CAREC Institute

Regulatory Framework for e-Commerce Development in CAREC

Policy Brief

April 2020

Disclaimer

The CAREC Institute working paper and policy brief series is a forum for stimulating discussion and eliciting feedback on ongoing and recently completed research and workshops undertaken by the CAREC Institute staff, consultants, or resource persons. The series deals with key economic and development issues, particularly those facing the CAREC region, as well as conceptual, analytical, or methodological issues relating to project/program economic analysis, and statistical data and measurement.

Mr. John Gregory, Research Consultant of the Asian Development Bank (ADB), in cooperation with the CAREC Institute, worked on the brief. This policy brief builds on a research report which will be published in Q3 2020.

The views expressed in this paper are the views of the author and do not necessarily reflect the views or policies of CAREC Institute, its funding entities, or its Governing Council. CAREC Institute does not guarantee the accuracy of the data included in this paper and accepts no responsibility for any consequences of their use. Terminology used may not necessarily be consistent with CAREC Institute official terms.

Central Asia Regional Economic Cooperation (CAREC) Institute
No. 376 Nanchang Road, Urumqi, Xinjiang, the PRC
f: +86.991.8891151
LinkedIn
km@carecinstitute.org
www.carecinstitute.org

Table of Contents

Abbreviations

ADB	Asian Development Bank
CAREC	Central Asia Regional Economic Cooperation
CISG	Convention on the International Sale of Goods
COE	Council of Europe
ECC	Electronic Communications Convention
ESCAP	United Nations Economic and Social Commission for Asia and the Pacific
FAPT	Framework Agreement on Facilitation of Cross-border Paperless Trade
ODR	Online Dispute Resolution
OECD	Organisation for Economic Co-operation and Development
PKI	Public Key Infrastructure
PRC	People's Republic of China
TFA	Trade Facilitation Agreement
UNCITRAL	United Nations Commission on International Trade Law
UNCTAD	United Nations Conference on Trade and Development

1. Executive Summary

Today, the whole world is in the information age. The globalization of commerce requires consistent laws and regulations not only to authorize but also to regulate electronic communications.

For this purpose, the CAREC members have all enacted relevant laws but the laws are not always consistent, and they are often out of step with the best practices. After a rigorous review of the relevant legislation and the dominant international literature and model laws, it is recommended that CAREC members update their legislative framework, ensure conformity with internationally recognized standards, and harmonize laws and approaches among themselves. Adherence to a number of international conventions is also recommended in this process.

This policy brief sets out the key policy issues: how strictly the state must prescribe acceptable methods of authenticating text and transacting parties; what shall be done to promote privacy, to prevent cybercrime and to protect consumers; how to follow the leading international trends, while expressing some concerns about the ability of private and public actors to make safe choices and about the ability of some member states to administer an effective regulatory regime.

2. Background

Most of the world today communicates electronically or would like to do so. Increasing proportions of the world's trade is carried out online, both internationally and within countries.

Electronic commerce offers many benefits at both levels. Domestically, in the words of ADB/ESCAP (2018), "[i]t has improved economic efficiency and created many new jobs in developing economies and least developed countries, offering a chance for them to narrow development gaps and increase inclusiveness—whether demographic, economic, geographic, cultural, or linguistic. It also helps narrow the rural–urban divide."

Internationally, as ESCAP has written (2019), "[b]enefits from the successful implementation of cross-border paperless trade are large, with the potential to cut transaction costs by 25% across Asia and the Pacific region, as well as to increase regulatory compliance, reduce illicit financial flows and facilitate engagement in the increasingly digital global economy." It "allows small and medium-sized enterprises to reach global markets and compete on an international scale." (ADB/ESCAP, 2018)

However, the commercial law applicable to these transactions has not always kept up to the new realities. To the extent that it has been amended with electronic commerce in mind, different countries have taken different paths. In a time of global or regional economic blocs, these differences can cause inefficiencies in or barriers to trade.

