[93] Kingdom of Nepal, ELECTRONIC TRANSACTIONS ORDINANCE NO. 32 OF THE YEAR 2061 B.S. (2005 A.D.), s 60-71.
[94] Commonwealth of Puerto Rico, ELECTRONIC GOVERNMENT ACT ("EGA"), Act No. 151 of 22 June 2004; http://www.oslpr.org/download/en/2004/0151.pdf.
[95] The Republic of Tonga is an example of a nation that has claimed long-arm jurisdiction over E-commerce parties, and its statute may be used as a model. See, Stephen E. Blythe, "South Pacific Computer Law: Promoting E-Commerce in Vanuatu and Fighting Cyber-Crime in Tonga," 10:1 JOURNAL OF SOUTH PACIFIC LAW (2006), a publication of the School of Law, University of the South Pacific, Emalus Campus, Port Vila, Republic of Vanuatu.

 [ISSN 2581-5369]

protections for E-commerce participants; (2) several new computer crimes; (3) information technology courts; (4) mandatory E-government; (5) and explicit long-arm jurisdiction.

*****

 [ISSN 2581-5369]