In short, there are two sets of issues: laws that do not recognize e-commerce and laws that recognize it inconsistently, and possibly inadequately.

These issues are observed among CAREC members, though they are far from unique to CAREC. Broadly defined, the present document makes recommendations that may help these states in improving their receptiveness to e-commerce.

3. Methodology

This policy brief builds on a research report which will be published in Q3 2020. The report reviews the legislative and regulatory texts from all CAREC members relating to electronic transactions,

electronic payments, privacy, cybercrime, and consumer protection. It also reviews the significant literature on contemporary e-commerce laws, notably from international bodies, such as the United Nations Commission on International Trade Law (UNCITRAL), the principal source of legal thinking in this field for over 30 years, as well as the United Nations Conference on Trade and Development (UNCTAD), the Asian Development Bank (ADB), and the UN Economic and Social Commission for Asia and the Pacific (UN/ESCAP). Publications of intergovernmental organizations and non-governmental bodies, e.g. the Council of Europe (COE) and the Organization of Economic Cooperation and Development (OECD), were also consulted. Private and academic studies were considered as well. The report contains a detailed bibliography.

4. Policy Context

Contemporary analysts of economic development and electronic commerce widely recognize that the legal regime applicable to e-commerce is only one element of its proper implementation and expansion. It is also crucial that a country reaches a proper state of economic development, with a trade relation infrastructure – commercial dealings, government communications – and access to technology that can support e-commerce.

In addition, popular attitudes to technology and to commerce generally can affect the social or even cultural acceptance of electronic transactions. If strangers are considered likely to be dishonest, or if e-communications are thought to be unreliable, then the law will have more difficulty enabling people to trust the transactions and engage in e-commerce. Opening the door does not mean that anyone will pass through it.

Moreover, different states have different capacities to govern a mature e-commerce system. Some of the trustworthy elements that may overcome the social or cultural hesitation just mentioned – such as good laws on personal privacy, the prevention of computer-based crime ("cybercrime") and legal basis for consumer protection – will succeed only with state power behind them. The CAREC members need to reflect on their capacity to design and administer effective regulatory and dispute-resolution systems for these purposes.

These collateral issues are beyond the scope of this document but cannot be beyond the concerns of policymakers wishing to promote e-commerce and modernize the economy and improve the lives of their citizens.

5. Policy Options and Recommendations

This chapter examines the key decisions needed to build or harmonize the legal and regulatory framework for electronic commerce.

5.1 Electronic Transactions

Should the statutes reflect technology neutrality or spell out the technology needed to have legal effect?

The principal global text on the law of electronic commerce is UNCITRAL's Model Law on Electronic Commerce (1996), supplemented by the Model Law on Electronic Signatures (2001). UNCITRAL's guiding principle is technology neutrality, i.e. not specifying what technology should be used to achieve legal validity for commercial uses of electronic communications.

Many states around the world have found this approach insufficient to ensure what they considered adequate reliability of authentication of origin or integrity of electronic documents. They require use of a special electronic signature known as a "digital signature," created by a special encryption ("public key cryptography"). Usually in such a system, the link between the signature code and the signatory is proved by a certificate from a trusted third party (a "certification service provider," though the name varies from country to country).

The network of duties and functions of issuers and users of digital signatures and certificates is known as a Public Key Infrastructure (PKI).

PKIs are appealing in principle but very cumbersome to manage in practice. Proving that one has complied with the technical demands can be difficult. As a result, a number of countries, including Russia, whose laws have influenced several CAREC members, have relaxed their e-signature requirements over the past decade to allow for some non-PKI signatures and some e-documents without a digital signature.

RECOMMENDATION: CAREC members should legislate a hybrid system maximizing the autonomy of commercial parties to satisfy themselves on signature and document technology, while ensuring that official or vulnerable parties have legal safe harbors for their reliable e-communications.

The situation among CAREC members is quite varied. Some have old-style PKI statutes, some have newer more flexible ones, while the terms and conditions are not consistent among them. This policy brief recommends more flexibility, considering that CAREC countries would benefit from increasing the right of transacting parties to agree on their own standards, within limits.

Some CAREC members have a single law on e-transactions, often called "law on electronic signature and electronic document." Such a law often makes an e-document legally effective only if it has a secure form of e-signature.

Other states have two laws, one on e-documents and one on e-signatures. They may give some scope for an e-document to stand on its own, legally, though they usually still need some form of e-signature associated with the document for it to be valid. The e-signature statute may go on to prescribe conditions for the certification of e-signatures to prove their reliability. It is desirable to have a single law to increase the chances of internal consistency, when all relevant rules are in one place.

i. IN FAVOUR OF TECHNOLOGY NEUTRALITY

- E-signatures can be flexible, serving the commercial and security needs of the transacting parties.
- The state need not be involved in prescribing technology that is bound to change over time (or have laws that require outdated technology.)

ii. IN FAVOUR OF TECHNOLOGY SPECIFICITY (DIGITAL SIGNATURES)

- Many transacting parties, whether businesses or individuals, do not have the capacity to judge the reliability of an e-signing technology or e-document, so having the law prescribe how to do it gives them more trust in the system.

- The business operations and best practices of a certification service provider are by now well-known and can be put into legislation or regulation in consistent ways.

iii. IN FAVOUR OF A "HYBRID" LAW WITH ELEMENTS OF BOTH SYSTEMS

- Some parties do not need the full PKI treatment and find it expensive and difficult.
- Some transactions do not justify the expense of using digital signature technology and the services of a trusted third party.
- On the other hand, some communications are particularly important (those with public officials, for example, or those in very high-value transactions) and require more assurance of authenticity than a routine commercial deal.

International Harmonization

Electronic communications cross national borders readily. Both businesses and governments benefit from this potential. The policy consequence is that laws should be harmonized according to reputable international standards.

The principal relevant international standards are:

A. United Nations Convention on the International Sale of Goods (CISG): The CISG, originally adopted in 1980, sets out basic rules of contract law for international sales of goods. Expert review in the early 21st century concluded that it could be applied to electronic sales.
B. UN/ESCAP Framework Agreement on the facilitation of cross-border paperless trade (Framework Agreement): The Framework Agreement sets out principles and priorities for member states to legislate on cross-border e-commerce, without prescribing specific texts. It also provides opportunities for collaboration and mutual support in legal development.
C. United Nations Convention on the use of electronic communication in international contracts, or Electronic Communications Convention (ECC): the ECC sets out how electronic contracts can be integrated into the commercial laws of member states. It can be made to work as domestic law as well.

RECOMMENDATION: CAREC members should harmonize their e-transactions laws by becoming members of these three conventions (CISG, UNESCAP, ECC), if they are not already members.

Further, the Trade Facilitation Agreement (TFA) of the World Trade Organization imposes certain obligations on parties to transact public business, such as customs processing electronically, etc. It would facilitation harmonization if the remaining CAREC members – Azerbaijan, Turkmenistan, Uzbekistan - joined the TFA.

5.2 Regulatory Matters

Privacy

Computers can collect huge amounts of personal information, directly or indirectly, in just about any activity that a person undertakes online. Bits of information can be combined by powerful

processors to give detailed profiles of people's lives and preferences. Such a potential can undermine people's trust in e-communications and reduce their engagement in e-commerce. This tendency has been considered dangerous for decades. The Organization for Economic Cooperation and Development (OECD) issued Guidelines for cross-border data flow in 1980, and their principles are reflected in privacy legislation of many countries. The OECD updated its guidelines in 2013 to account for increases in connectivity and computing power since 1980. In addition, there is an international convention to give legal effect to the OECD principles for cross-border transactions.

Most, though not all, CAREC members have some form of privacy legislation. The laws tend to reflect the main points of the international standards: personal data should be collected only with the consent the data subject and only for the purpose for which the consent was obtained. The data should not be kept longer than necessary.

RECOMMENDATION: All CAREC members should have privacy legislation consistent with international best practices and that ensures protection of personal data of their residents both at home and when it crosses national borders. Consideration should be given to adopting the latest Council of Europe convention on the topic.

Some classes of personal data are sensitive. Privacy laws often give special protection to these classes of data. Electronic data crosses national borders as if they did not exist. Privacy laws restrict the holders of data from transferring personal data outside the country except with consent of the data subject, unless the destination country gives equivalent protection to personal data as the country of origin. International treaties may ensure such equivalence or make special provisions about transfers.

It is assumed that there is no serious controversy about whether or even how to protect personal privacy. There may be questions of design of how privacy rights are enforced, but such matters of public administration are beyond the scope of this policy brief.

Cybercrime

All CAREC members have laws about criminal activity by traditional means, including documentary crimes like fraud or forgery. Computers give opportunities for new kinds of criminal activities, notably including interference with data and data flows. Such intangibles may not be protected by traditional laws. For example, courts in some countries have found that data as such could not be the subject of property, it could not be owned – and as a result could not be stolen.

Illicit online activities include:

- unauthorized access to a computer or a network, which is sometimes prohibited in every case and sometimes only if there is damage to data or interference in operations.
- infecting computers or networks with malware that harms or prevents their operation entirely, whether for malice, commercial advantage or extortion ("ransomware")
- exceeding one's authority to access a network and causing various harm.

The Council of Europe created the Budapest Convention on Cybercrime in 2001. It requires its parties (including two of CAREC members, Azerbaijan and Georgia) to legislate against a number of

crimes, including those mentioned above, plus online fraud, forgery and child pornography. It also provides for international cooperation to track down and prosecute cross-border offenders.
An alternative to the Budapest Convention has been proposed to the United Nations by Russia, with the support of the PRC. It too requires states to legislate against a similar list of crimes. Its administrative cooperation provisions differ from the Budapest Convention, though.

RECOMMENDATION: CAREC members should ensure that their laws prohibit the activities provided in the international conventions, and that their ability to collaborate in international enforcement efforts – including exchanging data on local proceedings and local suspects – is adequate to the challenges of cross-border crime.

Most CAREC members have very consistent provisions on cybercrime, clearly derived from a single model. Those that do not, should enact them. It may be that the administrative cooperation with foreign investigations is the most important gap in those statutes – though such matters may be covered elsewhere in the national law than the e-crime provisions.

Consumer Protection

The other major barrier to consumer trust in e-commerce is whether consumers will actually receive the goods and services that they buy online, and whether they can get a remedy if there are defects. Such issues are dealt with in consumer protection legislation, as adapted to the age of Internet commerce.

Many CAREC members have no consumer protection laws under that name, though provisions against fraud or misrepresentation would be relevant to consumers as well as to businesses. The laws in place in the countries that do have them are quite varied, some modern, some out of date or partial.

A serious challenge to effective consumer protection legislation is the need to enforce any rights it creates. Many countries set up consumer protection bureaus to deal with consumer complaints (offline or online), with the power to compel remedial behavior by the merchants. Some countries offer special tribunals to deal with low value high volume disputes in either courts ("small claims courts") or through alternative dispute resolution mechanisms, online (ODR) or offline.

Such mechanisms can be expensive and difficult to set up and run. States need to be cautious about raising expectations about protection that cannot be met. If that were to happen, consumer trust in e-commerce would be lower than it would be with no legislation.

RECOMMENDATION: CAREC members should adopt consumer protection legislation consistent with the UN and OECD models, with particular attention to the ability of the state to offer reliable enforcement of consumer rights given by the legislation.

Some CAREC countries are said to have consumer protection laws that are not effective because consumers do not know their rights or how to enforce them. A remedy to this problem lies in

direct government communications and possibly in enforcement action – not in the law as such. There are international models for consumer protection laws, notably from the United Nations, with a text from the OECD on e-commerce for consumers.

It may be noted that often small business purchasers have the same needs as consumers, and the same lack of bargaining power with large online sellers. As a result, trust in e-commerce at the merchant as well as the consumer level may be increased by extending similar protections to small businesses with respect to their suppliers as are given to consumers generally.

The CAREC members should also participate in the international enforcement of consumer rights, including assisting cross-border investigations. The International Consumer Protection and Enforcement Network (ICPEN) may be found to offer the right forum for this participation.

6. Way Forward

To facilitate implementation of recommendations, all CAREC members should collectively decide as a priority to ensure that their laws support electronic commerce, including rules on privacy, cybercrime and consumer protection, both domestically and among themselves.

Towards this goal, each state should take the following steps:

- Establish a dedicated multi-ministry task force with support at the highest levels.
- Include private-sector representation on some version of this group.
- Coordinate legal advice across government. Different departments or agencies must end up with consistent opinions on key matters.
- Ensure that all parts of the government and other players have the right and capacity to communicate electronically.
- Replicate the national work at the international level and coordinate the two levels.
- Work closely with ESCAP technical and legal working groups, if not already doing so. This can be done even before becoming a member of the Framework Agreement.

7. Consultation Mechanism

Governments should use their usual methods of consultation of affected interests. Among them would be surveys of business and trade associations or professional bodies, if any. Selected private-sector membership on national or international working groups would facilitate the two-way flow of information and advice.

This interaction could be particularly helpful in drawing the line between transactions or documents that may be authenticated as parties choose, and those subject to more reliable and technology specific processes, on the other.

The CAREC Program already has institutional methods of collaboration that can be used to coordinate the progress and the content of law reform. National efforts should not wait indefinitely for international developments to unroll, but so far as possible, all states should keep in mind the desirability of harmonized laws in this field.

8. Public and Private Responsibility and Control

A state must decide in any field of e-commerce whether to rely mostly on self-regulation or on state supervision Some factors to achieve the balance include:

- The importance of private initiative vs. need to control social and economic activity in the country.
- The degree of trust in the private sector's competence to choose appropriate measures vs. the degree to which the state itself or the population depends on government support.
- The perceived balance between the appropriate promotion of private interests vs. the promotion or protection of public policy goals.
- To a greater extent, the degree of regulation required by or wanted in a system depends on the degree of risk that the system is willing to tolerate. The risks include:

    - ✓ Risk to the parties themselves. Do they have the ability to make good decisions in novel areas? Are they competent to decide? Do they have a practical or moral freedom to fail? A prime example of an area of choice is authentication, including e-signatures.
    - ✓ Risk to others. Does a less-regulated system expose others (whether in business to business (B2B) or business to consumer (B2C) dealings) to fraud or mistake? To what extent can one trust the competence and honesty of private actors?
    - ✓ Risk to public policy. How much uncertainty can a government tolerate? How much business failure should be allowed? At what cost to the economy? At what cost to the state?

9. Conclusions

The CAREC members are on the way to having workable legislation and regulation for e-commerce. They are at different stages in this journey. This policy brief aims to facilitate modernization and harmonization of the e-commerce framework.

The CAREC members shall use their existing cooperation mechanisms to work toward these goals. The ultimate aim is to maximize consistency and minimize tendencies to protect one's own national interests, or even just legislative styles, against useful compliance with recognized international standards.

It is likely that member states will progress unevenly from their uneven starting points. This is not a reason to abandon the effort. Working to follow these recommendations will create better and more harmonized legislation than leaving such matters to chance or the changeable political currents of the day.

10. Appendices

10.1 Recommendations for Domestic Law Reform

Reform Needed	Countries	Discussion
Adopt UN ECC for domestic law	All	Models of domestic ECC laws in Singapore, Australia, Canada (Uniform Act)
Maximize and harmonize ability to use simple e-signatures	All	Some have some flexibility, but none has Enough
Harmonize certification process for digital signatures	All	Is one country's model working best? State supervision needed but not necessarily state monopoly.
Harmonize cybercrime legislation with international standards	All	CAREC members are largely consistent on this point. Consider the states' capacity to enforce.
Enact modern privacy legislation	PAK, TKM	Consider the states' capacity to enforce
Enact modern consumer protection legislation	GEO, KGZ, KAZ, MON, PAK, TAJ, TKM	Consider the states' capacity to enforce
Establish framework for electronic payments	PAK, UZB	All members have something in place, with exception of PAK and UZB

10.2 Recommendations for International Instruments

Instrument	Type/Scope	CAREC Members as Parties
UNCITRAL Electronic Communications Convention (ECC)	Global	AZE (Recommend: ALL for domestic & international)
ESCAP Framework Agreement on Facilitation of Cross-border Paperless Trade (FAPT)	Regional	AZE, CHN (Recommend: ALL)
Convention on the International Sale of Goods (CISG)	Global	AZ, CHN, GEO, KGZ, MON, UZB (Recommend: ALL)
World Trade Organization Trade Facilitation Agreement (WTO TFA)	Global	AFN, CHN, GEO, KGZ, KAZ, MON, PAK, TAJ
Revised Kyoto Customs Convention	Global	AZE, CHN, KAZ, MON (w/ UZB upcoming)
Council of Europe (Budapest) Cybercrime Convention	Global	AZE, GEO
TIR Trucking Convention (has an electronic supplement)	Global	AFN, AZE, CHN, GEO, KGZ, KAZ, MON, PAK, TAJ, TKM, UZB
[many others for specific areas of trade]	Global/ regional	Some mentioned in the body of the report (to be published in Q3 2020). Some may authorize e-documents even if general law does not.

11. References

Asian Development Bank (ADB) and United Nations Economic and Social Commission for Asia and the Pacific (ESCAP). (2018). Embracing the e-Commerce Revolution in Asia and the Pacific (ESCAP & ADB). Retrieved from https://www.adb.org/sites/default/files/publication/430401/embracing-e-commerce-revolution.pdf

United Nations Economic and Social Commission for Asia and the Pacific (ESCAP). (2019). Readiness Assessment for Cross-border Paperless Trade: MONGOLIA. Retrieved from https://www.unescap.org/resources/readiness-assessment-cross-border-paperless-trade-mongolia

United Nations Commission on International Trade Law (UNCITRAL). (1996). Model Law on Electronic Commerce. Retrieved from https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce

United Nations Commission on International Trade Law (UNCITRAL). (2001), Model Law on Electronic Signatures. Retrieved from https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures

United Nations Commission on International Trade Law (UNCITRAL). (1980). Convention on the International Sale of Goods. Retrieved from https://www.uncitral.org/pdf/english/texts/sales/cisg/V1056997-CISG-e-book.pdf

United Nations Economic and Social Commission for Asia and the Pacific (ESCAP). (2016). UN/ESCAP Framework Agreement on the facilitation of cross-border paperless trade. Retrieved from https://www.unescap.org/resources/framework-agreement-facilitation-cross-border-paperless-trade-asia-and-pacific

United Nations Commission on International Trade Law (UNCITRAL). (2005). Convention on the Use of Electronic Communications in International Contracts ("Electronic Communications Convention"). Retrieved from http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html

Organization for Economic Cooperation and Development (OECD). (1980, 2013). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Retrieved from: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Council of Europe. (2001). Budapest Cybercrime Convention. Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

Organization for Economic Cooperation and Development (OECD). (1999,2016). Guidelines for Consumer Protection in the Context of Electronic Commerce. Retrieved from https://www.oecd.org/sti/consumer/oecdguidelinesforconsumerprotectioninthecontextofelectroniccommerce1999.htm AND https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf